



Quidway S5300 Series Ethernet Switches  
V100R002C02

## **Configuration Guide - IP Service**

|                    |            |
|--------------------|------------|
| <b>Issue</b>       | 02         |
| <b>Date</b>        | 2009-02-16 |
| <b>Part Number</b> |            |

Huawei Technologies Co., Ltd. provides customers with comprehensive technical support and service. For any assistance, please contact our local office or company headquarters.

## Huawei Technologies Co., Ltd.

Address: Huawei Industrial Base  
Bantian, Longgang  
Shenzhen 518129  
People's Republic of China

Website: <http://www.huawei.com>

Email: [support@huawei.com](mailto:support@huawei.com)

**Copyright © Huawei Technologies Co., Ltd. 2009. All rights reserved.**

No part of this document may be reproduced or transmitted in any form or by any means without prior written consent of Huawei Technologies Co., Ltd.

### Trademarks and Permissions



HUAWEI and other Huawei trademarks are the property of Huawei Technologies Co., Ltd.

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

### Notice

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 the statements, information, and recommendations in this document do not constitute a warranty of any kind, express or implied.

---

# Contents

---

|  |            |
|--|------------|
| <b>About This Document.....</b>  | <b>1</b>   |
| <b>1 IP Addresses Configuration.....</b>   | <b>1-1</b> |
| 1.1 Overview.....  | 1-2        |
| 1.1.1 Introduction to IP Addresses.....  | 1-2        |
| 1.1.2 Features of IP Addresses Supported by the S-switch.....                    | 1-2        |
| 1.1.3 Update History.....  | 1-2        |
| 1.2 Configuring IP Addresses for Interfaces.....                                 | 1-2        |
| 1.2.1 Establishing the Configuration Task.....                                   | 1-2        |
| 1.2.2 Configuring a Primary IP Address for an VLAN Interface.....                | 1-3        |
| 1.2.3 (Optional) Configuring a Secondary IP Address for an VLANIF Interface..... | 1-4        |
| 1.2.4 Checking the Configuration.....  | 1-4        |
| 1.3 Maintaining.....   | 1-5        |
| 1.3.1 Monitoring Network Operation Status.....                                   | 1-5        |
| 1.4 Configuration Examples.....  | 1-5        |
| 1.4.1 Example for Configuring Primary and Secondary IP Addresses.....            | 1-5        |
| <b>2 ARP Configuration.....</b>  | <b>2-1</b> |
| 2.1 Overview.....  | 2-2        |
| 2.1.1 Introduction to ARP.....   | 2-2        |
| 2.1.2 Features of ARP Supported by the S-switch.....                             | 2-2        |
| 2.1.3 Update History.....  | 2-2        |
| 2.2 Configuring ARP.....   | 2-2        |
| 2.2.1 Establishing the Configuration Task.....                                   | 2-2        |
| 2.2.2 Configuring Static ARP Entries.....  | 2-3        |
| 2.2.3 Optimizing Dynamic ARP.....  | 2-4        |
| 2.2.4 Checking the Configuration.....  | 2-5        |
| 2.3 Configuring Proxy ARP.....   | 2-6        |
| 2.3.1 Establishing the Configuration Task.....                                   | 2-6        |
| 2.3.2 Configuring an IP Addresses for the VLANIF Interface.....                  | 2-6        |
| 2.3.3 Enabling Proxy ARP Function.....   | 2-7        |
| 2.3.4 Checking the Configuration.....  | 2-7        |
| 2.4 Configuring Proxy ARP Between VLANs.....                                     | 2-8        |
| 2.4.1 Establishing the Configuration Task.....                                   | 2-9        |

|   |            |
|---|------------|
| 2.4.2 Configuring an IP Addresses for the VLANIF Interface..... | 2-9        |
| 2.4.3 Enabling Proxy ARP Between VLANs.....                     | 2-10       |
| 2.4.4 Checking the Configuration.....                           | 2-10       |
| 2.5 Maintaining ARP.....  | 2-11       |
| 2.5.1 Clearing ARP Statistics.....                              | 2-11       |
| 2.5.2 Monitoring Network Operation Status.....                  | 2-12       |
| 2.5.3 Debugging ARP.....  | 2-12       |
| 2.6 Configuration Examples.....                                 | 2-12       |
| 2.6.1 Example for Configuring Static ARP.....                   | 2-13       |
| 2.6.2 Example for Configuring Dynamic ARP.....                  | 2-14       |
| 2.6.3 Example for Configuring Proxy ARP.....                    | 2-16       |
| 2.6.4 Example for Configuring Proxy ARP Between VLANs.....      | 2-18       |
| <b>3 DNS Configuration.....</b>                                 | <b>3-1</b> |
| 3.1 Overview.....   | 3-2        |
| 3.1.1 Introduction to DNS.....                                  | 3-2        |
| 3.1.2 DNS Supported by the S-switch.....                        | 3-2        |
| 3.1.3 Update History.....                                       | 3-2        |
| 3.2 Configuring DNS.....  | 3-2        |
| 3.2.1 Establishing the Configuration Task.....                  | 3-2        |
| 3.2.2 Configuring Static DNS Entries.....                       | 3-3        |
| 3.2.3 Configuring Dynamic DNS.....                              | 3-4        |
| 3.2.4 Checking the Configuration.....                           | 3-4        |
| 3.3 Maintaining DNS.....  | 3-5        |
| 3.3.1 Clearing DNS Entries.....                                 | 3-5        |
| 3.3.2 Monitoring Network Operation Status.....                  | 3-6        |
| 3.3.3 Debugging DNS.....  | 3-6        |
| 3.4 Configuration Examples.....                                 | 3-6        |
| 3.4.1 Example for Configuring DNS.....                          | 3-7        |
| <b>4 DHCP Configuration.....</b>                                | <b>4-1</b> |
| 4.1 Overview.....   | 4-2        |
| 4.1.1 Introduction to DHCP.....                                 | 4-2        |
| 4.1.2 DHCP Supported by the S-switch.....                       | 4-2        |
| 4.1.3 Update History.....                                       | 4-2        |
| 4.2 Configuring the Global Address Pool-based DHCP Server.....  | 4-2        |
| 4.2.1 Establishing the Configuration Task.....                  | 4-3        |
| 4.2.2 Configuring the DHCP Global Address Pool.....             | 4-3        |
| 4.2.3 Configure Static IP Address Binding.....                  | 4-4        |
| 4.2.4 Configuring DNS Services for the DHCP Client.....         | 4-5        |
| 4.2.5 Configuring NetBIOS Services for the DHCP Client.....     | 4-6        |
| 4.2.6 Configuring Egress Gateway for the DHCP Client.....       | 4-7        |
| 4.2.7 Configuring DHCP Self-Defined Options.....                | 4-7        |

|   |            |
|---|------------|
| 4.2.8 Assigning IP Addresses in the Global Address Pool to the DHCP Clients on the Specified Interface..... | 4-8        |
| 4.2.9 Checking the Configuration.....   | 4-9        |
| 4.3 Configuring VLANIF Interface Address Pool-based DHCP Server.....  | 4-11       |
| 4.3.1 Establishing the Configuration Task.....  | 4-11       |
| 4.3.2 Enabling Address Pools on VLANIF Interfaces.....  | 4-12       |
| 4.3.3 Configuring the Address Pool on the VLANIF Interface.....   | 4-13       |
| 4.3.4 Configuring DNS on the Address Pool of the VLANIF Interface.....                                      | 4-14       |
| 4.3.5 Configuring NetBIOS on the Address Pool of the VLANIF Interface.....                                  | 4-15       |
| 4.3.6 Configuring DHCP Self-Defined Options for the Address Pool of the VLANIF Interface.....               | 4-16       |
| 4.3.7 Checking the Configuration.....   | 4-17       |
| 4.4 Configuring the Security Function for DHCP.....   | 4-18       |
| 4.4.1 Establishing the Configuration Task.....  | 4-18       |
| 4.4.2 Starting the Detection of the Pseudo DHCP Server on a DHCP Server.....                                | 4-19       |
| 4.4.3 Avoiding Repetitive IP Address Assignment.....  | 4-19       |
| 4.4.4 Saving DHCP Data.....   | 4-20       |
| 4.4.5 Recovering DHCP Data.....   | 4-20       |
| 4.4.6 Checking the Configuration.....   | 4-21       |
| 4.5 Configuring DHCP Relay.....   | 4-21       |
| 4.5.1 Establishing the Configuration Task.....  | 4-22       |
| 4.5.2 Enabling DHCP Relay.....  | 4-22       |
| 4.5.3 Assigning IP Addresses to the Client Through Relay.....   | 4-23       |
| 4.5.4 Requesting the DHCP Server to Release IP Addresses of the Client.....                                 | 4-24       |
| 4.5.5 Checking the Configuration.....   | 4-25       |
| 4.6 Maintaining DHCP.....   | 4-25       |
| 4.6.1 Resetting DHCP.....   | 4-26       |
| 4.6.2 Releasing Conflicting IP Addresses.....   | 4-26       |
| 4.6.3 Clearing DHCP Statistics.....   | 4-26       |
| 4.6.4 Monitoring Network Operation Status.....  | 4-27       |
| 4.6.5 Debugging DHCP.....   | 4-27       |
| 4.7 Configuration Examples.....   | 4-28       |
| 4.7.1 Example for Configuring the Global Address Pool-based DHCP Server.....                                | 4-28       |
| 4.7.2 Example for Configuring the VLANIF Interface Address Pool-based DHCP Server.....                      | 4-31       |
| 4.7.3 Example for Configuring DHCP Relay.....   | 4-34       |
| <b>5 IP Performance Configuration.....</b>  | <b>5-1</b> |
| 5.1 Overview.....   | 5-2        |
| 5.1.1 Introduction to IP Performance.....   | 5-2        |
| 5.1.2 IP Performance Supported by the S-switch.....   | 5-2        |
| 5.1.3 Update History.....   | 5-3        |
| 5.2 Improving IP Performance.....   | 5-3        |
| 5.2.1 Establishing the Configuration Task.....  | 5-3        |
| 5.2.2 Verifying the Source IP Address.....  | 5-4        |

|   |            |
|---|------------|
| 5.2.3 Forwarding Broadcast Packets.....                                       | 5-4        |
| 5.2.4 Configuring ICMP Attributes.....  | 5-5        |
| 5.2.5 Configuring TCP Attributes.....   | 5-6        |
| 5.2.6 Checking the Configuration.....   | 5-6        |
| 5.3 Maintaining IP Performance.....   | 5-10       |
| 5.3.1 Clearing IP/TCP/UDP Statistics.....                                     | 5-10       |
| 5.3.2 Monitoring Network Operation Status.....                                | 5-10       |
| 5.3.3 Debugging IP/TCP/UDP.....   | 5-12       |
| 5.4 Configuration Examples.....   | 5-13       |
| 5.4.1 Example for Limiting Transmission of ICMP Host-Unreachable Packets..... | 5-13       |
| <b>6 ACL Configuration.....</b>   | <b>6-1</b> |
| 6.1 Overview.....   | 6-2        |
| 6.1.1 Introduction to ACL.....  | 6-2        |
| 6.1.2 ACL Supported by the S-switch.....                                      | 6-2        |
| 6.1.3 Update History.....   | 6-2        |
| 6.2 Configuring an ACL.....   | 6-2        |
| 6.2.1 Establishing the Configuration Task.....                                | 6-3        |
| 6.2.2 Creating a Time Range.....  | 6-3        |
| 6.2.3 Configuring ACL Descriptions.....                                       | 6-4        |
| 6.2.4 Configuring a Basic ACL.....  | 6-4        |
| 6.2.5 Configuring an Advanced ACL.....  | 6-5        |
| 6.2.6 Configuring ACL Step.....   | 6-6        |
| 6.2.7 Checking the Configuration.....   | 6-6        |
| 6.3 Maintaining an ACL.....   | 6-7        |
| 6.3.1 Clearing Statistics.....  | 6-7        |
| 6.3.2 Monitoring Network Operation Status.....                                | 6-7        |
| 6.4 Configuration Examples.....   | 6-7        |
| 6.4.1 Example for Configuring an ACL.....                                     | 6-7        |
| <b>7 DHCP Policy VLAN Configuration.....</b>                                  | <b>7-1</b> |
| 7.1 Overview.....   | 7-2        |
| 7.1.1 Introduction.....   | 7-2        |
| 7.1.2 DHCP Policy VLAN Supported by the S-switch.....                         | 7-2        |
| 7.1.3 Update History.....   | 7-2        |
| 7.2 Configuring DHCP Policy VLAN Based on MAC Addresses.....                  | 7-2        |
| 7.2.1 Establishing the Configuration Task.....                                | 7-2        |
| 7.2.2 Configuration Procedure.....  | 7-3        |
| 7.2.3 Checking the Configuration.....   | 7-4        |
| 7.3 Configuring the DHCP Policy VLAN Based on Interfaces.....                 | 7-4        |
| 7.3.1 Establishing the Configuration Task.....                                | 7-4        |
| 7.3.2 Configuration Procedure.....  | 7-5        |
| 7.3.3 Checking the Configuration.....   | 7-5        |
| 7.4 Configuring Generic DHCP Policy VLAN.....                                 | 7-6        |

|  |      |
|--|------|
| 7.4.1 Establishing the Configuration Task.....                             | 7-6  |
| 7.4.2 Configuration Procedure.....   | 7-6  |
| 7.4.3 Checking the Configuration.....                                      | 7-7  |
| 7.5 Maintaining DHCP Policy VLAN.....                                      | 7-7  |
| 7.5.1 Monitoring the Running Status.....                                   | 7-8  |
| 7.6 Configuration Examples.....  | 7-8  |
| 7.6.1 Example for Configuring DHCP Policy VLAN Based on MAC Addresses..... | 7-8  |
| 7.6.2 Example for Configuring DHCP Policy VLAN Based on Interfaces.....    | 7-10 |



---

## Figures

---

|   |      |
|---|------|
| <b>Figure 1-1</b> Configuring primary and secondary IP addresses for a VLANIF interface.....                    | 1-6  |
| <b>Figure 2-1</b> Networking diagram for configuring static ARP.....  | 2-13 |
| <b>Figure 2-2</b> Networking diagram for configuring dynamic ARP.....   | 2-15 |
| <b>Figure 2-3</b> Networking diagram of configuring proxy ARP.....  | 2-16 |
| <b>Figure 2-4</b> Networking diagram of configuring proxy ARP between VLANs.....                                | 2-18 |
| <b>Figure 3-1</b> Networking diagram of DNS.....  | 3-7  |
| <b>Figure 4-1</b> Networking diagram of the DHCP server and the client that are in the same network segment.... | 4-29 |
| <b>Figure 4-2</b> Networking diagram of the DHCP server based on the address pool on the VLANIF interface....   | 4-32 |
| <b>Figure 4-3</b> Networking diagram for configuring DHCP relay.....  | 4-35 |
| <b>Figure 5-1</b> Networking diagram of configuring ICMP host unreachable packets.....                          | 5-13 |
| <b>Figure 7-1</b> Networking for configuring DHCP policy VLAN based on MAC addresses.....                       | 7-8  |
| <b>Figure 7-2</b> Networking for configuring DHCP policy VLAN based on interfaces.....                          | 7-10 |



---

# About This Document

---

## Purpose

This document provides configuration procedures and examples for the IP Service features of the S-switch.

This document covers the following topics:

- Feature description
- Data preparations
- Pre-configuration tasks
- Configuration procedures
- Checking the configuration
- Configuration examples

This document helps you grasp the configuration procedures and application scenarios of the IP Service features of the S-switch.

## Related Versions

The following table lists the product versions related to this document.

| Product Name | Version     |
|--------------|-------------|
| S5300        | V100R002C02 |

## Intended Audience

This document is intended for:

- Commissioning engineers
- Data configuration engineers
- Network administrators
- System maintenance engineers

# Organization






This document is organized as follows.

| Chapter                                 | Description   |
|---|---|
| <b>1 IP Addresses Configuration</b>     | This chapter describes the basics, methods and examples for configuring IP Address.       |
| <b>2 ARP Configuration</b>              | This chapter describes the basics, methods and examples for configuring ARP.              |
| <b>3 DNS Configuration</b>              | This chapter describes the basics, methods and examples for configuring DNS.              |
| <b>4 DHCP Configuration</b>             | This chapter describes the basics, methods and examples for configuring DHCP.             |
| <b>5 IP Performance Configuration</b>   | This chapter describes the basics, methods and examples for configuring IP performance.   |
| <b>6 ACL Configuration</b>              | This chapter describes the basics, methods and examples for configuring ACL.              |
| <b>7 DHCP Policy VLAN Configuration</b> | This chapter describes the basics, methods and examples for configuring DHCP policy VLAN. |

# Conventions

## Symbol Conventions

The symbols that may be found in this document are defined as follows.

| Symbol   | Description   |
|--|---|
|  <b>DANGER</b>  | Indicates a hazard with a high level of risk, which if not avoided, will result in death or serious injury.   |
|  <b>WARNING</b> | Indicates a hazard with a medium or low level of risk, which if not avoided, could result in minor or moderate injuries.  |
|  <b>CAUTION</b> | Indicates a potentially hazardous situation, which if not avoided, could result in equipment damage, data loss, performance degradation, or unexpected results. |
|  <b>TIP</b>     | Indicates a tip that may help you address a problem or save your time.  |
|  <b>NOTE</b>    | Provides additional information to emphasize or supplement important points of the main text.   |

## General Conventions

| Convention      | Description  |
|-----------------|--|
| Times New Roman | Normal paragraphs are in Times New Roman.  |
| <b>Boldface</b> | Names of files, directories, folders, and users are in <b>Boldface</b> . For example, log in as user <b>Root</b> . |
| <i>Italic</i>   | Book titles are in <i>Italics</i> .  |
| Courier New     | Examples of information displayed on the screen are in Courier New.  |

## Command Conventions

| Convention        | Description   |
|-------------------|---|
| <b>Boldface</b>   | The keywords of a command line are in <b>boldface</b> .   |
| <i>Italic</i>     | Command arguments are in <i>italics</i> .   |
| [ ]               | Items (keywords or arguments) in brackets [ ] are optional.   |
| { x   y   ... }   | Alternative items are grouped in braces and separated by vertical bars. One is selected.  |
| [ x   y   ... ]   | Optional alternative items are grouped in square brackets and separated by vertical bars. One or none is selected.                    |
| { x   y   ... } * | Optional items are grouped in braces and separated by vertical bars. A minimum of one item or a maximum of all items can be selected. |
| [ x   y   ... ] * | Optional alternative items are grouped in square brackets and separated by vertical bars. Several or none is selected.                |
| &<1-n>            | The parameter before the & sign can be repeated 1 to n times.   |
| #                 | A line starting with the # sign is comments.  |

## GUI Conventions

| Convention      | Description  |
|-----------------|--|
| <b>boldface</b> | Buttons, menus, parameters, tabs, windows, and dialog titles are in <b>boldface</b> . For example, click <b>OK</b> .               |
| >               | Multi-level menus are in <b>boldface</b> and separated by the ">" signs. For example, choose <b>File &gt; Create &gt; Folder</b> . |

## Keyboard Operations

| Convention          | Description   |
|---------------------|---|
| <b>Key</b>          | Press the key. For example, press <b>Enter</b> and press <b>Tab</b> .   |
| <b>Key 1+Key 2</b>  | Press the keys concurrently. For example, pressing <b>Ctrl+Alt+A</b> means the three keys should be pressed concurrently. |
| <b>Key 1, Key 2</b> | Press the keys in turn. For example, pressing <b>Alt, F</b> means the two keys should be pressed in turn.                 |

## Mouse Operations

| Convention   | Description   |
|--------------|---|
| Click        | Select and release the primary mouse button without moving the pointer.                   |
| Double-click | Press the primary mouse button twice continuously and quickly without moving the pointer. |
| Drag         | Press and hold the primary mouse button and move the pointer to a certain position.       |

## Update History

Updates between document issues are cumulative. Therefore, the latest document version contains all updates made to previous versions.

### Updates in Issue 02 (2009-02-16)

Second commercial release. The document is updated as follows:

- Fixing bug
- Rewriting copyright statement
- Updating manual version

### Updates in Issue 01 (2008-12-16)

This is the first release.

# 1 IP Addresses Configuration

---

## About This Chapter

This chapter describes the fundamentals of IP address, including its classes, methods and important characteristics. It also describes the steps for IP address configuration, along with typical examples.

### [1.1 Overview](#)

This section describes the principle and concepts of the IP address.

### [1.2 Configuring IP Addresses for Interfaces](#)

This section describes how to configure IP addresses for interfaces.

### [1.3 Maintaining](#)

This section describes how to view configurations about IP addresses.

### [1.4 Configuration Examples](#)

This section provides several configuration examples of IP addresses.

## 1.1 Overview

This section describes the principle and concepts of the IP address.

### [1.1.1 Introduction to IP Addresses](#)

### [1.1.2 Features of IP Addresses Supported by the S-switch](#)

### [1.1.3 Update History](#)

## 1.1.1 Introduction to IP Addresses

To communicate with each other in an IP network, each host in the network must be assigned an IP address.

An IP address is a 32-bit number, composed of two parts, network ID and host ID.

The network ID identifies a network and the host ID identifies a host on the network. If the network IDs of hosts are the same, it indicates that the hosts are in the same network regardless of their physical location.

## 1.1.2 Features of IP Addresses Supported by the S-switch

The S-switch supports IP address configuration through the following methods:

- Manually configuring an IP address for an interface
- Get IP address by DHCP

## 1.1.3 Update History

| Version         | Revision                   |
|-----------------|----------------------------|
| V100R002C01B050 | This is the first release. |

## 1.2 Configuring IP Addresses for Interfaces

This section describes how to configure IP addresses for interfaces.

### [1.2.1 Establishing the Configuration Task](#)

### [1.2.2 Configuring a Primary IP Address for an VLAN Interface](#)

### [1.2.3 \(Optional\) Configuring a Secondary IP Address for an VLANIF Interface](#)

### [1.2.4 Checking the Configuration](#)

## 1.2.1 Establishing the Configuration Task

## Applicable Environment

To start the IP services on S-switch, configure the IP address on the VLANIF interface. You can assign several IP addresses to each interface. Among them, one is the primary IP address and the others are secondary IP addresses.

## Pre-configuration Tasks

Before configuring an IP address for an VLANIF interface, complete the following tasks:

- Configuring the physical parameters for the interface and ensuring that the status of the physical layer of the interface is Up
- Configuring the link layer parameters for the interface and ensuring that the status of the link layer protocol on the interface is Up
- Configuring the corresponding VLAN

## Data Preparation

To configure IP addresses for an VLANIF interface, you need the following data.

| No. | Data   |
|-----|--|
| 1   | VLANIF interface number  |
| 2   | Primary IP address and subnet mask for the VLANIF interface              |
| 3   | (Optional) Secondary IP address and subnet mask for the VLANIF interface |

Subordinate IP addresses are required when an VLANIF interface needs multiple addresses.

## 1.2.2 Configuring a Primary IP Address for an VLAN Interface

### Context

Do as follows on the S-switch:

### Procedure

**Step 1** Run:

```
system-view
```

The system view is displayed.

**Step 2** Run:

```
interface vlanif vlan interface number
```

The VLANIF interface view is displayed.

**Step 3** Run:

```
ip address ip-address { mask | mask-length }
```

Or

```
ip address dhcp-alloc
```

A primary IP address is configured.

An VLANIF interface has only one primary IP address. If the VLANIF interface already has a primary IP address, the newly configured primary IP address replaces the original one.

----End

## 1.2.3 (Optional) Configuring a Secondary IP Address for an VLANIF Interface

### Context

Do as follows on the S-switch:

### Procedure

**Step 1** Run:

```
system-view
```

The system view is displayed.

**Step 2** Run:

```
interface vlanif vlan interface number
```

The VLANIF interface view is displayed.

**Step 3** Run:

```
ip address ip-address { mask | mask-length } sub
```

A secondary IP address is configured.

----End

## 1.2.4 Checking the Configuration

Run the following commands to check the pervious configuration.

| Action                                      | Command   |
|---|---|
| View the IP configuration on the interface. | <b>display ip interface</b> [ <b>brief</b> ] [ <i>interface-type interface-number</i> ]   |
| View interface information.                 | <b>display interface</b> [ <i>interface-type</i> [ <i>interface-number</i> ] ] [   { <b>begin</b>   <b>exclude</b>   <b>include</b> } <i>regular-expression</i> ] |

Run the **display ip interface** command. If the physical status and link protocol status of the interface are Up, it means that the configuration succeeds.

Run the **display interface** command. If information about the IP address and mask of the interface is displayed, it means that the configuration succeeds. For example:

```
<Quidway> display ip interface brief vlanif 1
*down: administratively down
(l): loopback
(s): spoofing
```

```

Interface                IP Address      Physical  Protocol
Vlanif1                  192.168.32.22  up       up
<Quidway> display interface vlanif 1
Vlanif1 current state : UP
Line protocol current state : UP
Description : Huawei, Quidway Series, Vlanif1 Interface, Route Port
The Maximum Transmit Unit is 1500 bytes
Internet Address is 192.168.32.22/16
IP Sending Frames' Format is PKTFMT_ETHNT_2, Hardware address is 0010-8300-0026

```

## 1.3 Maintaining

This section describes how to view configurations about IP addresses.

### 1.3.1 Monitoring Network Operation Status

#### 1.3.1 Monitoring Network Operation Status

To obtain configurations about IP addresses in routine maintenance, run the following commands.

| Action   | Command   |
|--|---|
| View configurations about the IP address of the interface. | <b>display ip interface</b> [ <b>brief</b> ] [ <i>interface-type interface-number</i> ]   |
| View information about the interface.                      | <b>display interface</b> [ <i>interface-type</i> [ <i>interface-number</i> ] ] [   { <b>begin</b>   <b>exclude</b>   <b>include</b> } <i>regular-expression</i> ] |

## 1.4 Configuration Examples

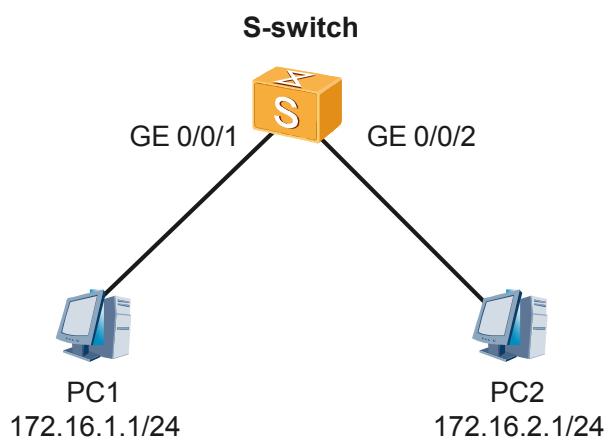
This section provides several configuration examples of IP addresses.

### 1.4.1 Example for Configuring Primary and Secondary IP Addresses

#### 1.4.1 Example for Configuring Primary and Secondary IP Addresses

##### Networking Requirements

As shown in [Figure 1-1](#), GigabitEthernet 0/0/1 and GigabitEthernet 0/0/2 of the S-switch are connected to two PCs and added to VLAN 1. The IP addresses of PC1 and PC2 are 172.16.1.1/24 and 172.16.2.1/24.

**Figure 1-1** Configuring primary and secondary IP addresses for a VLANIF interface

## Configuration Roadmap

The configuration roadmap is as follows:

1. Analyze the network segment where the interface locates.
2. Configure a primary IP address for the VLANIF interface and then configure a secondary IP address for the interface.

## Data Preparation

To complete the configuration, you need the following data:

- Primary IP address and subnet mask of the VLANIF interface
- Secondary IP address and subnet mask of the VLANIF interface

## Configuration Procedure

If you assign only one IP address to the VLANIF interface on the S-switch, you can access certain hosts through the S-switch. To access all the hosts in the network through the S-switch, you need to assign a secondary IP address to the VLANIF interface.

1. Add GigabitEthernet 0/0/1 and GigabitEthernet 0/0/2 of the S-switch to VLAN 1.
2. Configure the device.

# Configure the primary and secondary IP addresses for VLANIF 1 of the device.

```
<Quidway> system-view
[Quidway] interface vlanif 1
[Quidway-Vlanif1] ip address 172.16.1.2 255.255.255.0
[Quidway-Vlanif1] ip address 172.16.2.2 255.255.255.0 sub
```

3. Verify the configuration.

# Ping the host PC1 from the device. The ping succeeds.

```
[Quidway] ping 172.16.1.1
PING 172.16.1.1: 56 data bytes, press CTRL_C to break
Reply from 172.16.1.2: bytes=56 Sequence=1 ttl=128 time=25 ms
Reply from 172.16.1.2: bytes=56 Sequence=2 ttl=128 time=27 ms
Reply from 172.16.1.2: bytes=56 Sequence=3 ttl=128 time=26 ms
Reply from 172.16.1.2: bytes=56 Sequence=4 ttl=128 time=26 ms
```

```
Reply from 172.16.1.2: bytes=56 Sequence=5 ttl=128 time=26 ms
--- 172.16.1.1 ping statistics ---
 5 packet(s) transmitted
 5 packet(s) received
 0.00% packet loss
round-trip min/avg/max = 25/26/27 ms
```

# Ping the host PC2 from the device. The ping succeeds.

```
[Quidway] ping 172.16.2.1
PING 172.16.2.1: 56 data bytes, press CTRL_C to break
Reply from 172.16.2.2: bytes=56 Sequence=1 ttl=128 time=25 ms
Reply from 172.16.2.2: bytes=56 Sequence=2 ttl=128 time=26 ms
Reply from 172.16.2.2: bytes=56 Sequence=3 ttl=128 time=26 ms
Reply from 172.16.2.2: bytes=56 Sequence=4 ttl=128 time=26 ms
Reply from 172.16.2.2: bytes=56 Sequence=5 ttl=128 time=26 ms
--- 172.16.2.1 ping statistics ---
 5 packet(s) transmitted
 5 packet(s) received
 0.00% packet loss
round-trip min/avg/max = 25/25/26 ms
```

# The hosts PC1 and PC2 cannot ping each other.

## Configuration Files

The configuration file of the device is as follows:

```
#
interface Vlanif1
 ip address 172.16.1.2 255.255.255.0
 ip address 172.16.2.2 255.255.255.0 sub
#
return
```



# 2 ARP Configuration

---

## About This Chapter

This chapter describes the static and dynamic ARP, ARP proxy concepts and their configuration steps, along with typical examples.

### [2.1 Overview](#)

This section describes the basic principle and concepts of the Address Resolution Protocol (ARP).

### [2.2 Configuring ARP](#)

This section describes how to configure static ARP, and dynamic ARP.

### [2.3 Configuring Proxy ARP](#)

This section describes how to configure routed proxy ARP to make different sub-networks communicate with each other.

### [2.4 Configuring Proxy ARP Between VLANs](#)

This section describes how to implement communication between hosts in different VLANs.

### [2.5 Maintaining ARP](#)

This section describes how to display ARP configurations, clear ARP statistics and debug ARP.

### [2.6 Configuration Examples](#)

This section provides several configuration examples of ARP, proxy ARP in a VLAN, and proxy ARP between VLANs.

## 2.1 Overview

This section describes the basic principle and concepts of the Address Resolution Protocol (ARP).

### [2.1.1 Introduction to ARP](#)

### [2.1.2 Features of ARP Supported by the S-switch](#)

### [2.1.3 Update History](#)

## 2.1.1 Introduction to ARP

Each host or device in the Local Area Network (LAN) has a 32-bit IP address to communicate with others. In an Ethernet, a host or a device transmits Ethernet frames based on 48-bit Medium Access Control (MAC) addresses. A MAC address is also called physical address or hardware address. It is assigned to an Ethernet interface when a device is produced. IP addresses are independent of hardware addresses. Therefore, mappings between MAC addresses and IP addresses must be created through a certain address resolution mechanism.

The Address Resolution Protocol (ARP) emerges. It provides a mapping between an IP address and a MAC address.

## 2.1.2 Features of ARP Supported by the S-switch

ARP is classified into dynamic ARP and static ARP. The S-switch supports the dynamic ARP, static ARP, and proxy ARP.

## 2.1.3 Update History

| Version         | Revision                   |
|-----------------|----------------------------|
| V100R002C01B050 | This is the first release. |

## 2.2 Configuring ARP

This section describes how to configure static ARP, and dynamic ARP.

### [2.2.1 Establishing the Configuration Task](#)

### [2.2.2 Configuring Static ARP Entries](#)

### [2.2.3 Optimizing Dynamic ARP](#)

### [2.2.4 Checking the Configuration](#)

## 2.2.1 Establishing the Configuration Task

## Applicable Environment

Dynamic ARP is one of functions owned by a device or host. To enable this function, you modify some parameters of dynamic ARP actions instead of running the related command.

Static ARP is used in the following situations:

- The packets whose destination IP address is in another network segment traverse a gateway of the segment so that the gateway can forward the packets to their destination.
- When users need to filter out some packets with illegal destination IP addresses, static ARP can bind these illegal addresses to a nonexistent MAC address.

## Pre-configuration Tasks

Before configuring ARP, complete the following tasks:

- Configuring the physical parameters for the interface and ensuring that the status of the physical layer of the interface is Up
- Configuring the link layer parameters for the interface and ensuring that the status of the link layer protocol on the interface is Up
- Configuring the network layer parameters for the interface

## Data Preparation

To configure ARP, you need the following data.

| No. | Data  |
|-----|---|
| 1   | IP address and MAC address of the static ARP entry                |
| 2   | ID of the VLANIF interface to which the dynamic ARP entry belongs |
| 3   | Aging detection times of the dynamic ARP entry                    |
| 4   | Aging time of the dynamic ARP entry                               |

## 2.2.2 Configuring Static ARP Entries

### Context

Do as follows on the S-switch:

### Procedure

**Step 1** Run:

```
system-view
```

The system view is displayed.

**Step 2** Perform the following as required to add static ARP entries:

- To configure common static ARP entries, run the **arp static ip-address mac-address** command.

- To configure static ARP entries in a Virtual Local Area Network (VLAN), do as follows:
  - Run the **arp static** *ip-address mac-address vid vlan-id interface interface-type interface-number* command.
  - Run the **arp static** *ip-address mac-address [ vpn-instance vpn-instance-name ] vid vlan-id* command.  
  
This command is applied to the sub-interface that supports VLAN and can be bound to the VPN.
- To configure static ARP entries in a VPN instance, run the **arp static** *ip-address mac-address vpn-instance vpn-instance-name* command.

**NOTE**

Static ARP entries keep valid when a device works normally.

----End

## 2.2.3 Optimizing Dynamic ARP

### Context

Do as follows on the S-switch:

### Procedure

**Step 1** Run:

```
system-view
```

The system view is displayed.

**Step 2** Run:

```
interface vlanif vlan interface number
```

The VLAN interface view is displayed.

**Step 3** Run:

```
arp detect-times detect-times
```

The aging detection times of the dynamic ARP entries are configured.

**Step 4** Run:

```
arp expire-time expire-times
```

The timeout period for aging dynamic ARP entries is configured.

**Step 5** Run:

```
quit
```

Back to the system view.

**Step 6** Run:

```
arp-suppress enable
```

ARP suppression is enabled on the current device.

----End

## 2.2.4 Checking the Configuration

Run the following commands to check the pervious configuration.

| Action   | Command  |
|--|--|
| View information about ARP mapping tables based on interfaces. | <b>display arp interface</b> <i>interface-type interface-number</i> [   { <b>begin</b>   <b>exclude</b>   <b>include</b> } <i>regular-expression</i> ] |
| View statistics about ARP entries.                             | <b>display arp statistics</b>  |

Run the **display arp interface** command. If all the ARP entries of the interface are displayed, it means that the configuration succeeds. For example:

```
<Quidway> display arp interface vlanif 1
IP ADDRESS      MAC ADDRESS    EXPIRE (M)  TYPE  INTERFACE      VPN-INSTANCE
                                VLAN
-----
192.168.32.22    0010-8300-0026      I -   Vlanif1
192.168.1.255    Incomplete        0     D-0   Vlanif1
192.168.29.1     000e-4540-04b7     5     DF0   GE0/0/24
192.168.29.3     e000-0af0-e492     7     DF0   GE0/0/24
192.168.29.7     e000-0af0-cb68     7     DF0   GE0/0/24
192.168.29.2     e000-0af0-e497     7     DF0   GE0/0/24
192.168.29.4     e000-0af0-e090     7     DF0   GE0/0/24
192.168.29.6     e000-0af0-cb67     7     DF0   GE0/0/24
192.168.1.239    0018-8236-f110     9     DF0   GE0/0/24
192.168.1.232    0200-000a-1d34    10     DF0   GE0/0/24
192.168.1.220    0018-8261-2507    11     DF0   GE0/0/24
192.168.31.99    0019-21df-dd7c    17     DF0   GE0/0/24
192.168.32.171    0019-e00a-a8fc    17     DF0   GE0/0/24
192.168.31.181    001e-9089-c65a    17     DF0   GE0/0/24
192.168.31.253    000d-88f7-5fee    19     DF0   GE0/0/24
192.168.29.126    e000-0af0-cbba    19     DF0   GE0/0/24
192.168.1.145    0200-0016-0319    19     DF0   GE0/0/24
192.168.3.169    0018-8261-652c    20     DF0   GE0/0/24
192.168.1.143    0200-0016-0331    20     DF0   GE0/0/24
192.168.225.2     4e74-6300-0422    20     DF0   GE0/0/24
192.168.32.108    0018-8241-e376    20     DF0   GE0/0/24
-----
Total:21          Dynamic:20          Static:0          Interface:1
```

Run the **display arp statistics** command. If statistics about ARP entries are displayed, it means that the configuration succeeds. For example:

```
<Quidway> display arp statistics
Total:27      Dynamic:20      Static:0      Interface:7
```

## 2.3 Configuring Proxy ARP

This section describes how to configure routed proxy ARP to make different sub-networks communicate with each other.

### [2.3.1 Establishing the Configuration Task](#)

### [2.3.2 Configuring an IP Addresses for the VLANIF Interface](#)

### [2.3.3 Enabling Proxy ARP Function](#)

### [2.3.4 Checking the Configuration](#)

## 2.3.1 Establishing the Configuration Task

### Applicable Environment

When two hosts are located in different network segments without gateways configured, you can use the **arp-proxy enable** command to enable proxy ARP on the S-switch connecting these hosts. In this manner, IP addresses between these two hosts can be resolved through the S-switch.

### Pre-configuration Tasks

Before configuring proxy ARP, complete the following tasks:

- Configuring the physical parameters for the interface and ensuring that the status of the physical layer of the interface is Up
- Configuring the link layer parameters for the interface and ensuring that the status of the link layer protocol on the interface is Up

### Data Preparation

To configure proxy ARP, you need the following data.

| No. | Data  |
|-----|---|
| 1   | Number of the VLANIF interface enabled with proxy ARP     |
| 2   | IP address of the VLANIF interface enabled with proxy ARP |

## 2.3.2 Configuring an IP Addresses for the VLANIF Interface

### Context

Do as follows on the S-switch:

## Procedure

- Step 1** Run:  
`system-view`  
The system view is displayed.
- Step 2** Run:  
`interface vlanif vlan interface number`  
The VLANIF interface view is displayed.
- Step 3** Run:  
`ip address ip-address { mask | mask-length }`  
The VLANIF interface is configured with an IP address.
- End

## 2.3.3 Enabling Proxy ARP Function

### Context

Do as follows on the S-switch:

## Procedure

- Step 1** Run:  
`system-view`  
The system view is displayed.
- Step 2** Run:  
`interface interface-type interface-number`  
The VLANIF interface view is displayed.
- Step 3** Run:  
`arp-proxy enable`  
The proxy ARP function is enabled on the VLANIF interface.
- End

## 2.3.4 Checking the Configuration

Run the following commands to check the pervious configuration.

| Action   | Command   |
|--|---|
| View information about ARP mapping tables based on interfaces. | <code>display arp interface interface-type interface-number [ { begin   exclude   include } regular-expression ]</code> |
| View statistics about ARP entries.                             | <code>display arp statistics</code>   |

Run the **display arp interface** command. If all the ARP entries of the VLANIF interface are displayed, it means that the configuration succeeds. For example:

```
<Quidway> display arp interface vlanif 1
```

| IP ADDRESS      | MAC ADDRESS    | EXPIRE (M) | TYPE        | INTERFACE<br>VLAN | VPN-INSTANCE |
|-----------------|----------------|------------|-------------|-------------------|--------------|
| 192.168.32.11   | 0001-0168-0182 |            | I -         | Vlanif1           |              |
| 1.1.1.1         | 0001-0168-0182 |            | I -         | Vlanif1           |              |
| 192.168.6.255   | Incomplete     | 0          | D-0         | Vlanif1           |              |
| 192.168.1.255   | Incomplete     | 0          | D-0         | Vlanif1           |              |
| 192.168.29.255  | Incomplete     | 1          | D-0         | Vlanif1           |              |
| 192.168.6.10    | 0200-0010-0232 | 5          | DF0         | GE0/0/24          |              |
|                 |                |            | 1           |                   |              |
| 192.168.3.181   | 0018-8236-f110 | 6          | DF0         | GE0/0/24          |              |
|                 |                |            | 1           |                   |              |
| 192.168.3.182   | 0200-000b-3517 | 6          | DF0         | GE0/0/24          |              |
|                 |                |            | 1           |                   |              |
| 192.168.6.6     | 0018-8238-9212 | 6          | DF0         | GE0/0/24          |              |
|                 |                |            | 1           |                   |              |
| 192.168.3.240   | 0018-8261-2503 | 7          | DF0         | GE0/0/24          |              |
|                 |                |            | 1           |                   |              |
| 192.168.1.124   | 00e0-4c77-deff | 14         | DF0         | GE0/0/24          |              |
|                 |                |            | 1           |                   |              |
| 192.168.4.131   | 00e0-4c77-826b | 15         | DF0         | GE0/0/24          |              |
|                 |                |            | 1           |                   |              |
| 192.168.31.180  | 00e0-4c83-aae8 | 16         | DF0         | GE0/0/24          |              |
|                 |                |            | 1           |                   |              |
| 192.168.31.181  | 001e-9089-c65a | 18         | DF0         | GE0/0/24          |              |
|                 |                |            | 1           |                   |              |
| 192.168.81.13   | 00e0-4c77-b2cf | 18         | DF0         | GE0/0/24          |              |
|                 |                |            | 1           |                   |              |
| 192.168.216.99  | 00e0-4c77-7219 | 18         | DF0         | GE0/0/24          |              |
|                 |                |            | 1           |                   |              |
| 192.168.229.142 | 0018-8253-21cf | 19         | DF0         | GE0/0/24          |              |
|                 |                |            | 1           |                   |              |
| 192.168.3.169   | 0018-8261-652c | 20         | DF0         | GE0/0/24          |              |
|                 |                |            | 1           |                   |              |
| 192.168.100.55  | 0018-8252-3335 | 20         | DF0         | GE0/0/24          |              |
|                 |                |            | 1           |                   |              |
| 192.168.3.179   | 0200-0012-1534 | 20         | DF0         | GE0/0/24          |              |
|                 |                |            | 1           |                   |              |
| 192.168.225.2   | 4e74-6300-0422 | 20         | DF0         | GE0/0/24          |              |
|                 |                |            | 1           |                   |              |
| -----           |                |            |             |                   |              |
| Total:21        | Dynamic:19     | Static:0   | Interface:2 |                   |              |

Run the **display arp statistics** command. If statistics about ARP entries are displayed, it means that the configuration succeeds. For example:

```
<Quidway> display arp statistics
```

|          |            |          |             |
|----------|------------|----------|-------------|
| Total:27 | Dynamic:21 | Static:0 | Interface:6 |
|----------|------------|----------|-------------|

## 2.4 Configuring Proxy ARP Between VLANs

This section describes how to implement communication between hosts in different VLANs.

### 2.4.1 Establishing the Configuration Task

### 2.4.2 Configuring an IP Addresses for the VLANIF Interface

### 2.4.3 Enabling Proxy ARP Between VLANs

### 2.4.4 Checking the Configuration

## 2.4.1 Establishing the Configuration Task

### Applicable Environment

If two users belong to different VLANs and they need to communicate, you need to enable proxy ARP between VLANs on the sub-interface associated with the VLAN.

Sub-VLANs in a super-VLAN cannot communicate with each other. To solve this problem, enable proxy ARP between VLANs on the VLANIF interface corresponding to the super-VLAN.

Implementing communication between VLANs through proxy ARP occupies fewer resources than through configuring a VLANIF interface for each sub-VLAN.

IP addresses of hosts in a VLAN must be in the same network segment.

### Pre-configuration Tasks

Before configuring proxy ARP between VLANs, complete the following tasks:

- Configuring physical attributes for the interface and ensuring that the status of the physical layer of the interface is Up
- Configuring VLAN aggregation

### Data Preparation

To configure proxy ARP between VLANs, you need the following data.

| No. | Data  |
|-----|---|
| 1   | Number of the VLANIF interface to be enabled with proxy ARP between VLANs               |
| 2   | IP address of the VLANIF interface to be enabled with proxy ARP between VLANs           |
| 3   | VLAN ID associated with the VLANIF interface to be enabled with proxy ARP between VLANs |

## 2.4.2 Configuring an IP Addresses for the VLANIF Interface

### Context

Do as follows on the S-switch:

### Procedure

**Step 1** Run:

```
system-view
```

The system view is displayed.

**Step 2** Run:

```
interface vlanif vlan interface number
```

The VLANIF interface view is displayed.

**Step 3** Run:

```
ip address ip-address { mask | mask-length }
```

The VLANIF interface is configured with an IP address.

The IP address configured for the VLANIF interface must be in the same network segment with that of hosts in the VLAN associated with this interface.

----End

## 2.4.3 Enabling Proxy ARP Between VLANs

### Context

Do as follows on the S-switch:

### Procedure

**Step 1** Run:

```
system-view
```

The system view is displayed.

**Step 2** Run:

```
interface vlanif vlan interface number
```

The VLANIF interface view is displayed.

**Step 3** Run:

```
arp-proxy inter-sub-vlan-proxy enable
```

Proxy ARP between VLANs is enabled.

----End

## 2.4.4 Checking the Configuration

Run the following commands to check the pervious configuration.

| Action  | Command  |
|---|--|
| View information about ARP mapping tables based on VLANIF interfaces. | <b>display arp interface vlan interface</b> <i>vlan interface number</i> |
| View statistics about ARP entries.                                    | <b>display arp statistics</b>  |

Run the **display arp interface** command. If all the ARP entries of the VLANIF interface are displayed, it means that the configuration succeeds. For example:

```
<Quidway> display arp interface vlanif 1
IP ADDRESS      MAC ADDRESS    EXPIRE(M)  TYPE  INTERFACE  VPN-INSTANCE
                                VLAN
```

```
-----
192.168.32.11    0001-0168-0182    I -   Vlanif1
1.1.1.1         0001-0168-0182    I -   Vlanif1
192.168.6.255   Incomplete      0     D-0   Vlanif1
192.168.1.255   Incomplete      0     D-0   Vlanif1
192.168.29.255  Incomplete      1     D-0   Vlanif1
192.168.6.10    0200-0010-0232    5     DF0   GE0/0/24
                1
192.168.3.181   0018-8236-f110    6     DF0   GE0/0/24
                1
192.168.3.182   0200-000b-3517    6     DF0   GE0/0/24
                1
192.168.6.6     0018-8238-9212    6     DF0   GE0/0/24
                1
192.168.3.240   0018-8261-2503    7     DF0   GE0/0/24
                1
192.168.1.124   00e0-4c77-deff    14    DF0   GE0/0/24
                1
192.168.4.131   00e0-4c77-826b    15    DF0   GE0/0/24
                1
192.168.31.180  00e0-4c83-aae8    16    DF0   GE0/0/24
                1
192.168.31.181  001e-9089-c65a    18    DF0   GE0/0/24
                1
192.168.81.13   00e0-4c77-b2cf    18    DF0   GE0/0/24
                1
192.168.216.99  00e0-4c77-7219    18    DF0   GE0/0/24
                1
192.168.229.142 0018-8253-21cf    19    DF0   GE0/0/24
                1
192.168.3.169   0018-8261-652c    20    DF0   GE0/0/24
                1
192.168.100.55  0018-8252-3335    20    DF0   GE0/0/24
                1
192.168.3.179   0200-0012-1534    20    DF0   GE0/0/24
                1
192.168.225.2   4e74-6300-0422    20    DF0   GE0/0/24
                1
-----
Total:21        Dynamic:19        Static:0        Interface:2
```

Run the **display arp statistics** command. If statistics about ARP entries are displayed, it means that the configuration succeeds. For example:

```
<Quidway> display arp statistics
Total:27        Dynamic:21        Static:0        Interface:6
```

## 2.5 Maintaining ARP

This section describes how to display ARP configurations, clear ARP statistics and debug ARP.

### 2.5.1 Clearing ARP Statistics

### 2.5.2 Monitoring Network Operation Status

### 2.5.3 Debugging ARP

## 2.5.1 Clearing ARP Statistics

**CAUTION**

The mapping between the IP and MAC addresses is deleted after you clear ARP statistics.

To clear the ARP statistics, run the following **reset** command in the user view.

| Action  | Command  |
|---|--|
| Clear the ARP entries in the ARP mapping table. | <b>reset arp</b> { <b>all</b>   <b>dynamic</b>   <b>interface</b> <i>interface-type interface-number</i>   <b>static</b> } |

## 2.5.2 Monitoring Network Operation Status

To obtain configurations about ARP in routine maintenance, run the following command.

| Action  | Command  |
|---|--|
| View information about the ARP mapping table based on interfaces. | <b>display arp interface</b> <i>interface-type interface-number</i> [   { <b>begin</b>   <b>exclude</b>   <b>include</b> } <i>regular-expression</i> ] |

## 2.5.3 Debugging ARP

**CAUTION**

Debugging affects the performance of the system performance. So, after debugging, run the **undo debugging all** command to disable it immediately.

When faults occur during ARP operation, run the following **debugging** command in the user view to debug ARP and locate the fault.

| Action                      | Command  |
|-----------------------------|--|
| Enable ARP debugging.       | <b>debugging arp packet</b>  |
| Enable proxy ARP debugging. | <b>debugging arp-proxy</b> [ <b>inner-sub-vlan-proxy</b>   <b>inter-sub-vlan-proxy</b> ] [ <b>interface</b> <i>interface-type interface-number</i> ] |

## 2.6 Configuration Examples

This section provides several configuration examples of ARP, proxy ARP in a VLAN, and proxy ARP between VLANs.

### 2.6.1 Example for Configuring Static ARP

[2.6.2 Example for Configuring Dynamic ARP](#)

[2.6.3 Example for Configuring Proxy ARP](#)

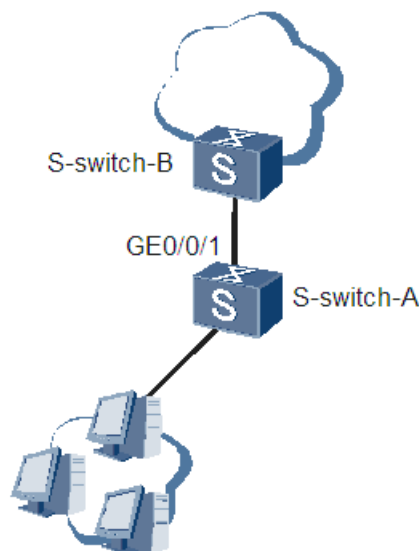
[2.6.4 Example for Configuring Proxy ARP Between VLANs](#)

## 2.6.1 Example for Configuring Static ARP

### Networking Requirements

As shown in **Figure 2-1**, the S-switch-A connected to the hosts also connects the S-switch-B through GigabitEthernet 0/0/1. It is required that a static ARP entry be added on GigabitEthernet 0/0/1. The IP address and MAC address of the S-switch-B are 10.2.2.3 and 00e0-fc01-0000 respectively; GigabitEthernet 0/0/1 belongs to VLAN 3.

**Figure 2-1** Networking diagram for configuring static ARP



### Configuration Roadmap

The configuration roadmap is as follows:

1. Create a VLAN and add the interface in the VLAN.
2. Create a static ARP entry.

### Data Preparation

To complete the configuration, you need the following data:

- GigabitEthernet 0/0/1 belonging to VLAN 3
- IP address 10.2.2.3 and MAC address 00e0-fc01-0000 of the S-switch-B

### Configuration Procedure

The procedure for configuring the S-switch-A is as follows:

1. Create a VLAN and add the interface in the VLAN.

# Create VLAN 3.

```
<Quitway> system-view
[Quitway] vlan 3
```

# Add GigabitEthernet 0/0/1 in VLAN 3.

```
[Quitway] interface gigabitethernet 0/0/1
[Quitway-GigabitEthernet0/0/1] port trunk allow-pass vlan 3
[Quitway-GigabitEthernet0/0/1] quit
```

2. Create a static ARP entry.

# Create VLANIF 3.

```
[Quitway] interface vlanif 3
```

# Assign an IP address to VLANIF 3.

```
[Quitway-Vlanif3] ip address 10.2.2.2 255.0.0.0
[Quitway-Vlanif3] quit
```

# Create a static ARP entry with IP address 10.2.2.3, MAC address 00e0-fc01-0000, VLAN ID 3, and outbound interface GigabitEthernet 0/0/1.

```
[Quitway] arp static 10.2.2.3 00e0-fc01-0000 vid 3 interface gigabitethernet 0/0/1
```

3. Verify the configuration.

# Run the **display arp** command to view the ARP mapping table.

```
<quitway> display arp static
P ADDRESS      MAC ADDRESS    EXPIRE (M)  TYPE  INTERFACE      VPN-INSTANCE
VLAN
-----
10.2.2.3       00e0-fc01-0000          S--
GE0/0/1
3
-----
Total:1         Dynamic:0        Static:1     Interface:0
```

## Configuration Files

- The following is the configuration file of the S-switch-A.

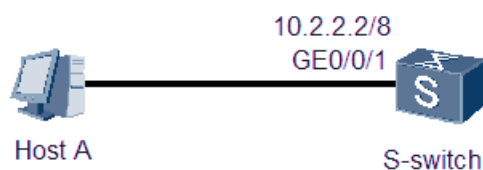
```
#
 sysname S-switch-A
#
vlan 3
#
arp static 10.2.2.3 00e0-fc01-0000 vid 3 interface GigabitEthernet0/0/1
#
interface Vlanif3
 ip address 10.2.2.2 255.0.0.0
#
interface GigabitEthernet 0/0/1
 port trunk allow-pass vlan 3
#
return
```

## 2.6.2 Example for Configuring Dynamic ARP

### Networking Requirements

As shown in [Figure 2-2](#), a host logs in to the S-switch through Telnet. It is required that the aging time of dynamic ARP entries be 60s and the S-switch delete the expired dynamic ARP entries after detecting them twice.

**Figure 2-2** Networking diagram for configuring dynamic ARP



## Configuration Roadmap

The configuration roadmap is as follows:

1. Create a VLAN.
2. Create a VLANIF interface and assign an IP address to the VLANIF interface.
3. Add the interface in the VLAN.
4. Configure ARP attributes for the VLANIF interface.

## Data Preparation

To complete the configuration, you need the following data:

- VLAN ID: 10
- IP address of the VLANIF interface: 10.2.2.2
- Aging time of the dynamic ARP entries of VLANIF 10: 60s, and number of detections: 2

## Configuration Procedure

1. # Create a VLAN.  

```
[Quidway] vlan 10  
[Quidway-vlan10] quit
```
2. # Create a VLANIF interface.  

```
[Quidway] interface vlanif 10
```
3. # Assign an IP address to the VLANIF interface.  

```
[Quidway-Vlanif10] ip address 10.2.2.2 255.0.0.0
```
4. # Add the interface in the VLAN.  

```
[Quidway] interface gigabitethernet 0/0/1  
[Quidway-GigabitEthernet0/0/1] port default vlan 10
```
5. # Configure ARP attributes for the VLANIF interface.  

```
[Quidway] interface vlanif 10  
[Quidway-Vlanif10] arp expire-time 60  
[Quidway-Vlanif10] arp detect-times 2
```
6. # Verify the configuration.

Host A telnets S-switch successfully through the VLANIF interface with IP address 10.2.2.2.

Run the **display arp interface vlanif** command. You can view the following information about the ARP mapping table:

```
[Quidway] display arp interface vlanif 10  
IP ADDRESS      MAC ADDRESS    EXPIRE (M)      TYPE INTERFACE  
                VLAN
```

```

-----
10.2.2.2      000b-0922-d8a3      I - Vlanif10
-----
Total:1      Dynamic:0      Static:0      Interface:1

```

## Configuration Files

Configuration file of S-switch

```

#
 sysname Quidway
 vlan batch 10
#
 interface Vlanif10
  ip address 10.2.2.2 255.0.0.0
  arp expire-time 60
  arp detect-times 2
#
 interface GigabitEthernet0/0/1
  port default vlan 10
#
return

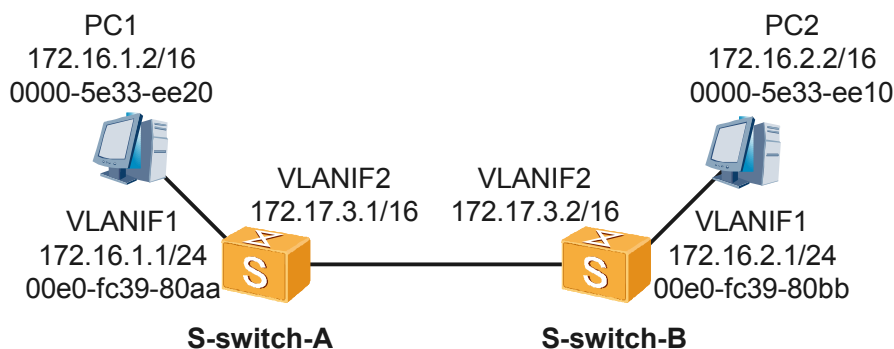
```

## 2.6.3 Example for Configuring Proxy ARP

### Networking Requirements

As shown in [Figure 2-3](#), two S-switches are directly connected. One Ethernet interface on each S-switch is connected to a LAN. Network numbers of the two LANs are 172.16.0.0/16. The default gateway is not configured on PC 1 or PC 2. Proxy ARP must be configured on the S-switch and hosts in the two LANs can access each other.

**Figure 2-3** Networking diagram of configuring proxy ARP



## Configuration Roadmap

The configuration roadmap is as follows:

1. Configure IP addresses for VLANIF interfaces.
2. Enable proxy ARP on VLANIF interfaces.
3. Configure the default routes.

## Data Preparation

To complete the configuration, you need the following data:

- IP address for related interfaces
- Default routes
- IP address of the host

## Configuration Procedure

### 1. Configure S-switch-A.

# Configure an IP address for VLANIF1.

```
<Quidway> system-view
[Quidway] sysname S-switch-A
[S-switch-A] interface vlanif 1
[S-switch-A-Vlanif1] ip address 172.16.1.1 255.255.255.0
```

# Enable proxy ARP.

```
[S-switch-A-Vlanif1] arp-proxy enable
[S-switch-A-Vlanif1] quit
```

# Configure a static route.

```
[S-switch-A] ip route-static 0.0.0.0 0 vlanif 2 172.17.3.2
```

# Configure an IP address for VLANIF2.

```
[S-switch-A] interface vlanif 2
[S-switch-A-Vlanif2] ip address 172.17.3.1 255.255.0.0
[S-switch-A-Vlanif2] quit
```

### 2. Configure S-switch-B.

# Configure an IP address for VLANIF1.

```
<Quidway> system-view
[Quidway] sysname S-switch-B
[S-switch-B] interface vlanif 1
[S-switch-B-Vlanif1] ip address 172.16.2.1 255.255.255.0
```

# Enable proxy ARP.

```
[S-switch-B-Vlanif1] arp-proxy enable
[S-switch-B-Vlanif1] quit
```

# Configure a static route.

```
[S-switch-B] ip route-static 0.0.0.0 0 vlanif 2 172.17.3.1
```

# Configure an IP address for VLANIF2.

```
[S-switch-B] interface vlanif 2
[S-switch-B-Vlanif2] ip address 172.17.3.2 255.255.0.0
[S-switch-B-Vlanif2] quit
```

### 3. Configure the host.

Configure the IP address of PC1 to 172.16.1.2/16.

Configure the IP address of PC2 to 172.16.2.2/16.

### 4. Verify the configuration.

# PC1 can ping through PC2.

# The ARP table of PC1 shows that the MAC address of PC2 is the MAC address of VLANIF1 on S-switch-A.

## Configuration Files

- Configuration file of S-switch-A
 

```
#
sysname S-switch-A
#
interface Vlanif1
 ip address 172.16.1.1 255.255.255.0
 arp-proxy enable
#
interface Vlanif2
 ip address 172.17.3.1 255.255.0.0
#
ip route-static 0.0.0.0 0 Vlanif2 172.17.3.2
#
return
```
- Configuration file of S-switch-B
 

```
#
sysname S-switch-B
#
interface Vlanif1
 ip address 172.16.2.1 255.255.255.0
 arp-proxy enable
#
interface Vlanif2
 ip address 172.17.3.2 255.255.0.0
#
ip route-static 0.0.0.0 0 Vlanif2 172.17.3.1
#
return
```

## 2.6.4 Example for Configuring Proxy ARP Between VLANs

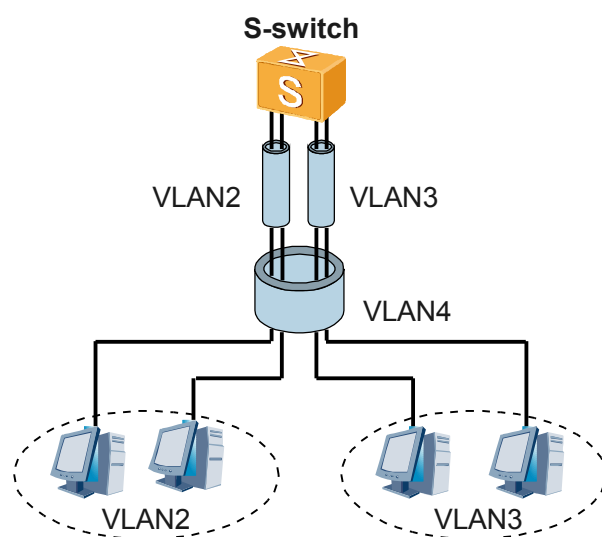
### Networking Requirements

As shown in [Figure 2-4](#), VLAN 2 and VLAN 3 compose a super-VLAN, VLAN 4.

The sub-VLANs, VLAN 2 and VLAN 3 cannot ping through each other.

To implement communication between VLAN 2 and VLAN 3, configure proxy ARP between VLANs.

**Figure 2-4** Networking diagram of configuring proxy ARP between VLANs



## Configuration Roadmap

The configuration roadmap is as follows:

1. Configure an IP address for the VLANIF4 interface.
2. Enable proxy ARP between VLANs on the VLANIF4 interface.

## Data Preparation

To complete the configuration, you need IP addresses of related interfaces.

## Configuration Procedure

This example covers only the commands used to configure proxy ARP between VLANs.

1. Configure an IP address for the VLANIF4 interface.  

```
<Quidway> system-view
[Quidway] sysname S-switch
[S-switch] interface vlanif 4
[S-switch-Vlanif4] ip address 192.168.1.100 255.255.255.0
[S-switch-Vlanif4] quit
```
2. Configure IP addresses for PCs.  
# Configure IP addresses for PCs. The IP addresses must be in the same network segment with the IP address of the VLANIF4 interface.  
# After configurations, PCs and the device can ping through each other but PCs in VLAN 2 and PCs in VLAN 3 cannot ping through each other.
3. Configure proxy ARP between VLANs.  

```
[S-switch] interface vlanif 4
[S-switch-Vlanif4] arp-proxy inter-sub-vlan-proxy enable
[S-switch-Vlanif4] quit
```
4. Verify the configuration.
  - PCs in VLAN 2 and PCs in VLAN 3 can ping through each other.
  - Check the ARP table on the PC.

# You can find that in the ARP table of any PC in VLAN 2, the MAC addresses of all PCs in VLAN 3 are the MAC address of the VLANIF4 interface on S-switch.

## Configuration Files

The configuration file of S-switch is as follows:

```
#
sysname S-switch
#
vlan batch 2 to 4
#
vlan 4
aggregate-vlan
access-vlan 2 to 3
#
interface Vlanif4
ip address 192.168.1.100 255.255.255.0
arp-proxy inter-sub-vlan-proxy enable
#
```

[Return](#)

# 3 DNS Configuration

---

## About This Chapter

This chapter describes the static and dynamic DNS concepts and their configuration steps, along with typical examples.

### [3.1 Overview](#)

This section describes the basic principle and concepts of Domain Name System (DNS).

### [3.2 Configuring DNS](#)

This section describes how to use the domain name to communicate with other devices.

### [3.3 Maintaining DNS](#)

This section describes how to clear DNS entries and debug DNS.

### [3.4 Configuration Examples](#)

This section provides a configuration example of DNS.

## 3.1 Overview

This section describes the basic principle and concepts of Domain Name System (DNS).

### [3.1.1 Introduction to DNS](#)

### [3.1.2 DNS Supported by the S-switch](#)

### [3.1.3 Update History](#)

## 3.1.1 Introduction to DNS

The Domain Name System (DNS) is a host naming mechanism provided by TCP/IP, with which hosts can be named in the form of character string. This system assumes a hierarchical naming structure. It designates a meaningful name for the device in the Internet and associates the name with the IP address through a domain name resolution server. In this manner, you can use domain names that are easy to remember instead of memorizing complex IP addresses.

## 3.1.2 DNS Supported by the S-switch

DNS has two resolution modes: dynamic DNS resolution and static DNS resolution. To resolve a domain name, the system first uses static DNS resolution. If this mode fails, the system uses dynamic DNS resolution. To improve resolution efficiency, you can put common domain names in a static domain name resolution table.

The S-switch supports static resolution and dynamic resolution.

## 3.1.3 Update History

| Version         | Revision                   |
|-----------------|----------------------------|
| V100R002C01B050 | This is the first release. |

## 3.2 Configuring DNS

This section describes how to use the domain name to communicate with other devices.

### [3.2.1 Establishing the Configuration Task](#)

### [3.2.2 Configuring Static DNS Entries](#)

### [3.2.3 Configuring Dynamic DNS](#)

### [3.2.4 Checking the Configuration](#)

## 3.2.1 Establishing the Configuration Task

## Applicable Environment

If local users accessing devices need to communicate with other devices by using domain names, you can configure DNS on the device.

If local users communicate with other devices hardly through the domain name or if the DNS server is unavailable, configure static DNS. Prior to configuring static DNS, you must know the mapping between the domain name and the IP address. In case of a change in the mapping, you must modify the DNS entry manually.

You can configure dynamic DNS on the device if local users frequently use domain names for communicating with other devices and the DNS server is available.

## Pre-configuration Tasks

Before configuring DNS, complete the following tasks:

- Configuring physical attributes of the interface and ensuring that the physical layer status of the interface is Up
- Configuring parameters of the link layer protocol of the interface and ensuring that the link layer protocol status of the interface is Up
- Configuring routes between the local device and the DNS server
- Configuring the DNS server

## Data Preparation

To configure DNS, you need the following data.

| No. | Data   |
|-----|--|
| 1   | Domain name and the corresponding IP address in a static DNS entry |
| 2   | IP address of a DNS server   |
| 3   | Domain name or the domain name list of a dynamic DNS entry         |

## 3.2.2 Configuring Static DNS Entries

### Context

You can configure a maximum of 50 static DNS entries.

Do as follows on the S-switch:

### Procedure

**Step 1** Run:

```
system-view
```

The system view is displayed.

**Step 2** Run:

```
ip host host-name ip-address
```

The IP address corresponding to the host name is configured.

A host name corresponds to only one IP address. When you configure an IP address for a host for several times, only the IP address configured at the latest is valid. To resolve several host names, repeat Step 2.

----End

### 3.2.3 Configuring Dynamic DNS

#### Context

Do as follows on the S-switch:

#### Procedure

**Step 1** Run:

**system-view**

The system view is displayed.

**Step 2** Run:

**dns resolve**

The function of dynamic domain name resolution is enabled.

**Step 3** Run:

**dns server** *ip-address*

A DNS server is specified.

**Step 4** Run:

**dns domain** *domain-name*

The suffix of the domain name is added.

----End

#### Postrequisite

The system supports the configuration of a maximum of 6 domain name servers, 1 source address, and 10 domain name suffixes.

To configure more than one domain name server, repeat Step 3.

To configure more than one domain name suffix, repeat Step 4.

### 3.2.4 Checking the Configuration

Run the following commands to check the previous configuration.

| Action  | Command                   |
|---|---------------------------|
| Check information about the static DNS entry table. | <b>display ip host</b>    |
| Check configurations about DNS servers.             | <b>display dns server</b> |

| Action  | Command                         |
|---|---------------------------------|
| Check configurations about domain name suffixes.                      | <b>display dns domain</b>       |
| Check information about dynamic DNS entries in the domain name cache. | <b>display dns dynamic-host</b> |

Run the **display ip host** command. If static DNS entries including the mappings between host names and IP addresses, are displayed, it means that the configuration succeeds. For example:

```
<Quidway> display ip host
Host      Age      Flags      Address
hw        0          static    10.1.1.1
gww       0          static    192.168.1.1
```

Run the **display dns server** command. If IP addresses of all domain servers are displayed, it means that the configuration succeeds. For example:

```
<Quidway> display dns server
IPv4 Dns Servers :
Domain-server      IPAddress
1                  172.16.1.1
2                  172.16.1.2
```

```
IPv6 Dns Servers :
No configured servers.
```

Run the **display dns domain** command. If the list of suffixes of domain names is displayed, it means that the configuration succeeds. For example:

```
<Quidway> display dns domain
No      Domain-name
1       com
2       net
```

Run the **display dns dynamic-host** command. If information about the dynamic domain name cache is displayed, it means that the configuration succeeds. For example:

```
<Quidway> display dns dynamic-host
No  Domain-name      IPAddress      TTL      Alias
1   www.huawei.com    91.1.1.1      3521
2   www.huawei.com.cn 87.1.1.1      3000
```

## 3.3 Maintaining DNS

This section describes how to clear DNS entries and debug DNS.

### 3.3.1 Clearing DNS Entries

### 3.3.2 Monitoring Network Operation Status

### 3.3.3 Debugging DNS

## 3.3.1 Clearing DNS Entries

**CAUTION**

DNS entries cannot be restored after being cleared. So, confirm the action before you use this command.

To clear DNS entries, run the following **reset** command in the user view.

| Action  | Command                       |
|---|-------------------------------|
| Clear dynamic DNS entries in the domain name cache. | <b>reset dns dynamic-host</b> |

### 3.3.2 Monitoring Network Operation Status

In routine maintenance, to obtain configurations about DNS, run the following commands.

| Action  | Command                         |
|---|---------------------------------|
| Check information about the static DNS entry table.                   | <b>display ip host</b>          |
| Check configurations about DNS servers.                               | <b>display dns server</b>       |
| Check configurations about domain name suffixes.                      | <b>display dns domain</b>       |
| Check information about dynamic DNS entries in the domain name cache. | <b>display dns dynamic-host</b> |

### 3.3.3 Debugging DNS

**CAUTION**

Debugging affects the performance of the system. So after debugging, run the **undo debugging all** command to disable it immediately.

Run the following **debugging** command in the user view to debug DNS and locate the fault.

| Action                        | Command              |
|-------------------------------|----------------------|
| Enable dynamic DNS debugging. | <b>debugging dns</b> |

## 3.4 Configuration Examples

This section provides a configuration example of DNS.

#### 3.4.1 Example for Configuring DNS

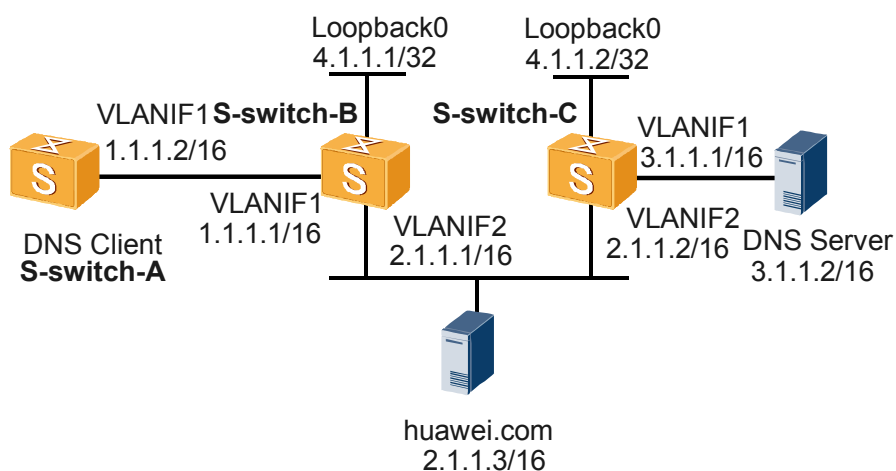
## 3.4.1 Example for Configuring DNS

### Networking Requirements

As shown in [Figure 3-1](#), S-switch-A acts as a DNS client, being required to access the host 2.1.1.3/16 by using the domain name huawei.com. You need to configure domain name suffixes "com" and "net".

On S-switch-A, configure static DNS entries of S-switch-B and S-switch-C so that S-switch-A can communicate with them by using domain names.

**Figure 3-1** Networking diagram of DNS



### Configuration Roadmap

The configuration roadmap is as follows:

1. Configure static DNS entries.
2. Enable DNS resolution.
3. Configure an IP address for the DNS server.
4. Configure suffixes of domain names.

### Data Preparation

To complete the configuration, you need the following data:

- Domain names of S-switch-B and S-switch-C
- IP address of the DNS server
- Suffixes of domain names

## Configuration Procedure

### NOTE

Before performing configurations, suppose:

- S-switch-A and each host have been configured with IP addresses and other configurations.
- The mapping between the domain name "huawei.com" and the IP address 2.1.1.3/16 is available on the DNS server.
- The DNS server works normally.

#### 1. Configure S-switch-A.

# Configure static DNS entries.

```
<S-switch-A> system-view
[S-switch-A] ip host S-switch-B 4.1.1.1
[S-switch-A] ip host S-switch-C 4.1.1.2
```

# Enable DNS resolution.

```
[S-switch-A] dns resolve
```

# Configure an IP address for the DNS server.

```
[S-switch-A] dns server 3.1.1.2
```

# Configure a domain name suffix "net".

```
[S-switch-A] dns domain net
```

# Configure a domain name suffix "com".

```
[S-switch-A] dns domain com
```

### NOTE

To complete DNS resolution, configuring routes from S-switch-A to the DNS server is mandatory.

#### 2. Verify the configuration.

# Run the **ping huawei.com** command on S-switch-A to ping the IP address 2.1.1.3. The ping succeeds.

```
<S-switch-A> ping huawei.com
Trying DNS server (3.1.1.2)
  PING huawei.com (2.1.1.3): 56 data bytes, press CTRL_C to break
    Reply from 2.1.1.3: bytes=56 Sequence=1 ttl=126 time=6 ms
    Reply from 2.1.1.3: bytes=56 Sequence=2 ttl=126 time=4 ms
    Reply from 2.1.1.3: bytes=56 Sequence=3 ttl=126 time=4 ms
    Reply from 2.1.1.3: bytes=56 Sequence=4 ttl=126 time=4 ms
    Reply from 2.1.1.3: bytes=56 Sequence=5 ttl=126 time=4 ms
  --- huawei.com ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 4/4/6 ms
```

# Run the **display ip host** command on S-switch-A to view static DNS entries, including mappings between host names and IP addresses.

```
<S-switch-A> display ip host
Host                Age      Flags Address
S-switch-B          0       static 4.1.1.1
S-switch-C          0       static 4.1.1.2
```

# Run the **display dns dynamic-host** command on S-switch-A to view dynamic DNS entries in the domain name cache.

```
<S-switch-A> display dns dynamic-host
No  Domain-name      IpAddress      TTL      Alias
1   huawei.com        2.1.1.3        3579
```



TTL value in the above display indicates the lifetime of an entry. It is in seconds.

## Configuration Files

- Configuration file of S-switch-A

```
#
sysname S-switch-A
#
ip host S-switch-B 4.1.1.1
ip host S-switch-C 4.1.1.2
#
dns resolve
dns server 3.1.1.2
dns domain net
dns domain com
#
interface Vlanif1
ip address 1.1.1.2 255.255.0.0
#
rip 1
network 1.0.0.0
#
return
```

- Configuration file of S-switch-B

```
#
sysname S-switch-B
#
interface Vlanif2
ip address 2.1.1.1 255.255.0.0
#
interface Vlanif1
ip address 1.1.1.1 255.255.0.0
#
interface LoopBack0
ip address 4.1.1.1 255.255.255.255
#
rip 1
network 2.0.0.0
network 1.0.0.0
network 4.0.0.0
#
return
```

- Configuration file of S-switch-C

```
#
sysname S-switch-C
#
interface Vlanif2
ip address 2.1.1.2 255.255.0.0
#
interface Vlanif1
ip address 3.1.1.1 255.255.0.0
#
interface LoopBack0
ip address 4.1.1.2 255.255.255.255
#
rip 1
network 2.0.0.0
network 3.0.0.0
network 4.0.0.0
#
return
```



# 4 DHCP Configuration

---

## About This Chapter

This chapter describes the DHCP fundamentals including DHCP service, DHCP server, and relay agent. It also includes configuration steps for DHCP Server based on different parameters, DHCP relay agent, and security functions in DHCP service, along with typical examples.

### [4.1 Overview](#)

This section describes the principle and concepts of the Dynamic Host Configuration Protocol (DHCP).

### [4.2 Configuring the Global Address Pool-based DHCP Server](#)

This section describes how to configure a DHCP server when hosts are connected with S-switch through other devices.

### [4.3 Configuring VLANIF Interface Address Pool-based DHCP Server](#)

This section describes how to configure a DHCP server that uses the address pool of the VLANIF interface.

### [4.4 Configuring the Security Function for DHCP](#)

This section describes how to enhance the security of the DHCP service.

### [4.5 Configuring DHCP Relay](#)

This section describes how to enable DHCP relay so that DHCP relay can forward DHCP requests from local clients to the DHCP server on other networks.

### [4.6 Maintaining DHCP](#)

This section describes how to clear the statistics about DHCP and debug DHCP.

### [4.7 Configuration Examples](#)

This section provides several configuration examples of the DHCP server and DHCP relay.

## 4.1 Overview

This section describes the principle and concepts of the Dynamic Host Configuration Protocol (DHCP).

### [4.1.1 Introduction to DHCP](#)

### [4.1.2 DHCP Supported by the S-switch](#)

### [4.1.3 Update History](#)

## 4.1.1 Introduction to DHCP

With the rapid growth in network scale and complexity, network configuration becomes more difficult. The location of hosts changes (such as laptops and wireless network) and the number of hosts has exceeded that of the available IP addresses. The Dynamic Host Configuration Protocol (DHCP) is developed to solve these problems.

## 4.1.2 DHCP Supported by the S-switch

The S-switch supports the following DHCP applications, ensures the security of DHCP services, and provides the DHCP relay agent function.

- Global address pool
- Address pool on the VLAN logical interface

## 4.1.3 Update History

| Version         | Revision                   |
|-----------------|----------------------------|
| V100R002C01B050 | This is the first release. |

## 4.2 Configuring the Global Address Pool-based DHCP Server

This section describes how to configure a DHCP server when hosts are connected with S-switch through other devices.

### [4.2.1 Establishing the Configuration Task](#)

### [4.2.2 Configuring the DHCP Global Address Pool](#)

### [4.2.3 Configure Static IP Address Binding](#)

### [4.2.4 Configuring DNS Services for the DHCP Client](#)

### [4.2.5 Configuring NetBIOS Services for the DHCP Client](#)

### [4.2.6 Configuring Egress Gateway for the DHCP Client](#)

### [4.2.7 Configuring DHCP Self-Defined Options](#)

[4.2.8 Assigning IP Addresses in the Global Address Pool to the DHCP Clients on the Specified Interface](#)

[4.2.9 Checking the Configuration](#)

## 4.2.1 Establishing the Configuration Task

### Applicable Environment

To obtain IP addresses from the device dynamically, you need to configure a global address pool-based DHCP server.

The global address pool-based DHCP server usually works together with the DHCP relay agent.

### Pre-configuration Tasks

Before configuring the global address pool-based DHCP server, complete the following tasks:

- Configuring the DNS server
- Configuring the NetBIOS server
- Configuring the routes to the DNS server and the NetBIOS server

### Data Preparation

To configure the global address pool-based DHCP server, you need the following data.

| No. | Data  |
|-----|---|
| 1   | Name and the address range of the address pool  |
| 2   | Range of the IP addresses that cannot be dynamically assigned to hosts  |
| 3   | IP addresses and the MAC addresses that need to be bound statically   |
| 4   | Lease of the IP address   |
| 5   | IP address of the DNS server and the domain name of the DHCP client   |
| 6   | IP address of the NetBIOS server and the NetBIOS node type of the DHCP client                                   |
| 7   | Coding of the DHCP self-defined options and the corresponding ASCII strings or hexadecimal number or IP address |

## 4.2.2 Configuring the DHCP Global Address Pool

### Context

Do as follows on the S-switch:

## Procedure

**Step 1** Run:

```
system-view
```

The system view is displayed.

**Step 2** Run:

```
dhcp enable
```

DHCP is enabled.

**Step 3** Run:

```
dhcp server ip-pool pool-name
```

A DHCP address pool is created and the DHCP address pool view is displayed.

 **NOTE**

Each DHCP server can be configured with a maximum of 128 global address pools.

**Step 4** Run:

```
network ip-address [ mask { mask | mask-length } ]
```

The address pool range is configured.

**Step 5** Run:

```
expired { day day [ hour hour [ minute minute ] ] | unlimited }
```

The lease of the IP addresses dynamically assigned to hosts is configured. By default, the IP lease is one day.

 **NOTE**

The DHCP server can specify the IP lease for each address pool. The IP lease may vary with address pools. The addresses in the same DHCP address pool, however, have the same IP lease.

**Step 6** Run:

```
quit
```

Back to the system view.

**Step 7** Run:

```
dhcp server forbidden-ip low ip address [ high ip address ]
```

The range of IP addresses that cannot be dynamically assigned is configured.

 **NOTE**

After repeatedly running the **dhcp server forbidden-ip** command, you can configure multiple IP address segments that cannot be automatically assigned. When using the **undo dhcp server forbidden-ip** command to delete the setting, ensure that the specified parameters are consistent with the previously configured parameters. That is, you cannot delete only partial originally configured addresses.

----End

## 4.2.3 Configure Static IP Address Binding

### Context

Do as follows on the S-switch:

## Procedure

**Step 1** Run:

```
system-view
```

The system view is displayed.

**Step 2** Run:

```
dhcp server ip-pool pool-name
```

A DHCP address pool is created and the DHCP address pool view is displayed.

**Step 3** Run:

```
static-bind ip-address ip-address [ mask { mask | mask-length } ]
```

Certain IP addresses are statically bound.

**Step 4** Run:

```
static-bind mac-address mac-address
```

MAC addresses of certain clients are statically bound.

----End

## Postrequisite

Based on the clients' needs, you can adopt either static address binding or dynamic address assignation. However, you cannot configure the same DHCP address pool with these two modes at the same time.

Dynamic address distribution needs specification of the address range for assignment, while static address binding can be regarded as a special DHCP address pool with only one address.

Some clients may need fixed IP addresses that are bound with their MAC addresses. When the client with a specific MAC address uses DHCP to apply for an IP address, the DHCP server finds out the fixed IP address bound with the MAC address and assigns it to the client.

 **NOTE**

The **static-bind ip-address** command must be used together with the **static-bind mac-address** command. The new configuration supersedes the previous one when you use the two commands for several times.

## 4.2.4 Configuring DNS Services for the DHCP Client

### Context

Do as follows on the S-switch:

### Procedure

**Step 1** Run:

```
system-view
```

The system view is displayed.

**Step 2** Run:

```
dhcp server ip-pool pool-name
```

The DHCP address pool view is displayed.

**Step 3** Run:

```
domain-name domain-name
```

The domain name of the DHCP client is configured.

**Step 4** Run:

```
dns-list ip-address <1-8>
```

The IP address of the DNS server of the DHCP client is configured.

----End

## Postrequisite

On the DHCP server, designate a domain name for the client per address pool basis.

When a host accesses the Internet by using the domain name, the DNS server resolves the domain name into an IP address. Therefore, to ensure that the client can successfully access the Internet, the DHCP server also needs to specify the DNS server address for the client when it assigns IP addresses.

To perform load balancing and improve the network reliability, you can configure several DNS servers and egress gateways.

## 4.2.5 Configuring NetBIOS Services for the DHCP Client

### Context

Do as follows on the S-switch:

### Procedure

**Step 1** Run:

```
system-view
```

The system view is displayed.

**Step 2** Run:

```
dhcp server ip-pool pool-name
```

The DHCP address pool view is displayed.

**Step 3** Run:

```
nbns-list ip-address <1-8>
```

The IP address of the NetBIOS server of the DHCP client is configured.

**Step 4** Run:

```
netbios-type { b-node | h-node | m-node | p-node }
```

The NetBIOS node type of the DHCP client is configured.

By default, the node type of the DHCP client is not specified.

----End

## Postrequisite

For the client using the OS of Microsoft, Windows Internet Naming Service (WINS) server provides resolution from the host name to the IP address. This is given to the host that uses NetBIOS protocol for communication. Most of the Windows clients need to be configured with WINS.

When a DHCP client communicates in a WAN by adopting the NetBIOS protocol, a mapping between the host name and the IP address should be set up. The following lists the types of NetBIOS nodes for obtaining mappings:

- Type b nodes (b-node): "b" stands for broadcast; that is, type b nodes obtain the mapping relation by means of broadcast.
- Type p nodes (p-node): "p" stands for peer-to-peer, namely, type p nodes obtain the mapping relation by means of communicating with NetBIOS servers.
- Type m nodes (m-node): "m" stands for mixed. Type m nodes are the type p nodes owning part of the broadcasting features.
- Type h nodes (h-node): "h" stands for hybrid. Type h nodes are type b nodes owning the "peer-to-peer" communicating mechanism.

## 4.2.6 Configuring Egress Gateway for the DHCP Client

### Context

### Procedure

**Step 1** Run:

```
system-view
```

The system view is displayed.

**Step 2** Run:

```
dhcp server ip-pool pool-name
```

The DHCP address pool view is displayed.

**Step 3** Run:

```
gateway-list ip-address &<1-8>
```

The egress gateway of the DHCP client is configured.

When a DHCP client wants to access a server (or host) that is not on the local network, an egress gateway needs to be configured on the local network.

To perform load balancing and improve the network reliability, you can configure several DNS servers and egress gateways.

----End

## 4.2.7 Configuring DHCP Self-Defined Options

## Context



### NOTE

Configuring DHCP self-defined options are optional. Services, such as DNS on the client, NETBIOS, and IP lease cannot be configured through the **option code** command but through the commands early mentioned.

Do as follows on the S-switch:

## Procedure

### Step 1 Run:

```
system-view
```

The system view is displayed.

### Step 2 Run:

```
dhcp server ip-pool pool-name
```

The DHCP address pool view is displayed.

### Step 3 Run:

```
option code { ascii ascii-string | hex hex-string | ip-address ip-address <1-8> }
```

The DHCP self-defined options are configured.

----End

## Postrequisite

The Option field in DHCP packets carries the control information and parameters that are not defined in some common protocols. If the DHCP server is configured with Option, the DHCP client gets the configuration information saved in the Option field of DHCP response packets.

You need to add the options to the attribute tables of the DHCP servers. For example,

- To configure the IP address of a log server to 10.110.204.1, use the command **option 7 ip-address 10.110.204.1**.
- To configure the TTL of the client packet to 64, use the command **option 23 hex 40**.



### NOTE

Using the **option** command, you can specify the options to be included in the DHCP response packets.

Before using the **option** command, you need to know the function of each option: Option 77 identifies user types or applications of DHCP client. Based on User Class in the Option field, the DHCP server selects the proper address pool and configuration parameters. Option 77 usually is configured on the client.

## 4.2.8 Assigning IP Addresses in the Global Address Pool to the DHCP Clients on the Specified Interface

## Context

Do as follows on the S-switch:

## Procedure

- Assigning IP addresses to the clients on the current VLANIF interface
  1. Run:  
**system-view**  
The system view is displayed.
  2. Run:  
**interface vlanif** *VLANIF interface-number*  
The VLNAIF interface view is displayed.
  3. Run:  
**ip address** *ip-address* { *mask* | *mask-length* } [ **sub** ]  
The VLNAIF interface is configured with an IP address.
  4. Run:  
**dhcp select global**  
The IP addresses in the global address pool are assigned.
- Assigning IP addresses to the clients in VLANs
  1. Run:  
**system-view**  
The system view is displayed.
  2. Run:  
**dhcp select global vlan** { *vlan-id1* [ *to* *vlan-id2* ] } &<1-10>  
The IP addresses in the global address pool are assigned.

----End

## 4.2.9 Checking the Configuration

Run the following commands to check the previous configuration.

| Action   | Command   |
|--|---|
| Check the available address information in the DHCP address pool.    | <b>display dhcp server free-ip</b>  |
| Check the expired lease in the DHCP address pool.                    | <b>display dhcp server expired</b> { <b>all</b>   <b>ip</b> <i>ip-address</i>   <b>pool</b> [ <i>pool-name</i> ]   <b>vlan</b> <i>vlan-id</i> }   |
| Check address binding information.                                   | <b>display dhcp server ip-in-use</b> { <b>all</b>   <b>ip</b> <i>ip-address</i>   <b>pool</b> [ <i>pool-name</i> ]   <b>vlan</b> <i>vlan-id</i> } |
| Check the statistics about the DHCP server.                          | <b>display dhcp server statistics</b>   |
| Check information about the tree-structure of the DHCP address pool. | <b>display dhcp server tree</b> { <b>all</b>   <b>pool</b> [ <i>pool-name</i> ]   <b>vlan</b> <i>vlan-id</i> }                                    |

Run the **display dhcp server free-ip** command. If there are unused IP addresses in the address pool, it means that the configuration succeeds.

```
<Quidway> display dhcp server free-ip
IP Range from 5.5.5.1          to 5.5.5.254
IP Range from 202.38.160.1      to 202.38.160.1
IP Range from 202.38.160.4      to 202.38.160.126
```

Run the **display dhcp server expired** command. If information about the expired leases of IP addresses in DHCP address pools is displayed, it means that the configuration succeeds.

```
<Quidway> display dhcp server expired all
Global pool:
  IP address   Hardware address   Lease expiration   Type
Interface pool:
  IP address   Hardware address   Lease expiration   Type
```

Run the **display dhcp server ip-in-use** command. If the binding information of IP address, such as the hardware address and the IP lease, is displayed, it means that the configuration succeeds.

```
<Quidway> display dhcp server ip-in-use all
Global pool:
  IP address   Hardware address   Lease expiration   Type
Interface pool:
  IP address   Hardware address   Lease expiration   Type
5.5.5.1       0050-ba28-930a Jul 5 2006 13: 00:10 PM   Auto:COMMITTED
```

Run the **display dhcp server statistics** command. If statistics of the DHCP server, including the number of DHCP address pools, the number of the automatic binding, the manual binding and the expired binding and the number of DHCP packets is displayed, it means that the configuration succeeds.

```
<Quidway> display dhcp server statistics
Global Pool:
Pool Number:          5
Binding
Auto:                  0
Manual:                1
Expire:                0
Interface Pool:
Pool Number:          1
Binding
Auto:                  1
Manual:                0
Expire:                0
Boot Request:         6
Dhcp Discover:         1
Dhcp Request:          4
Dhcp Decline:          0
Dhcp Release:          1
Dhcp Inform:           0
Boot Reply:            4
Dhcp Offer:            1
Dhcp Ack:               3
Dhcp Nak:               0
Bad Messages:          0
HA Message:
BatchBackup send msg:  0
BatchBackup recv msg:  0
BatchBackup send lease: 0
BatchBackup recv lease: 0
```

Run the **display dhcp server tree** command. If the tree structure of the DHCP address pool, including DNS, the IP lease and Option parameters, is displayed, it means that the configuration succeeds.

```
<Quidway> display dhcp server tree all
Global pool:
Pool name: 5          network 10.10.1.0 255.255.255.0
Child node:6
Sibling node:7
```

```
option 1 ip-address 255.0.0.0
expired 1 0 0
option 58 hex 00 00 A8 C0
option 59 hex 00 00 00 3C
Pool name: 6          host 10.10.1.2 255.0.0.0
      hardware-address 1111.2222.3333 gigabitethernet
Parent node:5
option 1 ip-address 255.255.0.0
expired 1 0 0
option 58 hex 00 00 A8 C0
option 59 hex 00 00 00 3C
```

## 4.3 Configuring VLANIF Interface Address Pool-based DHCP Server

This section describes how to configure a DHCP server that uses the address pool of the VLANIF interface.

### [4.3.1 Establishing the Configuration Task](#)

### [4.3.2 Enabling Address Pools on VLANIF Interfaces](#)

### [4.3.3 Configuring the Address Pool on the VLANIF Interface](#)

### [4.3.4 Configuring DNS on the Address Pool of the VLANIF Interface](#)

### [4.3.5 Configuring NetBIOS on the Address Pool of the VLANIF Interface](#)

### [4.3.6 Configuring DHCP Self-Defined Options for the Address Pool of the VLANIF Interface](#)

### [4.3.7 Checking the Configuration](#)

## 4.3.1 Establishing the Configuration Task

### Applicable Environment

The interface address pool on the VLANIF interface, is used for devices to support the switched Ethernet interface. Because the switched Ethernet interface cannot be configured with IP addresses directly, you need to create a VLANIF interface and then configure DHCP address pools on the VLANIF interface.

### Pre-configuration Tasks

Before configuring the VLANIF interface address pool-based DHCP server, complete the following tasks:

- Creating a VLANIF interface
- Configuring the DNS server
- Configuring the NetBIOS server
- Configuring routes to the DNS server and the NetBIOS server

### Data Preparation

To configure the VLANIF interface address pool-based DHCP server, you need the following data.

| No. | Data  |
|-----|---|
| 1   | Number, IP address and subnet mask of the VLANIF interface  |
| 2   | IP addresses in the address pools of VLANIF interface and the MAC addresses to be bound with the IP addresses   |
| 3   | Lease of the IP address   |
| 4   | IP address of the DNS server and the domain name of the DHCP client   |
| 5   | IP address of the NetBIOS server and the NetBIOS node type of the DHCP client                                   |
| 6   | Coding of the DHCP self-defined options and the corresponding ASCII strings or hexadecimal number or IP address |

## 4.3.2 Enabling Address Pools on VLANIF Interfaces

### Context

Do as follows on the DHCP server:

### Procedure

- Enabling address pools in the VLANIF interface view
  1. Run:  
**system-view**  
The system view is displayed.
  2. Run:  
**vlan** *vlan-id*  
A VLAN is created.
  3. Run:  
**quit**  
Back to the system view.
  4. Run:  
**interface** **vlanif** *vlan-id*  
The VLANIF interface is displayed.
  5. Run:  
**ip address** *ip-address* { *mask* | *mask-length* }  
The IP address of the VLANIF interface is configured.
  6. Run:  
**dhcp select interface**  
The address pool on the VLANIF interface is enabled.
- Enabling address pools on one VLANIF interface or multiple VLANIF interfaces in the system view
  1. Run:  
**system-view**

- The system view is displayed.
2. Run:  
`vlan vlan-id`  
A VLAN is created.
  3. Run:  
`quit`  
Back to the system view.
  4. Run:  
`interface vlanif VLANIF interface number`  
The VLANIF interface is displayed.
  5. Run:  
`ip address ip-address { mask | mask-length }`  
The IP address of the VLANIF interface is configured.
  6. Run:  
`quit`  
Back to the system view.
  7. Run:  
`dhcp select interface vlan { vlan-id1 [ to vlan-id2 ] } <1-10>`  
The address pool on the specified VLANIF interface is enabled.

----End

### 4.3.3 Configuring the Address Pool on the VLANIF Interface

#### Context

Do as follows on the DHCP server:

#### Procedure

- Step 1** Run:  
`system-view`  
The system view is displayed.
- Step 2** Run:  
`dhcp enable`  
DHCP is enabled.
- Step 3** Run:  
`interface vlanif VLANIF interface number`  
The VLANIF interface view is displayed.
- Step 4** Run:  
`dhcp select interface`  
The address pool on the interface is enabled.

**Step 5** Run:

```
dhcp server static-bind ip-address ip-address mac-address mac-address
```

Certain IP addresses and MAC addresses are bound with the address pool.

**Step 6** The following steps are optional, so perform them as required.

Run:

```
dhcp server expired { day day [ hour hour [ minute minute ] ] | unlimited }
```

The IP lease of the VLANIF interface is configured. By default, the IP lease is one day.

Or

Run:

```
quit
```

Return to the system view.

Run:

```
dhcp server expired { day day [ hour hour [ minute minute ] ] | unlimited } vlan  
{ vlan-id1 [ to vlan-id2 ] } <1-10>
```

The leases of the IP addresses of several VLANIF interfaces are configured. By default, the IP lease is one day.

----End

**Postrequisite**

The IP address and its mask of the VLANIF interface determine the range of the address pool on the VLANIF interface. If you need to configure several address pools for VLANIF interfaces, repeat Steps 3, 4, 5, and 6.

**4.3.4 Configuring DNS on the Address Pool of the VLANIF Interface****Context**

Do as follows on the DHCP server:

**Procedure**

- Configuring DNS on VLANIF interfaces

1. Run:

```
system-view
```

The system view is displayed.

2. Run:

```
interface vlanif VLANIF interface number
```

The VLAIF interface view is displayed.

3. Run:

```
dhcp server domain-name domain-name
```

Domain names are configured for the clients of the VLANIF interface.

4. Run:

```
dhcp server dns-list ip-address <1-8>
```

The IP address of the DNS server is specified for the clients of the VLANIF interface.

- Configuring DNS on one or multiple VLANIF interfaces

1. Run:

```
system-view
```

The system view is displayed.

2. Run:

```
dhcp server domain-name domain-name vlan { vlan-id1 [ to vlan-id2 ] }  
<1-10>
```

The domain name of the DHCP client is configured.

3. Run:

```
dhcp server dns-list ip-address <1-8> vlan { vlan-id1 [ to vlan-id2 ] }  
<1-10>
```

The IP address of the DNS server is specified for the DHCP client.

----End

## 4.3.5 Configuring NetBIOS on the Address Pool of the VLANIF Interface

### Context

Do as follows on the DHCP server:

### Procedure

- Configuring NetBIOS on VLANIF interfaces

1. Run:

```
system-view
```

The system view is displayed.

2. Run:

```
interface vlanif VLANIF interface number
```

The VLANIF interface view is displayed.

3. Run:

```
dhcp server nbns-list ip-address <1-8>
```

The IP address of the NetBIOS server is specified for the DHCP clients of the VLANIF interface.

4. Run:

```
dhcp server netbios-type { b-node | h-node | m-node | p-node }
```

The NetBIOS node type is specified for the DHCP clients of the VLANIF interface.

- Configuring NetBIOS on one or multiple VLANIF interfaces

1. Run:

```
system-view
```

The system view is displayed.

2. Run:

```
dhcp server nbns-list ip-address <1-8> vlan { vlan-id1 [ to vlan-id2 ] }  
<1-10>
```

The IP address of the NetBIOS server is specified for the DHCP client.

3. Run:

```
dhcp server netbios-type { b-node | h-node | m-node | p-node } vlan { vlan-  
id1 [ to vlan-id2 ] } <1-10>
```

The NetBIOS node type is specified for the DHCP client.

By default, the node type of the client is not specified.

----End

## Postrequisite

Before using the NetBIOS service, make sure that

- The NetBIOS server is configured correctly
- There are routes between the device and the NetBIOS server.

For the client using the OS of Microsoft, WINS server provides the resolution from the host name to the IP address for the host that uses the NetBIOS protocol to communicate. In this way, most of the Windows network clients need to be configured with WINS.

When a DHCP client communicates on a WAN, by adopting NetBIOS protocol, a mapping between the host name and the IP address should be set up. The types of NetBIOS nodes for obtaining mappings are as follows:

- Type b nodes (b-node): "b" stands for broadcast; that is, type b nodes obtain the mapping relation by means of broadcast.
- Type p nodes (p-node): "p" stands for peer-to-peer; that is, type p nodes obtain the mapping relation by means of communicating with NetBIOS servers.
- Type m nodes (m-node): "m" stands for mixed. Type m nodes are the type p nodes owning part of the broadcasting features.
- Type h nodes (h-node): "h" stands for hybrid. Type h nodes are type b nodes owning the "peer-to-peer" communicating mechanism.

## 4.3.6 Configuring DHCP Self-Defined Options for the Address Pool of the VLANIF Interface

### Context

 **NOTE**

Configuring DHCP self-defined options is optional. Services, such as DNS on the client, NETBIOS and IP lease cannot be configured through the **option code** command but through the related command described above.

Do as follows on the S-switch:

## Procedure

### Step 1 Run:

```
system-view
```

The system view is displayed.

### Step 2 Run:

```
dhcp server option code { ascii ascii-string | hex hex-string | ip-address ip-  
address <1-8> } { vlan { vlan-id1 [ to vlan-id2 ] } <1-10> }
```

The DHCP self-defined options are configured.

The DHCP self-defined options are optional. You can configure it when needed.

----End

## Postrequisite

The Option field in DHCP packets carries the control information and parameters that are not defined in some common protocols. If the DHCP server is configured with Option, the DHCP client gets the configuration information saved in Option field of DHCP response packets.

You can add new options to the attribute list of the DHCP server by manual definition. For example,

- To configure the IP address of the log server to 10.110.204.1, run the **dhcp server option 7 ip-address 10.110.204.1** command.
- To configure the TTL of the client packet to 64, run the **dhcp server option 23 hex 40** command.



#### NOTE

Using the **option code** command, you can specify the options that need be included in the DHCP response packets.

Before using the **option code** command, you need to know the function of each option: Option 77 applies to identify user types or applications of DHCP client. Based on User Class in the Option field, the DHCP server selects proper address pool and configuration parameters. Option 77 usually is configured by the client.

## 4.3.7 Checking the Configuration

Run the following commands to check the previous configuration.

| Action   | Command  |
|--|--|
| Check the expired lease in the DHCP address pool of the specified VLANIF interface.      | <b>display dhcp server expired vlan</b> <i>vlan-id</i>   |
| Check information about the DHCP address bound to the specified VLANIF interface.        | <b>display dhcp server ip-in-use vlan</b> <i>vlan-id</i> |
| Check information about the tree-structure of DHCP address pool on the VLANIF interface. | <b>display dhcp server tree vlan</b> <i>vlan-id</i>      |

Run the **display dhcp server tree vlan** command. If the tree structure information of DHCP address pools on VLANIF interfaces, such as DNS, IP lease and Option parameters, is displayed, it means that the configuration succeeds.

```
<Quidway> display dhcp server tree vlan 2
Interface pool:
Pool name: Vlanif2
network 50.1.1.0 mask 255.255.255.0
gateway-list 50.1.1.1
expired day 1 hour 0 minute 0
```

Run the **display dhcp server ip-in-use vlan** command. If the binding information of IP address on VLANIF interfaces, such as the hardware address and the IP lease, is displayed, it means that the configuration succeeds.

```
<Quidway> display dhcp server ip-in-use vlan 2
IP address      Hardware address  Lease expiration      Type
50.1.1.12       0023-0034-0053     NOT Used              Manual
```

Run the **display dhcp server expired** command. If the expired IP address in the address pool on VLANIF interfaces is displayed, it means that the configuration succeeds.

```
<Quidway> display dhcp server expired vlan 2
IP address      Hardware address  Lease expiration      Type
```

## 4.4 Configuring the Security Function for DHCP

This section describes how to enhance the security of the DHCP service.

### 4.4.1 Establishing the Configuration Task

### 4.4.2 Starting the Detection of the Pseudo DHCP Server on a DHCP Server

### 4.4.3 Avoiding Repetitive IP Address Assignment

### 4.4.4 Saving DHCP Data

### 4.4.5 Recovering DHCP Data

### 4.4.6 Checking the Configuration

## 4.4.1 Establishing the Configuration Task

### Applicable Environment

After configuring the DHCP server, you need to configure the security function of DHCP to enhance the security.

### Pre-configuration Tasks

Before configuring the security function of DHCP, complete the DHCP server configuration.

### Data Preparation

To configure the security function of DHCP service, you need the following data.

| No. | Data   |
|-----|--|
| 1   | Interval at which ping packets are sent and the number of ping packets |
| 2   | Interval for saving the DHCP data                                      |

## 4.4.2 Starting the Detection of the Pseudo DHCP Server on a DHCP Server

### Context

If a private DHCP server exists in the network, users cannot obtain correct IP addresses and thus cannot log in to the network because this private DHCP server will interact with the DHCP client during address application. Such a private DHCP server is called a pseudo DHCP server.

Do as follows on the DHCP server:

### Procedure

**Step 1** Run:

```
system-view
```

The system view is displayed.

**Step 2** Run:

```
dhcp server detect
```

Detecting the pseudo DHCP server is enabled on the DHCP server.

By default, this function is disabled.

----End

## 4.4.3 Avoiding Repetitive IP Address Assignment

### Context

Do as follows on the DHCP server:

### Procedure

**Step 1** Run:

```
system-view
```

The system view is displayed.

**Step 2** Run:

```
dhcp server ping timeout milliseconds
```

The time for waiting the response after the ping packets is sent by the DHCP server is configured.

**Step 3** Run:

```
dhcp server ping packets number
```

The maximum number of ping packets sent by the DHCP server is configured.

By default, the maximum number of ping packets being sent is 2 and the longest waiting time for ping response packets is 500 ms.

----End

## Postrequisite

Before assigning addresses to a client, the DHCP server should detect the IP address to avoid address collision.

Using the **ping** command, you can check if there is a ping response of the address to be assigned within the specific time. If there is no response after a specific time, the DHCP server re-sends ping packets to this address until it reaches the maximum number of ping packets allowed to be sent. If there is still no response, it indicates that the IP address is not in use. In this way, it is ensured that a unique IP address is assigned to the client.

## 4.4.4 Saving DHCP Data

### Context

Do as follows on the DHCP server:

### Procedure

**Step 1** Run:

```
system-view
```

The system view is displayed.

**Step 2** Run:

```
dhcp server database enable
```

Saving the DHCP data to the Flash is enabled.

**Step 3** Run:

```
dhcp server database write-delay seconds
```

The time delay for saving the data is set.

By default, DHCP data cannot be saved to the Flash. If the function is enabled, the default interval for saving the current DHCP data is 300 seconds, and the new data overwrites the previous data.

----End

## Postrequisite

The DHCP data is saved with a fixed file name on the Flash. Normally, the IP leasing information is saved in **lease.txt** file and the address collision information is saved in **conflict.txt** file. Back up these two files to other directories because they are replaced regularly.

## 4.4.5 Recovering DHCP Data

## Context

Do as follows on the DHCP server:

## Procedure

### Step 1 Run:

```
system-view
```

The system view is displayed.

### Step 2 Run:

```
dhcp server database recover
```

DHCP data is recovered after reboot.

----End

## 4.4.6 Checking the Configuration

Run the following commands to check the previous configuration.

| Action   | Command   |
|--|---|
| View the statistics of DHCP address collisions.                  | <b>display dhcp server conflict { all   ip ip-address }</b> |
| View the storage path and file information of the DHCP database. | <b>display dhcp server database</b>                         |

Run the **display dhcp server conflict** command. If the conflicted IP address and the time when the conflict occurs are displayed, it means that the configuration succeeds.

```
<Quidway> display dhcp server conflict all
Address          Discover Time
10.110.1.2       Jan 11 2003 11:57: 7 PM
```

Run the **display dhcp server database** command. If the saved path of the DHCP data is displayed, it means that the configuration succeeds.

```
<Quidway> display dhcp server database
Status: disable
Recover from files after reboot: disable
File saving lease items: flash:/dhcp/lease.txt
File saving conflict items: flash:/dhcp/conflict.txt
Save Interval: 300 (seconds)
```

## 4.5 Configuring DHCP Relay

This section describes how to enable DHCP relay so that DHCP relay can forward DHCP requests from local clients to the DHCP server on other networks.

### 4.5.1 Establishing the Configuration Task

### 4.5.2 Enabling DHCP Relay

### 4.5.3 Assigning IP Addresses to the Client Through Relay

[4.5.4 Requesting the DHCP Server to Release IP Addresses of the Client](#)[4.5.5 Checking the Configuration](#)

## 4.5.1 Establishing the Configuration Task

### Applicable Environment

When there is no DHCP server configured on the local network, enable the DHCP relay function on the device. Thus, the DHCP relay can forward the DHCP requests from local clients to the DHCP server on the other network. That is, the interface connecting the DHCP server to the DHCP relay must not be configured with any interface address pool.

**NOTE**

The relay between the server and the client cannot exceed four. Otherwise, the DHCP packet is discarded.

### Pre-configuration Tasks

Before configuring the DHCP relay, complete the following tasks:

- Configuring the DHCP server
- Configuring the routes from the local device to the DHCP server

### Data Preparation

To configure the DHCP relay, you need the following data.

| No. | Data  |
|-----|---|
| 1   | IP address of the DHCP server                               |
| 2   | Number of the VLAN to be enabled the DHCP relay function    |
| 3   | IP address to be released and the corresponding MAC address |

## 4.5.2 Enabling DHCP Relay

### Context

Each interface can be configured with up to 20 IP relay addresses.

Do as follows on the S-switch acting as the DHCP relay:

### Procedure

- Enabling DHCP relay in the interface view

1. Run:

```
system-view
```

The system view is displayed.

2. Run:

```
interface vlanif VLANIF interface number
```

The interface view is displayed.

3. Run:

```
ip address ip-address { mask | mask-length }
```

The IP address of the interface is configured.

 **NOTE**

This IP address must be in the same network segment with the IP addresses in the address pool on the DHCP server.

4. Run:

```
ip relay address ip-address
```

The relay IP address of the interface is added.

The relay IP address indicates the IP address of the DHCP server specified on the DHCP relay device. After the DHCP relay is enabled on one interface, the DHCP server is specified by the IP relay address. The DHCP broadcast packets received on the interface are sent to the specified DHCP server.

- Enabling DHCP Relay in the system view

1. Run:

```
system-view
```

The system view is displayed.

2. Run:

```
ip relay address ip-address vlan vlan-id
```

The IP relay address of the VLANIF interface is added.

----End

## Postrequisite

Because the DHCP client may send broadcast packets during DHCP configuration, the interface where IP relay is enabled should support the broadcast mode.

## 4.5.3 Assigning IP Addresses to the Client Through Relay

### Context

Do as follows on the S-switch acting as the DHCP relay:

### Procedure

- Assigning IP addresses to the client of the current interface

1. Run:

```
system-view
```

The system view is displayed.

2. Run:

```
interface vlanif VLANIF interface number
```

The VLANIF interface view is displayed.

3. Run:

```
dhcp select relay
```

IP addresses are assigned through DHCP relay.

- Assigning IP addresses to the clients of the VLAN

1. Run:

```
system-view
```

The system view is displayed.

2. Run:

```
dhcp select relay vlan { vlan-id1 [ to vlan-id2 ] }<1-10>
```

IP addresses are assigned through DHCP relay.

----End

## 4.5.4 Requesting the DHCP Server to Release IP Addresses of the Client

### Context

Do as follows on the S-switch acting as the DHCP relay:

### Procedure

- Requesting all the DHCP servers to release an IP address
  1. Run:

```
system-view
```

The system view is displayed.
  2. Run:

```
dhcp relay release client-ip-address mac-address
```

The DHCP servers are required to release the IP address.
- Requesting the specified DHCP server to release an IP address
  1. Run:

```
system-view
```

The system view is displayed.
  2. Run:

```
dhcp relay release client-ip-address mac-address server-ip-address
```

The specified DHCP server is required to release the IP address.
- Requesting the DHCP server connected with the interface to release an IP address
  1. Run:

```
system-view
```

The system view is displayed.
  2. Run:

```
interface vlanif VLANIF interface number
```

The VLANIF interface view is displayed.

3. Run:

```
dhcp relay release client-ip-address mac-address [ server-ip-address ]
```

The DHCP server connected with the interface on the DHCP relay is required to release the IP address.

----End

## 4.5.5 Checking the Configuration

Run the flowing commands to check the previous configuration.

| Action   | Command   |
|--|---|
| Check the related statistics about the DHCP relay. | <b>display dhcp relay statistics</b>                  |
| Check the DHCP relay address of the interface.     | <b>display dhcp relay address vlan</b> <i>vlan-id</i> |

Run the **display dhcp relay address** command. If there are available DHCP relay addresses and related configuration information, it means that the configuration succeeds.

```
<Quidway> display dhcp relay address vlan 1
** Vlanif1 DHCP Relay Address **
Relay Address [0] : 3.3.3.3
```

Run the **display dhcp relay statistics** command. If statistics of DHCP relay, such as the number of wrong DHCP packets and the number of various DHCP packet, is displayed, it means that the configuration succeeds.

```
<Quidway> display dhcp relay statistics
Bad Packets received: 0
DHCP packets received from clients: 0
  DHCP DISCOVER packets received: 0
  DHCP REQUEST packets received: 0
  DHCP INFORM packets received: 0
  DHCP DECLINE packets received: 0
DHCP packets received from servers: 0
  DHCP OFFER packets received: 0
  DHCP ACK packets received: 0
  DHCP NAK packets received: 0
DHCP packets sent to servers: 0
DHCP packets sent to clients: 0
  Unicast packets sent to clients: 0
  Broadcast packets sent to clients: 0
```

## 4.6 Maintaining DHCP

This section describes how to clear the statistics about DHCP and debug DHCP.

### 4.6.1 Resetting DHCP

### 4.6.2 Releasing Conflicting IP Addresses

### 4.6.3 Clearing DHCP Statistics

### 4.6.4 Monitoring Network Operation Status

#### 4.6.5 Debugging DHCP

### 4.6.1 Resetting DHCP



#### CAUTION

Resetting DHCP binding through the **reset dhcp** command interrupts the operation of the DHCP server.

To reset DHCP, run the following **reset** commands in the user view.

| Action   | Command  |
|--|--|
| Reset information about the binding of the specified IP address.                                 | <b>reset dhcp server ip-in-use ip</b> <i>ip-address</i>      |
| Reset information about the dynamic address bindings of the global address pool.                 | <b>reset dhcp server ip-in-use pool</b> [ <i>pool-name</i> ] |
| Reset information about dynamic IP address bindings on the address pool of the VLANIF interface. | <b>reset dhcp server ip-in-use vlan</b> <i>vlan-id</i>       |
| Reset information about the dynamic address bindings of all the address pools.                   | <b>reset dhcp server ip-in-use all</b>                       |

### 4.6.2 Releasing Conflicting IP Addresses



#### CAUTION

After the conflicting IP addresses are released, they can be reallocated by the DHCP server.

To release the conflicting IP addresses, run the following **reset** commands in the user view.

| Action  | Command  |
|---|--|
| Release the conflicting IP addresses in the specified address pool. | <b>reset dhcp server conflict ip</b> <i>ip-address</i> |
| Release all conflicting IP addresses.                               | <b>reset dhcp server conflict all</b>                  |

The DHCP server detects the conflicting IP addresses through the **ping** command while the DHCP client detects the conflicting IP address through sending ARP packets.

### 4.6.3 Clearing DHCP Statistics



## CAUTION

DHCP statistics cannot be restored after you clear it. So, confirm the action before you use the command.

To clear the DHCP statistics, run the following **reset** commands.

| Action                                      | Command                             |
|---|-------------------------------------|
| Reset the statistics about the DHCP server. | <b>reset dhcp server statistics</b> |
| Reset the statistics about the DHCP relay.  | <b>reset dhcp relay statistics</b>  |

## 4.6.4 Monitoring Network Operation Status

To obtain configuration about DHCP in routine maintenance, run the following commands.

| Action   | Command   |
|--|---|
| View information about available IP addresses in the DHCP address pool.                | <b>display dhcp server free-ip</b>  |
| View information about the IP addresses with expired leases in the DHCP address pool.  | <b>display dhcp server expired { all   ip <i>ip-address</i>   pool [ <i>pool-name</i> ]   vlan <i>vlan-id</i> }</b>   |
| View information about address bindings.   | <b>display dhcp server ip-in-use { all   ip <i>ip-address</i>   pool [ <i>pool-name</i> ]   vlan <i>vlan-id</i> }</b> |
| View statistics about the DHCP server.   | <b>display dhcp server statistics</b>   |
| View information about the tree structure of the DHCP address pool.                    | <b>display dhcp server tree { all   pool [ <i>pool-name</i> ]   vlan <i>vlan-id</i> }</b>                             |
| View information about the conflict addresses in the DHCP address pool.                | <b>display dhcp server conflict { all   ip <i>ip-address</i> }</b>  |
| View the path at which DHCP database is saved and file information about the database. | <b>display dhcp server database</b>   |
| View configurations about the DHCP relay address.                                      | <b>display dhcp relay address vlan <i>vlan-id</i></b>   |

## 4.6.5 Debugging DHCP

**CAUTION**

Debugging affects the performance of the system. So after debugging, run the **undo debugging all** command to disable it immediately.

Run the following **debug** commands in the user view to debug DHCP and locate the fault.

| Action                        | Command   |
|-------------------------------|---|
| Enable DHCP server debugging. | <b>debugging dhcp server</b> { <b>all</b>   <b>error</b>   <b>event</b>   <b>packet</b> }   |
| Enable DHCP relay debugging.  | <b>debugging dhcp relay</b> { <b>all</b>   <b>error</b>   <b>event</b>   <b>packet</b> [ <b>client mac</b> <i>mac-address</i> ] } |

## 4.7 Configuration Examples

This section provides several configuration examples of the DHCP server and DHCP relay.

[4.7.1 Example for Configuring the Global Address Pool-based DHCP Server](#)

[4.7.2 Example for Configuring the VLANIF Interface Address Pool-based DHCP Server](#)

[4.7.3 Example for Configuring DHCP Relay](#)

### 4.7.1 Example for Configuring the Global Address Pool-based DHCP Server

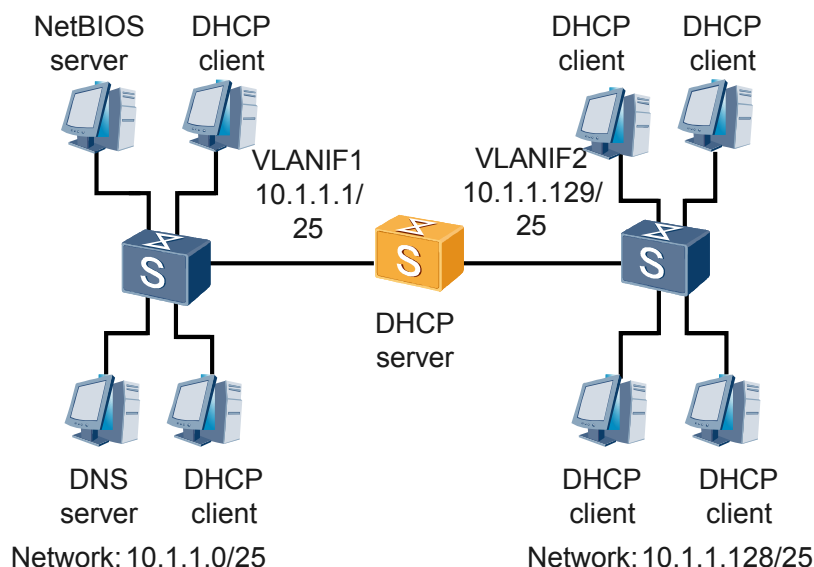
#### Networking Requirements

As shown in [Figure 4-1](#), a DHCP server dynamically assigns the IP addresses to a client in the same network segment. The address pool segment 10.1.1.0/24 is divided into two segments: 10.1.1.0/25 and 10.1.1.128/25. The IP addresses of the two VLANIF interfaces on the DHCP server are 10.1.1.1/25 and 10.1.1.129/25.

The IP lease of the segment 10.1.1.0/25 is 10 days and 12 hours, with domain name as huawei.com, DNS address as 10.1.1.2, egress device address as 10.1.1.126 and without the NetBIOS address.

The IP lease of the segment 10.1.1.128/25 is 5 days, with domain name as huawei.com, DNS address as 10.1.1.2, egress device address as 10.1.1.254, and NetBIOS address as 10.1.1.4.

**Figure 4-1** Networking diagram of the DHCP server and the client that are in the same network segment



## Configuration Roadmap

The configuration roadmap is as follows:

1. Enable DHCP.
2. Configure the IP addresses that need not be assigned automatically, such as IP addresses of the DNS server, the NetBIOS server and the egress gateway.
3. Configure an address pool, including the address range and the domain name, and configure the IP address of the DNS server.
4. Configure related attributes for the address pool, such as the address range, the egress gateway, the IP address of the NetBIOS server and the IP lease.

This example covers the configurations of three address pools. Address pool 0 is configured with the common attribute of all client; address pool 1 and address pool 2 are configured with different attributes of various clients.

In this example, you can configure only address pool 1 and address pool 2. They cannot adopt configurations of the root address pool. You need to configure attributes for them respectively.

## Data Preparation

To complete the configuration, you need the following data:

- IP address that need not be assigned automatically
- Address pool number

## Configuration Procedure

1. Configure the DHCP server.  
# Enable DHCP on the device.

```
<Quidway> system-view
[Quidway] sysname S-switch
[S-switch] dhcp enable
```

# Configure the IP addresses that do not participate in auto-allocation, including addresses of the DNS server, the NetBIOS server and the egress gateway.

```
[S-switch] dhcp server forbidden-ip 10.1.1.2
[S-switch] dhcp server forbidden-ip 10.1.1.4
[S-switch] dhcp server forbidden-ip 10.1.1.126
[S-switch] dhcp server forbidden-ip 10.1.1.254
```

# Configure general attributes of DHCP address pool 0, including the address pool range, domain name and the IP address of the DNS server.

```
[S-switch] dhcp server ip-pool 0
[S-switch-dhcp-0] network 10.1.1.0 mask 255.255.255.0
[S-switch-dhcp-0] domain-name huawei.com
[S-switch-dhcp-0] dns-list 10.1.1.2
[S-switch-dhcp-0] quit
```

# Configure attributes of DHCP address pool 1, including the address pool range, egress gateway and the IP lease.

```
[S-switch] dhcp server ip-pool 1
[S-switch-dhcp-1] network 10.1.1.0 mask 255.255.255.128
[S-switch-dhcp-1] expired day 10 hour 12
[S-switch-dhcp-1] gateway-list 10.1.1.126
[S-switch-dhcp-1] quit
```

# Configure attributes of DHCP address pool 2, including the address pool range, egress gateway, the IP address of the NetBIOS server and the IP lease.

```
[S-switch] dhcp server ip-pool 2
[S-switch-dhcp-2] network 10.1.1.128 mask 255.255.255.128
[S-switch-dhcp-2] expired day 5
[S-switch-dhcp-2] nbns-list 10.1.1.4
[S-switch-dhcp-2] gateway-list 10.1.1.254
[S-switch-dhcp-2] quit
```

# Configure the clients of the VLANIF1 to obtain their IP addresses from the global address pool.

```
[S-switch] interface vlanif 1
[S-switch-Vlanif1] ip address 10.1.1.1 255.255.255.128
[S-switch-Vlanif1] dhcp select global
[S-switch-Vlanif1] quit
```

# Configure the clients of the VLANIF2 to obtain their IP addresses from the global address pool.

```
[S-switch] interface vlanif 2
[S-switch-Vlanif2] ip address 10.1.1.129 255.255.255.128
[S-switch-Vlanif2] dhcp select global
[S-switch-Vlanif2] quit
```

## 2. Verify the configuration.

After the configuration, run the **display dhcp server tree** command on the DHCP server. If the tree structure information of DHCP address pools, including DNS, IP lease, and Option parameters, is displayed, it means that the configuration succeeds.

```
[S-switch] display dhcp server tree all
Global pool:
Pool name: 0
Child node:1
  network 10.1.1.0 mask 255.255.255.0
  dns-list 10.1.1.2
  domain-name huawei.com
  expired day 1 hour 0 minute 0
Pool name: 1
Parent node:0
Sibling node:2
  network 10.1.1.0 mask 255.255.255.128
```

```
gateway-list 10.1.1.126
dns-list 10.1.1.2
domain-name huawei.com
expired day 10 hour 12 minute 0
Pool name: 2
Parent node:0
PrevSibling node:1
network 10.1.1.128 mask 255.255.255.128
gateway-list 10.1.1.254
dns-list 10.1.1.2
domain-name huawei.com
nbns-list 10.1.1.4
expired day 5 hour 0 minute 0
```

## Configuration File

The configuration file of S-switch is as follows:

```
#
 sysname S-switch
#
dhcp server ip-pool 0
 network 10.1.1.0 mask 255.255.255.0
 dns-list 10.1.1.2
 domain-name huawei.com
#
dhcp server ip-pool 1
 network 10.1.1.0 mask 255.255.255.128
 gateway-list 10.1.1.126
 expired day 10 hour 12
#
dhcp server ip-pool 2
 network 10.1.1.128 mask 255.255.255.128
 gateway-list 10.1.1.254
 nbns-list 10.1.1.4
 expired day 5
#
interface Vlanif1
 ip address 10.1.1.1 255.255.255.128
#
interface Vlanif2
 ip address 10.1.1.129 255.255.255.128
#
dhcp server forbidden-ip 10.1.1.2
dhcp server forbidden-ip 10.1.1.4
dhcp server forbidden-ip 10.1.1.126
dhcp server forbidden-ip 10.1.1.254
#
 dhcp enable
#
return
```

### NOTE

By default, IP addresses in the global address pool are assigned. So, the configuration file does not contain the **dhcp select global** command.

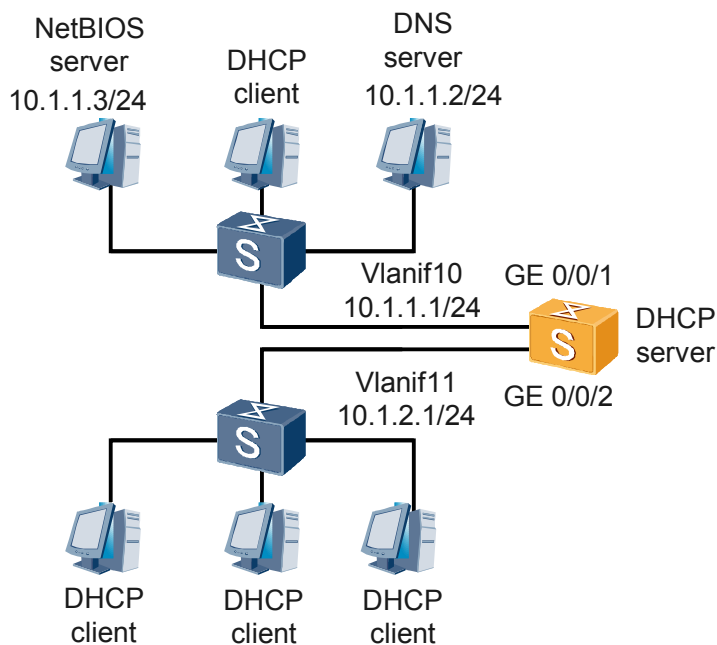
## 4.7.2 Example for Configuring the VLANIF Interface Address Pool-based DHCP Server

### Networking Requirements

**Figure 4-2** shows the diagram of applying the VLANIF-interface-based address pool to the device that supports switched Ethernet interfaces. The Ethernet interface cannot be configured

with an IP address, so you need to create a VLANIF interface and configure a DHCP address pool on it to assign IP addresses.

**Figure 4-2** Networking diagram of the DHCP server based on the address pool on the VLANIF interface



## Configuration Roadmap

The configuration roadmap is as follows:

1. Enable DHCP.
2. Configure the IP addresses that need not be assigned automatically, such as IP addresses of the DNS server, IP addresses of the NetBIOS server.
3. Create VLANIF interfaces and configure IP addresses for them.
4. Enable the address pool that is based on the VLANIF interface.
5. Configure related attributes for the address pool, such as the domain name, IP addresses of the NetBIOS server and the DNS server, and the IP lease.

## Data Preparation

To complete the configuration, you need the following data:

- IP address that need not be assigned automatically
- Address pool number

## Configuration Procedure

1. Configure the DHCP server.  
# Enable DHCP on the device.

```
<Quidway> system-view
[Quidway] sysname S-switch
[S-switch] dhcp enable

# Configure the IP addresses that do not participate in auto-allocation, including IP
addresses of the DNS server and NetBIOS server.

[S-switch] dhcp server forbidden-ip 10.1.1.2
[S-switch] dhcp server forbidden-ip 10.1.1.3

# Create a VLAN.

[S-switch] vlan 10
[S-switch-vlan10] quit
[S-switch] vlan 11
[S-switch-vlan11] quit

# Configure attributes for the switched Ethernet interface and join the interface to a VLAN.

[S-switch] interface gigabitethernet 0/0/1
[S-switch-GigabitEthernet0/0/1] port default vlan 10
[S-switch-GigabitEthernet0/0/1] quit
[S-switch] interface gigabitethernet 0/0/2
[S-switch-GigabitEthernet0/0/2] port default vlan 11
[S-switch-GigabitEthernet0/0/2] quit

# Create a VLANIF interface and configure an IP address for the VLANIF interface.

[S-switch] interface vlanif 10
[S-switch-Vlanif10] ip address 10.1.1.1 24
[S-switch-Vlanif10] quit
[S-switch] interface vlanif 11
[S-switch-Vlanif11] ip address 10.1.2.1 24
[S-switch-Vlanif11] quit

# Enable the address pool on the VLANIF interface.

[S-switch] dhcp select interface vlan 10 to 11

# Configure the domain name of the address pool and IP addresses of the DNS server and
the NetBIOS server.

[S-switch] dhcp server domain-name huawei.com vlan 10 to 11
[S-switch] dhcp server dns-list 10.1.1.2 vlan 10 to 11
[S-switch] dhcp server nbns-list 10.1.1.3 vlan 10 to 11
[S-switch] dhcp server netbios-type b-node vlan 10 to 11

# Configure the IP lease.

[S-switch] dhcp server expired day 10 hour 12 vlan 10 to 11
```

## 2. Verify the configuration.

After the configuration, run the **display dhcp server tree** command on the DHCP server. If the tree structure information of DHCP address pools, including DNS, IP lease, and Option parameters, is displayed, it means that the configuration succeeds.

```
[S-switch] display dhcp server tree all
Interface pool:
Pool name: Vlanif10
network 10.1.1.0 mask 255.255.255.0
gateway-list 10.1.1.1
dns-list 10.1.1.2
domain-name huawei.com
nbns-list 10.1.1.3
netbios-type b-node
expired day 10 hour 12 minute 0
Pool name: Vlanif11
network 10.1.2.0 mask 255.255.255.0
gateway-list 10.1.2.1
dns-list 10.1.1.2
domain-name huawei.com
nbns-list 10.1.1.3
netbios-type b-node
expired day 10 hour 12 minute 0
```

## Configuration Files

The configuration file of S-switch is as follows:

```
#
sysname S-switch
#
vlan batch 10 to 11
#
interface Vlanif10
ip address 10.1.1.1 255.255.255.0
dhcp select interface
dhcp server dns-list 10.1.1.2
dhcp server domain-name huawei.com
dhcp server nbns-list 10.1.1.3
dhcp server netbios-type b-node
dhcp server expired day 10 hour 12
#
interface Vlanif11
ip address 10.1.2.1 255.255.255.0
dhcp select interface
dhcp server dns-list 10.1.1.2
dhcp server domain-name huawei.com
dhcp server nbns-list 10.1.1.3
dhcp server netbios-type b-node
dhcp server expired day 10 hour 12
#
interface gigabitEthernet0/0/1
port default vlan 10
#
interface gigabitEthernet0/0/2
port default vlan 11
#
dhcp server forbidden-ip 10.1.1.2
dhcp server forbidden-ip 10.1.1.3
#
dhcp enable
#
return
```

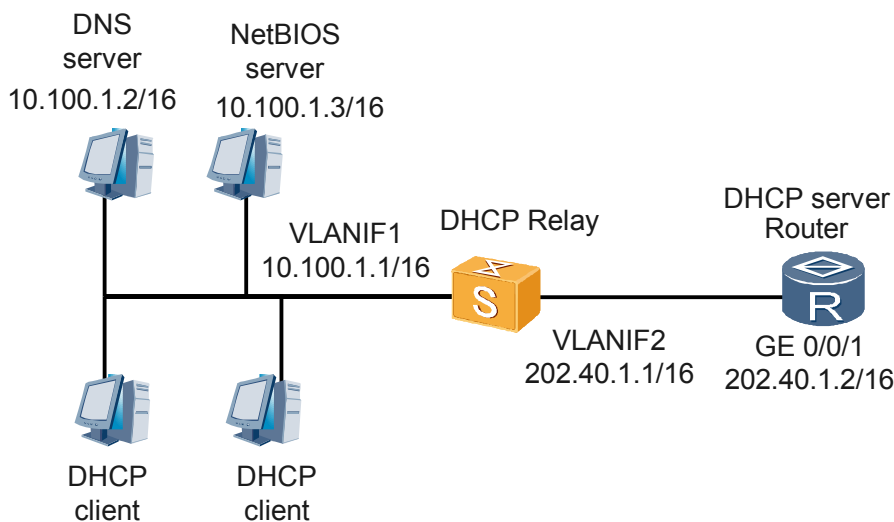
### 4.7.3 Example for Configuring DHCP Relay

#### Networking Requirements

As shown in [Figure 4-3](#), the DHCP client is in the network segment 10.100.0.0/16, while the DHCP server is in the network segment 202.40.0.0/16. A DHCP relay device is needed to relay DHCP packets so that the DHCP client obtains the IP addresses from the DHCP server.

The DHCP server is assigned with an address pool in the network segment 10.100.0.0/16. The IP address of the DNS server is 10.100.1.2/16, the IP address of the NetBIOS server is 10.100.1.3/16, and the IP address of the egress gateway is 10.100.1.4. On the DHCP server, the routing table must contain at least one reachable a route to the network segment 10.110.0.0.

**Figure 4-3** Networking diagram for configuring DHCP relay



## Configuration Roadmap

The configuration roadmap is as follows:

1. Enable DHCP on S-switch that acts as the DHCP relay.
2. Configure the IP address for interface VLANIF2.
3. Configure the IP relay address for VLANIF1 and enable DHCP relay on VLANIF1.
4. Configure a route from the DHCP server to the network segment 10.100.0.0/16.
5. Enable DHCP on the Router.
6. Configure the clients attached to GE 0/0/1 to obtain IP addresses through the global address pool.
7. Configure a global address pool on the Router.

## Data Preparation

To complement the configuration, you need the following data:

- IP address of the interface that need to be enabled with DHCP relay
- IP address of the DHCP server

## Configuration Procedure

1. Configure the DHCP relay.

# Enable DHCP on the device.

```
<Quidway> system-view
[Quidway] sysname S-switch
[S-switch] dhcp enable
```

# Configure an IP address for VLANIF2.

```
[S-switch] interface vlanif 2
[S-switch-Vlanif2] ip address 202.40.1.1 255.255.0.0
[S-switch-Vlanif2] quit
```

# Enter the view of the interface that needs to be enabled with DHCP relay. Configure the IP address and mask of the interface, which should be in the same network segment with that of the DHCP client.

```
[S-switch] interface vlanif 1
[S-switch-Vlanif1] ip address 10.100.1.1 255.255.0.0
[S-switch-Vlanif1] ip relay address 202.40.1.2
[S-switch-Vlanif1] dhcp select relay
[S-switch-Vlanif1] quit
```

## 2. Configure the DHCP server.

# On the Router, configure routes to VLANIF1 that connects S-switch and its client.

```
<Quidway> system-view
[Quidway] sysname Router
[Router] ip route-static 10.100.0.0 255.255.0.0 202.40.1.1
```

# Enable DHCP.

```
[Router] dhcp enable
```

# Configure the clients of GE 0/0/1 to obtain the IP addresses from the global address pool.

```
[Router] interface GigabitEthernet 0/0/1
[Router-GigabitEthernet 0/0/1] ip address 202.40.1.2 255.255.0.0
[Router-GigabitEthernet 0/0/1] dhcp select global
[Router-GigabitEthernet 0/0/1] quit
```

# Configure the IP addresses that do not participate in auto-allocation, including IP addresses of the DNS server, the NetBIOS server and the egress gateway.

```
[Router] dhcp server forbidden-ip 10.100.1.2
[Router] dhcp server forbidden-ip 10.100.1.3
[Router] dhcp server forbidden-ip 10.100.1.4
```

# Configure attributes of DHCP address pool 1, including the address pool range, domain name, egress gateway, the IP address of the DNS server and IP lease.

```
[Router] dhcp server ip-pool 1
[Router-dhcp-1] network 10.100.0.0 mask 255.255.0.0
[Router-dhcp-1] domain-name huawei.com
[Router-dhcp-1] dns-list 10.100.1.2
[Router-dhcp-1] nbns-list 10.100.1.3
[Router-dhcp-1] gateway-list 10.100.1.4
[Router-dhcp-1] expired day 10 hour 12
[Router-dhcp-1] quit
```

## 3. Verify the configuration.

Run the **display dhcp server tree** command on the DHCP server. If the tree structure information of DHCP address pools, including DNS, IP lease, and Option parameters, is displayed, it means that the configuration succeeds.

```
[Router] display dhcp server tree all
Global pool:
Pool name: 1
network 10.100.0.0 mask 255.255.0.0
gateway-list 10.100.1.4
dns-list 10.100.1.2
domain-name huawei.com
nbns-list 10.100.1.3
expired day 10 hour 12 minute 0
```

Run the **display dhcp relay address vlan 1** command on the DHCP relay device to view configurations of the relay IP address.

```
[S-switch] display dhcp relay address vlan 1
** Vlanif1 DHCP Relay Address **
Relay Address [0] : 202.40.1.2
```

## Configuration Files

- Configuration file of S-switch

```
#
 sysname S-switch
#
interface Vlanif1
 ip address 10.100.1.1 255.255.0.0
 ip relay address 202.40.1.2
 dhcp select relay
#
interface Vlanif2
 ip address 202.40.1.1 255.255.0.0
#
return
```

- Configuration file of the Router

```
#
 sysname Router
#
dhcp server ip-pool 1
 network 10.100.0.0 mask 255.255.0.0
 gateway-list 10.100.1.4
 dns-list 10.100.1.2
 domain-name huawei.com
 nbns-list 10.100.1.3
 expired day 10 hour 12
#
interface GigabitEthernet 0/0/1
 ip address 202.40.1.2 255.255.0.0
#
dhcp server forbidden-ip 10.100.1.2
dhcp server forbidden-ip 10.100.1.3
dhcp server forbidden-ip 10.100.1.4
#
ip route-static 10.100.0.0 255.255.0.0 202.40.1.1
#
return
```



# 5 IP Performance Configuration

---

## About This Chapter

This chapter describes the parameters and function required for IP performance optimization and provides procedures and examples for optimizing IP performance.

### [5.1 Overview](#)

This section describes the parameters and concepts concerning IP performance.

### [5.2 Improving IP Performance](#)

This section describes how to enhance the performance of a specified network through setting some IP parameters.

### [5.3 Maintaining IP Performance](#)

This section describes how to clear IP/TCP/UDP statistics and debug IP/TCP/UDP.

### [5.4 Configuration Examples](#)

This section provides several configuration examples of the IP performance.

## 5.1 Overview

This section describes the parameters and concepts concerning IP performance.

### 5.1.1 Introduction to IP Performance

#### 5.1.2 IP Performance Supported by the S-switch

#### 5.1.3 Update History

### 5.1.1 Introduction to IP Performance

IP performance optimization should be performed on the basis of configurations of some parameters and enablement of related functions, for example, ICMP function, and TCP attributes.

Internet Control Message Protocol (ICMP) messages are used by either the IP layer or the higher layer protocol (TCP or UDP). ICMP communicates error messages or other conditions that require attention.

### 5.1.2 IP Performance Supported by the S-switch

#### ICMP

- **ICMP Host Unreachable Messages**

When forwarding packets, the device discards the packets and returns an ICMP host unreachable message to the source to notify that the source must stop sending packets to this destination if the device encounters the following situations:

  - There is no route to the destination.
  - The packet is not for itself.
- **ICMP Redirection Messages**

During packet forwarding, if the device finds the following situations, the device needs to send an ICMP redirection message to the source device and notices the host to reselect a correct device to forward packets.

  - The interfaces to receive and forward packets are the same.
  - The selected route is not created or modified by the ICMP redirection packet.
  - The selected route is not the route destined for the destination 0.0.0.0.
  - The subnet mask bit of the source address is the same as that of the outgoing interface.
- **ICMP Packet Sending Switches**

In normal circumstance, ICMP host unreachable and redirection messages can ensure normal packet transmission. However, when devices encounter the preceding conditions frequently, network traffic becomes heavy because devices send a large number of ICMP messages. This increases the traffic burden. In the case of malicious attacks, network congestion becomes worse.

To solve this problem, two control switches are added on the outgoing interface of ICMP messages. These two switches are used to respectively enable or disable the sending of ICMP host unreachable or redirection messages. If these two switches are disabled, the

device does not send out these two types of packets. This can reduce the traffic burden and protect the network from malicious attacks.

## Broadcast Packet Forwarding

Broadcast packet forwarding is used to control whether broadcast packets are forwarded on a specified interface. Run the **ip forward-broadcast** command on an interface. For the broadcast packets that are not generated by the local host, this interface sends the broadcast packets to the local host before forwarding them.

When forwarding broadcast packets is enabled, the ACL rules can be specified. The interface forwards only the broadcast packets that match the ACL. It sends back the broadcast packets that do not match the ACL to the host without forwarding them.

S-switch generally do not forward directional broadcast packets. In some cases, however, you may require the device to forward directional broadcast packets. Thus, you can run the **ip forward-broadcast** command to enable an interface to forward directional broadcast packets. This makes the networking to be flexible.

### 5.1.3 Update History

| Version         | Revision                   |
|-----------------|----------------------------|
| V100R002C01B050 | This is the first release. |

## 5.2 Improving IP Performance

This section describes how to enhance the performance of a specified network through setting some IP parameters.

[5.2.1 Establishing the Configuration Task](#)

[5.2.2 Verifying the Source IP Address](#)

[5.2.3 Forwarding Broadcast Packets](#)

[5.2.4 Configuring ICMP Attributes](#)

[5.2.5 Configuring TCP Attributes](#)

[5.2.6 Checking the Configuration](#)

### 5.2.1 Establishing the Configuration Task

#### Applicable Environment

In some special network environments, you must adjust the IP parameters to achieve the best performance. Improving IP performance involves configurations of a series of parameters.

#### Pre-configuration Tasks

Before improving IP performance, complete the following tasks:

- Configuring the physical parameters for related interfaces and ensuring that the status of the physical layer of the interface is Up
- Configuring the link layer protocol for related interfaces and ensuring that the status of the link layer protocol on the interface is Up
- Configuring the IP addresses for related interfaces
- Configuring the ACL

## Data Preparation

To improve IP performance, you need the following data.

| No. | Data   |
|-----|--|
| 1   | Number of the interface  |
| 2   | Number of the interface which needs source address verification  |
| 3   | Number of the interface which needs to forward broadcast packets and ACL number which is used to specify the broadcast packets |
| 4   | Number of the interface which needs to configure ICMP host-unreachable   |
| 5   | SYN-WAIT timer, FIN-WAIT timer, receiving and sending buffer size of the socket  |

## 5.2.2 Verifying the Source IP Address

### Context

Do as follows on the S-switch:

### Procedure

**Step 1** Run:

```
system-view
```

The system view is displayed.

**Step 2** Run:

```
interface vlanif vlan interface number
```

The interface view is displayed.

**Step 3** Run:

```
ip verify source-address
```

The source IP address verification is enabled on the interface.

By default, the function is disabled on all interfaces.

----End

## 5.2.3 Forwarding Broadcast Packets

## Context

Do as follows on the S-switch:

## Procedure

**Step 1** Run:

```
system-view
```

The system view is displayed.

**Step 2** Run:

```
interface vlanif vlan interface number
```

The interface view is displayed.

**Step 3** Run:

```
ip forward-broadcast [ acl acl-number ]
```

The interface is configured to forward broadcast packets.

By default, broadcast packets are not forwarded by any interface.

----End

## 5.2.4 Configuring ICMP Attributes

### Context

By default, sending ICMP redirection packets and unreachable packets is enabled.



### CAUTION

- If the transmission of ICMP redirection messages is disabled, the device no longer sends the ICMP redirection message.
  - If the transmission of ICMP host unreachable messages is disabled, the device no longer sends the ICMP host unreachable message.
- 

Do as follows on the S-switch:

## Procedure

**Step 1** Run:

```
system-view
```

The system view is displayed.

**Step 2** Run:

```
interface interface-type interface-number
```

The interface view is displayed.

**Step 3** Run:

```
icmp host-unreachable send
```

Sending ICMP host unreachable packets is enabled.

----End

## 5.2.5 Configuring TCP Attributes

### Context

The TCP attributes that can be configured include:

- The SYN-Wait timer: On sending SYN packets, the TCP starts the SYN-Wait timer. If response packets are not received before the SYN-Wait timer timeout, the TCP connection is terminated. The SYN-Wait timer timeout ranges from 2 seconds to 600 seconds, and the default value is 75 seconds.
- The FIN-Wait timer: When the TCP connection status turns from FIN\_WAIT\_1 to FIN\_WAIT\_2, the FIN-Wait timer starts. If FIN packets are not received before the FIN-Wait timer timeout, the TCP connection is terminated. The FIN-Wait timer timeout ranges from 76 seconds to 3600 seconds, and the default value is 675 seconds.
- The receiving and sending *window-size* of the connection-oriented socket: It ranges from 1K bytes to 32K bytes, and the default value is 8K bytes.

If an attribute of TCP is configured for many times in the system view, only the last configuration takes effect.

Do as follows on the S-switch:

### Procedure

**Step 1** Run:

```
system-view
```

The system view is displayed.

**Step 2** Run:

```
tcp timer syn-timeout interval
```

The SYN-Wait timer of setting up TCP connections is configured.

**Step 3** Run:

```
tcp timer fin-timeout interval
```

The FIN\_WAIT\_2 timer of setting TCP connections is configured.

**Step 4** Run:

```
tcp window window-size
```

The receiving/sending buffer size of the TCP socket is configured.

----End

## 5.2.6 Checking the Configuration

Run the following commands to check the pervious configuration.

| Action   | Command  |
|--|--|
| View the TCP connection status.  | <b>display tcp status</b> [ [ <i>task-id task-id</i> ] [ <i>socket-id socket-id</i> ] [ [ <i>local-ip ip-address</i> ] [ <i>local-port local-port-number</i> ] [ <i>remote-ip ip-address</i> ] [ <i>remote-port remote-port-number</i> ] ] ] |
| View the TCP traffic statistics.   | <b>display tcp statistics</b>  |
| View the UDP traffic statistics.   | <b>display udp statistics</b>  |
| View the table information of the IP layer interface.  | <b>display ip interface</b> [ <i>interface-type interface-number</i> ]<br><b>display ip interface brief</b> [ <i>interface-type</i> [ <i>interface-number</i> ] ]  |
| View the IP traffic statistics.  | <b>display ip statistics</b>   |
| View the ICMP traffic statistics.  | <b>display icmp statistics</b>   |
| View the Rawlink statistics.   | <b>display rawlink statistics</b>  |
| View the FIB table of the interface board.   | <b>display fib</b>   |
| View the filtered FIB information.   | <b>display fib acl</b> <i>acl-number</i> [ <b>verbose</b> ]  |
| View the FIB entry which matches a destination address.  | <b>display fib</b> <i>destination-address1</i> [ <i>destination-mask1</i> ] [ <b>longer</b> ] [ <b>verbose</b> ]   |
| View the FIB entry whose destination address is in the range of <i>destination-address1 destination-mask1</i> to <i>destination-address2 destination-mask2</i> . | <b>display fib</b> <i>destination-address1 destination-mask1 destination-address2 destination-mask2</i> [ <b>verbose</b> ]   |
| View the FIB entries that have passed filtering in a certain format according to the input IP prefix name.   | <b>display fib ip-prefix</b> <i>prefix-name</i> [ <b>verbose</b> ]   |
| View the FIB entries that have passed filtering in a certain format according to the input interface type and interface number.                                  | <b>display fib interface</b> <i>interface-type interface-number</i>  |
| View the FIB entries that have passed filtering in a certain format according to the input next hop address.   | <b>display fib next-hop</b> <i>ip-address</i>  |
| View the total number of FIB entries.  | <b>display fib statistics</b>  |
| View the summary of the FIB.   | <b>display fib</b> [ [ { <i>begin</i>   <i>exclude</i>   <i>include</i> } <i>regular-expression</i> ] ]  |
| View all the current socket API information.   | <b>display ip socket</b> [ <b>monitor</b> ] [ <i>task-id task-id</i> ] [ <i>sock-type sock-type</i> ]  |

Run the **display tcp status** command. If the information about the TCP connection status is displayed, it means that the configuration succeeds. For example:

```
<Quidway> display tcp status
TCPCB   Tid/SoId Local Add:port      Foreign Add:port  VPNID  State
87cc374c 36 /1      0.0.0.0:23       0.0.0.0:0        14849  Listening
869b8884 36 /3      172.16.255.6:23  192.168.31.180:1268 0      Established
36 /4      172.16.255.6:23  192.168.31.181:1486 0      Established
```

Run the **display tcp statistics** command. If the TCP traffic statistics are displayed, it means that the configuration succeeds. For example:

```
<Quidway> display tcp statistics
Received packets:
    Total: 0
    packets in sequence: 0 (0 bytes)
    window probe packets: 0, window update packets: 0
    checksum error: 0, offset error: 0, short error: 0

    duplicate packets: 0 (0 bytes), partially duplicate packets: 0 (0 bytes)
    out-of-order packets: 0 (0 bytes)
    packets of data after window: 0 (0 bytes)
    packets received after close: 0

    ACK packets: 0 (0 bytes)
    duplicate ACK packets: 0, too much ACK packets: 0

Sent packets:
    Total: 0
    urgent packets: 0
    control packets: 0 (including 0 RST)
    window probe packets: 0, window update packets: 0

    data packets: 0 (0 bytes), data packets retransmitted: 0 (0 bytes)
    ACK-only packets: 0 (0 delayed)

Retransmitted timeout: 0, connections dropped in retransmitted timeout: 0
Keep alive timeout: 0, keep alive probe: 0, Keep alive timeout, so connections d
isconnected : 0
Initiated connections: 0, accepted connections: 0, established connections: 0
Closed connections: 0 (dropped: 0, initiated dropped: 0)
Packets dropped with MD5 authentication: 0
Packets permitted with MD5 authentication: 0
```

Run the **display udp statistics** command. If the UDP traffic statistics are displayed, it means that the configuration succeeds. For example:

```
<Quidway> display udp statistics
Received packets:
    Total: 0
    checksum error: 0
    shorter than header: 0, data length larger than packet: 0
    unicast(no socket on port): 0
    broadcast/multicast(no socket on port): 0
    not delivered, input socket full: 0
    input packets missing pcb cache: 0
Sent packets:
    Total: 0
```

Run the **display ip interface** command. If the information about IP interfaces is displayed, it means that the configuration succeeds. For example:

```
<Quidway> display ip interface vlanif 1
Vlanif1 current state : DOWN
Line protocol current state : DOWN
The Maximum Transmit Unit : 1500 bytes
input packets : 0, bytes : 0, multicasts : 0
output packets : 0, bytes : 0, multicasts : 0
Directed-broadcast packets:
    received packets: 0, sent packets: 0
    forwarded packets: 0, dropped packets: 0
Internet Address is 172.18.255.1/24
```

```
Broadcast address : 172.18.255.255
TTL invalid packet number:      0
ICMP packet input number:      0
  Echo reply:                   0
  Unreachable:                  0
  Source quench:                0
  Routing redirect:             0
  Echo request:                 0
  Router advert:                0
  Router solicit:               0
  Time exceed:                  0
  IP header bad:                0
  Timestamp request:            0
  Timestamp reply:              0
  Information request:          0
  Information reply:            0
  Netmask request:              0
  Netmask reply:                0
  Unknown type:                 0
DHCP packet deal mode:  global
```

Run the **display ip statistics** command. If the IP traffic statistics are displayed, it means that the configuration succeeds. For example:

```
<Quidway> display ip statistics
Input:      sum      10153      local      10153
           bad protocol    0      bad format    0
           bad checksum    0      bad options    0
           TTL exceeded    0
Output:     forwarding    0      local      11589
           dropped        0      no route    0
Fragment:   input         0      output     0
           dropped        0
           fragmented     0      couldn't fragment 0
Reassembling:sum          0      timeouts    0
```

Run the **display icmp statistics** command. If the ICMP traffic statistics are displayed, it means that the configuration succeeds. For example:

```
<Quidway> display icmp statistics
Input: bad formats    0      bad checksum    0
      echo           4      destination unreachable 0
      source quench  0      redirects      0
      echo reply     5      parameter problem 0
      timestamp      0      information request 0
      mask requests  0      mask replies    0
      time exceeded  0
Output:echo          5      destination unreachable 0
      source quench  0      redirects      0
      echo reply     4      parameter problem 0
      timestamp      0      information reply 0
      mask requests  0      mask replies    0
      time exceeded  0
```

Run the **display rawlink statistics** command. If the Rawlink statistics are displayed, it means that the configuration succeeds. For example:

```
<Quidway> display rawlink statistics
Received packets:
  Total: 0
  ifnet is null: 0
  input packets missing pcb cache: 0
  not pass multicast: 0
  no join multicast: 0
  full sock and pstMbuf to be freed: 0
  full sock and nothing to be freed: 0
  full sock and other reason: 0
Send packets:
  Total: 0
```

Run the **display fib** command. If the brief information about the FIB is displayed, it means that the configuration succeeds. For example:

```
<Quidway> display fib
Destination/Mask  Nexthop      Flag TimeStamp      Interface  TunnelID
127.0.0.1/32     127.0.0.1    HU   t[57]           InLoop0    0x0
127.0.0.0/8      127.0.0.1    U    t[57]           InLoop0    0x0
172.16.255.6/32  127.0.0.1    HU   t[86]           InLoop0    0x0
172.16.255.4/30  172.16.255.6 U    t[86]           Vlanif2002 0x0
0.0.0.0/0        172.16.255.5 GSU   t[86]           Vlanif2002 0x0
192.168.0.0/16   172.16.255.5 GSU   t[86]           Vlanif2002 0x0
172.16.255.5/32  172.16.255.5 HLU   t[650]          GE0/0/18   0x0

<Quidway> display fib acl 2010
Route entry matched by access-list 2010:
Summary counts: 1
Destination/Mask  Nexthop      Flag TimeStamp      Interface  TunnelID
127.0.0.0/8      127.0.0.1    U    t[0]           InLoopBack0 0x0
```

## 5.3 Maintaining IP Performance

This section describes how to clear IP/TCP/UDP statistics and debug IP/TCP/UDP.

### 5.3.1 Clearing IP/TCP/UDP Statistics

#### 5.3.2 Monitoring Network Operation Status

#### 5.3.3 Debugging IP/TCP/UDP

### 5.3.1 Clearing IP/TCP/UDP Statistics



#### CAUTION

IP/TCP/UDP statistics cannot be restored after you clear it. So, confirm the action before you use the command.

To clear the IP/TCP/UDP statistics, run the following **reset** commands in the user view.

| Action                                      | Command   |
|---|---|
| Reset the IP statistics.                    | <b>reset ip statistics</b> [ <b>interface</b> <i>interface-type</i> <i>interface-number</i> ] |
| Clear information about the socket monitor. | <b>reset ip socket monitor</b>  |
| Reset the TCP traffic statistics.           | <b>reset tcp statistics</b>   |
| Reset the UDP traffic statistics.           | <b>reset udp statistics</b>   |
| Reset the Rawlink statistics.               | <b>reset rawlink statistics</b>   |

### 5.3.2 Monitoring Network Operation Status

To obtain configurations about ICMP in routine maintenance, run the following commands.

| Action  | Command  |
|---|--|
| View TCP connection status.   | <b>display tcp status</b> [ [ <b>task-id</b> <i>task-id</i> ] [ <b>socket-id</b> <i>socket-id</i> ] [ [ <b>local-ip</b> <i>ip-address</i> ] [ <b>local-port</b> <i>local-port-number</i> ] [ <b>remote-ip</b> <i>ip-address</i> ] [ <b>remote-port</b> <i>remote-port-number</i> ] ] |
| View statistics about TCP traffic.  | <b>display tcp statistics</b>  |
| View statistics about UDP traffic.  | <b>display udp statistics</b>  |
| View information about IP interfaces.   | <b>display ip interface</b> [ <i>interface-type interface-number</i> ]<br><b>display ip interface brief</b> [ <i>interface-type</i> [ <i>interface-number</i> ] ]  |
| View statistics about IP traffic.   | <b>display ip statistics</b>   |
| View statistics about ICMP traffic.   | <b>display icmp statistics</b>   |
| View statistics about Rawlink.  | <b>display rawlink statistics</b>  |
| View the FIB on the specified interface board.  | <b>display fib</b>   |
| View the FIB information selectively through filtering.   | <b>display fib acl</b> <i>acl-number</i> [ <b>verbose</b> ]  |
| Filter FIB entries by matching destination IP addresses.  | <b>display fib</b> [ <i>slot-id</i> ] <i>destination-address1</i> [ <i>desinationt-mask1</i> ] [ <b>longer</b> ] [ <b>verbose</b> ]  |
| View the FIB entries with the destination IP addresses in the range from <i>destination-address1 destination-mask1</i> to <i>destination-address2 destination-mask2</i> . | <b>display fib</b> [ <i>slot-id</i> ] <i>destination-address1 destination-mask1 destination-address2 destination-mask2</i> [ <b>verbose</b> ]  |
| View the FIB entries that have passed filtering in a certain format according to the input IP prefix name.  | <b>display fib ip-prefix</b> <i>prefix-name</i> [ <b>verbose</b> ]   |
| View the FIB entries that have passed filtering in a certain format according to the input interface type and interface number.   | <b>display fib interface</b> <i>interface-type interface-number</i>  |
| View the FIB entries that have passed filtering in a certain format according to the input next hop address.  | <b>display fib next-hop</b> <i>ip-address</i>  |
| View the total number of FIB entries.   | <b>display fib statistics</b>  |
| View brief information about the forwarding table.  | <b>display fib</b> [ [ { <b>begin</b>   <b>exclude</b>   <b>include</b> } <i>regular-expression</i> ]  |
| View information about all the socket interfaces of the system.   | <b>display ip socket</b> [ <b>monitor</b> ] [ <b>task-id</b> <i>task-id</i>   <b>sock-type</b> <i>sock-type</i> ]  |

### 5.3.3 Debugging IP/TCP/UDP



#### CAUTION

Debugging affects the performance of the system. So after debugging, run the **undo debugging all** command to disable it immediately.

Run the following **debug** commands in the user view to debug IP/TCP/UDP/RAWIP/RAWLINK and locate the fault.

| Action                                   | Command   |
|--|---|
| Enable IP packets debugging.             | <b>debugging ip packet</b> [ <b>error</b> ] [ <b>acl</b> <i>acl-number</i> ]  |
| Enable ICMP debugging.                   | <b>debugging ip icmp</b>  |
| Enable UDP packets debugging.            | <b>debugging udp packet</b> [ <b>local-ip</b> <i>ip-address</i> ] [ <b>local-port</b> <i>local-port</i> ] [ <b>remote-ip</b> <i>ip-address</i> ] [ <b>remote-port</b> <i>remote-port</i> ]<br><b>debugging udp packet</b> [ <b>task-id</b> <i>task-id</i> ] [ <b>socket-id</b> <i>socket-id</i> ]   |
| Enable TCP packets debugging.            | <b>debugging tcp packet</b> [ <b>local-ip</b> <i>ip-address</i> ] [ <b>local-port</b> <i>local-port</i> ] [ <b>remote-ip</b> <i>ip-address</i> ] [ <b>remote-port</b> <i>remote-port</i> ] [ <b>flag</b> <i>flag-number</i> ]<br><b>debugging tcp packet</b> [ <b>task-id</b> <i>task-id</i> ] [ <b>socket-id</b> <i>socket-id</i> ] [ <b>flag</b> <i>flag-number</i> ] |
| Enable TCP event debugging.              | <b>debugging tcp event</b> [ <b>local-ip</b> <i>local-address</i> ] [ <b>local-port</b> <i>local-port</i> ] [ <b>remote-ip</b> <i>remote-address</i> ] [ <b>remote-port</b> <i>remote-port</i> ]<br><b>debugging tcp event</b> [ <b>task-id</b> <i>task-id</i> ] [ <b>socket-id</b> <i>socket-id</i> ]  |
| Enable TCP MD5 authentication debugging. | <b>debugging tcp md5</b> [ <b>local-ip</b> <i>local-address</i> ] [ <b>local-port</b> <i>local-port</i> ] [ <b>remote-ip</b> <i>remote-address</i> ] [ <b>remote-port</b> <i>remote-port</i> ]<br><b>debugging tcp md5</b> [ <b>task-id</b> <i>task-id</i> ] [ <b>socket-id</b> <i>socket-id</i> ]  |
| Enable RAWIP packets debugging.          | <b>debugging rawip packet</b> [ <b>local-ip</b> <i>ip-address</i> ] [ <b>remote-ip</b> <i>ip-address</i> ] [ <b>protocol</b> <i>protocol-number</i> ] [ <b>verbose</b> <i>verbose-number</i> ]<br><b>debugging rawip packet</b> [ <b>task-id</b> <i>task-id</i> ] [ <b>socket-id</b> <i>socket-id</i> ] [ <b>verbose</b> <i>verbose-number</i> ]                        |

| Action                            | Command  |
|-----------------------------------|--|
| Enable RAWLINK packets debugging. | <b>debugging rawlink packet</b> [ <i>local-mac local-mac</i> ]<br>[ <i>remote-mac remote-mac</i> ] [ <b>verbose</b> <i>verbose-number</i> ]<br><b>debugging rawlink packet</b> [ <i>task-id task-id</i> ] [ <b>socket-id</b> <i>socket-id</i> ] [ <b>verbose</b> <i>verbose-number</i> ] |

## 5.4 Configuration Examples

This section provides several configuration examples of the IP performance.

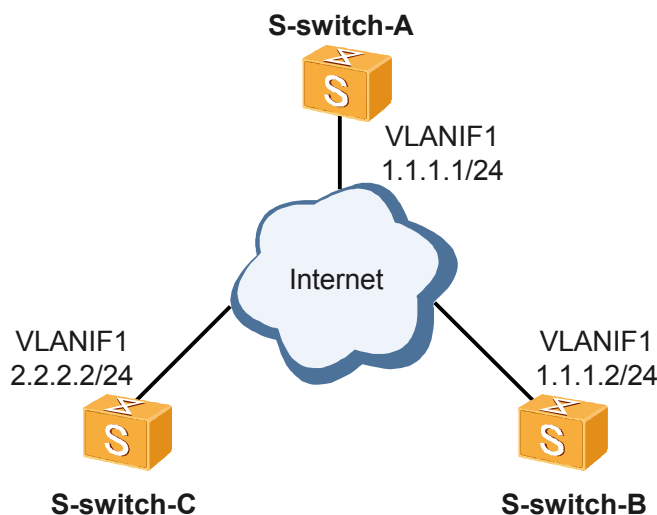
### 5.4.1 Example for Limiting Transmission of ICMP Host-Unreachable Packets

#### 5.4.1 Example for Limiting Transmission of ICMP Host-Unreachable Packets

##### Networking Requirements

As shown in [Figure 5-1](#), S-switch-A, S-switch-B and S-switch-C are connected with each other through their VLANIF to test limiting transmission of host-unreachable packets.

**Figure 5-1** Networking diagram of configuring ICMP host unreachable packets



##### Configuration Roadmap

The configuration roadmap is as follows:

1. Configure IP addresses for the interfaces on devices.
2. Configure static routes between devices that are not directly connected.

3. Enable limiting transmission of ICMP Host-unreachable packets.

## Data Preparation

To complete the configuration, you need the following data:

- Static routes between devices that are not directly connected
- IP addresses for the interfaces

## Configuration Procedure

1. Configure S-switch-A.

# Configure static routes on S-switch-A.

```
<Quidway> system-view
[Quidway] sysname S-switch-A
[S-switch-A] ip route-static 2.2.2.2 24 1.1.1.2
```

# Configure an IP address for VLANIF1.

```
[S-switch-A] interface vlanif 1
[S-switch-A-Vlanif1] ip address 1.1.1.1 24
[S-switch-A-Vlanif1] quit
```

2. Configure S-switch-B.

# Disable sending ICMP host unreachable packets on S-switch-B and configure an IP address for VLANIF1

```
<Quidway> system-view
[Quidway] sysname S-switch-B
[S-switch-B] interface vlanif 1
[S-switch-B-Vlanif1] undo icmp host-unreachable send
[S-switch-B-Vlanif1] ip address 1.1.1.2 24
[S-switch-B-Vlanif1] quit
[S-switch-B] quit
```

3. Configure S-switch-C.

# Configure an IP address for VLANIF1 on S-switch-C.

```
<Quidway> system-view
[Quidway] sysname S-switch-C
[S-switch-C] interface vlanif 1
[S-switch-C-Vlanif1] ip address 2.2.2.2 24
[S-switch-C-Vlanif1] quit
```

4. Verify the configuration.

# Enable the debugging of the ICMP packets of S-switch-B.

```
<S-switch-B> debugging ip icmp
```

# Run the **ping 2.2.2.2** command on S-switch-A. If you can view that S-switch-B does not send the host unreachable packets, it means that the configuration succeeds. For example:

```
[S-switch-A] ping 2.2.2.2
```

## Configuration Files

- Configuration file of S-switch-A

```
#
sysname S-switch-A
#
interface Vlanif1
ip address 1.1.1.1 255.255.255.0
#
ip route-static 2.2.2.0 255.255.255.0 1.1.1.2
#
```

```
return
```

- Configuration file of S-switch-B

```
#
sysname S-switch-B
#
interface Vlanif1
ip address 1.1.1.2 255.255.255.0
undo icmp host-unreachable send
#
return
```

- Configuration file of S-switch-C

```
#
sysname S-switch-C
#
interface Vlanif1
ip address 2.2.2.2 255.255.255.0
#
return
```



# 6 ACL Configuration

---

## About This Chapter

This chapter describes the fundamentals of ACL along with its types such as basic, advanced and interface based ACL. It also includes basic ACL configuration steps, along with typical examples.

### [6.1 Overview](#)

This section describes basic concepts and parameters of the Access Control List (ACL).

### [6.2 Configuring an ACL](#)

This section describes how to configure a basic ACL and an advanced ACL.

### [6.3 Maintaining an ACL](#)

This section describes how to clear operation information about an ACL.

### [6.4 Configuration Examples](#)

This section provides a configuration example of an ACL.

## 6.1 Overview

This section describes basic concepts and parameters of the Access Control List (ACL).

### [6.1.1 Introduction to ACL](#)

### [6.1.2 ACL Supported by the S-switch](#)

### [6.1.3 Update History](#)

## 6.1.1 Introduction to ACL

To enable a device to filter the passing packets, you can configure a series of rules on the device to determine what kinds of packets can pass filtering. The rules configured on the device are called Access Control List (ACL) rules.

An ACL includes a group of orderly rules that consist of **rule { deny | permit }** clauses. The rules are described based on the source address, the destination address, and the port number of data packets. The ACL classifies data packets according to these rules. After these rules are applied to the device, the device can determine whether to receive or deny packets.

The ACL is classified into two types:

- Basic ACL: classifies packets based on the source address and destination address.
- Advanced ACL: classifies packets more detailedly based on the source address, destination address, source port number, destination port number, and protocol type.



#### NOTE

Actually, an ACL is a group of rules used to define classes of packets. It cannot be used to filter packet. For detailed processing methods of packets, you need to import detailed functions of ACL.

## 6.1.2 ACL Supported by the S-switch

The S-switch supports basic ACLs and advanced ACLs.

## 6.1.3 Update History

| Version         | Revision                   |
|-----------------|----------------------------|
| V100R002C01B050 | This is the first release. |

## 6.2 Configuring an ACL

This section describes how to configure a basic ACL and an advanced ACL.

### [6.2.1 Establishing the Configuration Task](#)

### [6.2.2 Creating a Time Range](#)

### [6.2.3 Configuring ACL Descriptions](#)

### [6.2.4 Configuring a Basic ACL](#)

[6.2.5 Configuring an Advanced ACL](#)

[6.2.6 Configuring ACL Step](#)

[6.2.7 Checking the Configuration](#)

## 6.2.1 Establishing the Configuration Task

### Applicable Environment

An ACL can be applied to various services such as route policies and packet filtering. It distinguishes different kinds of packets for different processing.

### Pre-configuration Tasks

None.

### Data Preparation

To configure an ACL, you need the following data.

| No. | Data   |
|-----|--|
| 1   | Name of the time range during which an ACL takes effect, the start time and the end time   |
| 2   | ACL number   |
| 3   | Rule IDs of an ACL and rules to define packet types, including the protocol number, source address and source port, destination address and destination port, ICMP type and code, IP precedence, ToS, and whether the packet is fragmented |
| 4   | ACL remarks  |
| 5   | ACL step   |

## 6.2.2 Creating a Time Range

### Context

Do as follows on the S-switch:

### Procedure

**Step 1** Run:

```
system-view
```

The system view is displayed.

**Step 2** Run:

```
time-range time-name { start-time to end-time days | from time1 date1 [ to time2  
date2 ] }
```

An ACL time range is created.

You can configure multiple time ranges at the same name.

----End

## 6.2.3 Configuring ACL Descriptions

### Context

Do as follows on the S-switch:

### Procedure

**Step 1** Run:

```
system-view
```

The system view is displayed.

**Step 2** Run:

```
acl acl-number
```

The ACL view is displayed.

**Step 3** Run:

```
description text
```

ACL description is created.

The ACL description covers the function of ACL rules. Its length must be less than 127 characters.

----End

## 6.2.4 Configuring a Basic ACL

### Context

The range of *acl-number* of a basic ACL is 2000 to 2999.

Do as follows on the S-switch:

### Procedure

**Step 1** Run:

```
system-view
```

The system view is displayed.

**Step 2** Run:

```
acl [ number ] acl-number
```

A basic ACL is created.

**Step 3** Run:

```
rule [ rule-id ] { deny | permit } [ fragment | source { source-ip-address source-wildcard | any } | time-range time-range name ] *
```

ACL rules are defined.

----End

## 6.2.5 Configuring an Advanced ACL

### Context

The range of *acl-number* of an advanced ACL is 3000 to 3999.

Do as follows on the S-switch:

### Procedure

**Step 1** Run:

```
system-view
```

The system view is displayed.

**Step 2** Run:

```
acl [ number ] acl-number
```

An advanced ACL is created.

**Step 3** Perform the following as required.

- When *protocol* is specified as TCP or UDP

Run:

```
rule [ rule-id ] { deny | permit } protocol [ destination { destination-ip-address destination-wildcard | any } | destination-port operator port-number | fragment | precedence precedence | source { source-ip-address source-wildcard | any } | source-port operator port-number | time-range time-range name ] *
```

ACL rules are defined.

- When *protocol* is specified as ICMP

Run:

```
rule [ rule-id ] { deny | permit } protocol [ destination { destination-ip-address destination-wildcard | any } | fragment | icmp-type { icmp-name | icmp-type icmp-code } | precedence precedence | source { source-ip-address source-wildcard | any } | time-range time-range name ] *
```

ACL rules are defined.

- When *protocol* is specified as other protocol except TCP, UDP or ICMP

Run:

```
rule [ rule-id ] { deny | permit } protocol [ destination { destination-ip-address destination-wildcard | any } | dscp dscp | fragment | precedence precedence | source { source-ip-address source-wildcard | any } | time-range time-range name | tos tos ] *
```

Configure different advanced ACLs on the device for different protocols over IP. Different protocols have different parameters combination. For example, TCP and UDP have optional

parameter [ **source-port** *operator port* ] [ **destination-port** *operator port*] while other protocols do not.

----End

## 6.2.6 Configuring ACL Step

### Context

Do as follows on the S-switch:

### Procedure

**Step 1** Run:

**system-view**

The system view is displayed.

**Step 2** Run:

**acl** [ **number** ] *acl-number*

The ACL view is displayed.

**Step 3** Run:

**step** *step*

ACL step is configured.

Note the following when modifying ACL configurations:

- The **undo step** command restores the step to the default and realigns ACL rules.
- The default step of the ACL rule is 5.

----End

## 6.2.7 Checking the Configuration

Run the following commands in any view to check the previous configuration.

| Action                        | Command   |
|-------------------------------|---|
| View the configured ACL rule. | <b>display acl</b> { <i>acl-number</i>   <b>all</b> }             |
| View the time range.          | <b>display time-range</b> { <i>time-range name</i>   <b>all</b> } |

Run the **display acl** command. If the ACL number, the number of rules, and detailed step description, and ACL rules are displayed, it means that the configuration succeeds. For example:

```
<Quidway> display acl 3000
Advanced ACL 3000, 1 rule
Acl's step is 5
rule 5 deny ip source 10.1.1.1 0 (5 times matched)
```

Run the **display time-range** command. If the configuration and status of the current time range are displayed, it means that the configuration succeeds. For example:

```
<Quidway> display time-range all
Current time is 14:19:16 3-15-2006 Wednesday
Time-range : time1 ( Inactive )
    10:00 to 12:00 daily
Time-range : time2 ( Inactive )
    from 13:00 2006/4/1 to 23:59 2099/12/31
Time-range : active1 ( Active )
    14:00 to 00:00 daily
```

## 6.3 Maintaining an ACL

This section describes how to clear operation information about an ACL.

### 6.3.1 Clearing Statistics

#### 6.3.2 Monitoring Network Operation Status

### 6.3.1 Clearing Statistics



#### CAUTION

Statistics cannot restore after you clear it. So, confirm the action before you use the command.

To clear the operation information about an ACL, run the following **reset** command in the user view.

| Action                 | Command   |
|------------------------|---|
| Reset the ACL counter. | <b>reset acl counter</b> { <i>acl-number</i>   <b>all</b> } |

### 6.3.2 Monitoring Network Operation Status

To obtain configurations about the ACL in routine maintenance, run the following commands.

| Action                          | Command   |
|---------------------------------|---|
| View rules of the ACL.          | <b>display acl</b> { <i>acl-number</i>   <b>all</b> }             |
| View the time range of the ACL. | <b>display time-range</b> { <i>time-range name</i>   <b>all</b> } |

## 6.4 Configuration Examples

This section provides a configuration example of an ACL.

### 6.4.1 Example for Configuring an ACL

### 6.4.1 Example for Configuring an ACL

For details on the example for configuring an ACL, refer to the example for configuring QoS.

# 7 DHCP Policy VLAN Configuration

---

## About This Chapter

This chapter describes the concept, operating mode, and configuration of Dynamic Host Configuration Protocol (DHCP) policy Virtual Local Area Network (VLAN), and provides configuration examples.

### [7.1 Overview](#)

This section describes the concept of DHCP policy VLAN.

### [7.2 Configuring DHCP Policy VLAN Based on MAC Addresses](#)

This section describes how to configure DHCP Policy VLAN Based on MAC Addresses

### [7.3 Configuring the DHCP Policy VLAN Based on Interfaces](#)

This section describes how to configure the DHCP policy VLAN based on interfaces.

### [7.4 Configuring Generic DHCP Policy VLAN](#)

This section describes how to configure Generic DHCP Policy VLAN

### [7.5 Maintaining DHCP Policy VLAN](#)

This section describes how to maintain DHCP policy VLAN.

### [7.6 Configuration Examples](#)

This section provides several configuration examples of DHCP policy VLAN.

## 7.1 Overview

This section describes the concept of DHCP policy VLAN.

### [7.1.1 Introduction](#)

### [7.1.2 DHCP Policy VLAN Supported by the S-switch](#)

### [7.1.3 Update History](#)

#### 7.1.1 Introduction

When the policy for VLANs is configured on the S-switch, the VLAN to which each host connects to the interface on the S-switch belongs is determined by the network segment to which the IP address of the host belongs. When a host that accesses the network for the first time is connected to an interface, the host cannot be added to its associated VLAN because it has no valid IP address.

DHCP policy VLAN is thus introduced. With DHCP policy VLAN, hosts that access the network for the first time can obtain valid IP addresses from the DHCP server and then be added to the VLANs whose network segments the IP addresses belong to.

#### 7.1.2 DHCP Policy VLAN Supported by the S-switch

The S-switch supports the following types of DHCP policy VLAN:

- DHCP policy VLAN based on MAC addresses
- DHCP policy VLAN based on interfaces
- Generic DHCP policy VLAN

#### 7.1.3 Update History

| Version         | Revision                   |
|-----------------|----------------------------|
| V100R002C02B050 | This is the first release. |

## 7.2 Configuring DHCP Policy VLAN Based on MAC Addresses

This section describes how to configure DHCP Policy VLAN Based on MAC Addresses

### [7.2.1 Establishing the Configuration Task](#)

### [7.2.2 Configuration Procedure](#)

### [7.2.3 Checking the Configuration](#)

#### 7.2.1 Establishing the Configuration Task

## Applicable Environment

When multiple hosts access the network through an interface on the S-switch, you need to configure DHCP policy VLAN based on MAC addresses so that the hosts can obtain IP addresses from the DHCP server and be added to specific VLANs.

## Pre-configuration Tasks

Before configuring DHCP policy VLAN based on MAC addresses, complete the following tasks:

- Configuring the default VLAN for the interface on the S-switch that connects to the newly added hosts

## Data Preparation

To configure DHCP policy VLAN based on MAC addresses, you need the following data.

| No. | Data  |
|-----|---|
| 1   | MAC addresses of the newly added hosts          |
| 2   | ID of the VLAN to which the DHCP server belongs |

## 7.2.2 Configuration Procedure

### Context

Do as follows on the S-switch.

### Procedure

#### Step 1 Run:

```
system-view
```

The system view is displayed.

#### Step 2 Run:

```
interface interface-type interface-number
```

The view of the interface on the S-switch that connects to multiple hosts is displayed.

#### Step 3 Run:

```
port hybrid untagged vlan { { vlan-id1 [ to vlan-id2 ] } <1-10> | all }
```

The interface is added to the specified VLANs, ensuring that frames from the VLANs pass through the interface in untagged mode.

#### Step 4 Run:

```
vlan vlan id
```

The view of the VLAN to which the DHCP server belongs is displayed.

**Step 5** Run:

```
policy-vlan dhcp-mac mac-address1 [ to mac-address2 ] [ priority priority ]
```

The DHCP policy VLAN based on MAC addresses is configured.

----End

## 7.2.3 Checking the Configuration

Run the following command to check the previous configuration.

| Action  | Command             |
|---|---------------------|
| Check the configuration of the S-switch in the VLAN view. | <b>display this</b> |

Run the **display this** command in the VLAN view of the S-switch where DHCP policy VLAN based on MAC addresses is configured, you can view that the configuration of DHCP policy VLAN based on MAC addresses is correct.

```
[Quidway-vlan2] display this
#
vlan 2
 policy-vlan dhcp-mac 0002-0002-0002 priority 2
#
```

## 7.3 Configuring the DHCP Policy VLAN Based on Interfaces

This section describes how to configure the DHCP policy VLAN based on interfaces.

### [7.3.1 Establishing the Configuration Task](#)

### [7.3.2 Configuration Procedure](#)

### [7.3.3 Checking the Configuration](#)

## 7.3.1 Establishing the Configuration Task

### Applicable Environment

When multiple hosts access the network through different interfaces on the S-switch, you need to configure DHCP policy VLAN based on interfaces so that the hosts can obtain IP addresses from the DHCP server.

### Pre-configuration Tasks

Before configuring DHCP policy VLAN based on interfaces, complete the following tasks:

- Configuring the default VLAN for the interface that connects to the newly added host on the S-switch

- Configuring the interface that connects to the newly added host on the S-switch as a hybrid interface

## Data Preparation

To configure DHCP policy VLAN based on interfaces, you need the following data.

| No. | Data  |
|-----|---|
| 1   | Number of the interface that connects to the newly added host on the S-switch |
| 2   | ID of the VLAN to which the DHCP server belongs                               |

## 7.3.2 Configuration Procedure

### Context

Do as follows on the S-switch.

### Procedure

#### Step 1 Run:

```
system-view
```

The system view is displayed.

#### Step 2 Run:

```
interface interface-type interface-number
```

The view of the interface that connects to the newly added host on the S-switch is displayed.

#### Step 3 Run:

```
port hybrid untagged vlan { { vlan-id1 [ to vlan-id2 ] }&<1-10> | all }
```

The interface is added to the specified VLANs, ensuring that frames from the VLANs pass through the interface in untagged mode.

#### Step 4 Run:

```
vlan vlan id
```

The view of the VLAN to which the DHCP server belongs is displayed.

#### Step 5 Run:

```
policy-vlan dhcp-port interface-type interface-number1 [ to interface-number2 ]  
[ priority priority ]
```

The DHCP policy VLAN based on interfaces is configured.

----End

## 7.3.3 Checking the Configuration

Run the following commands to check the previous configuration.

| Action  | Command             |
|---|---------------------|
| Check the configuration of the S-switch in the VLAN view. | <b>display this</b> |

Run the **display this** command in the VLAN view of the S-switch where DHCP policy VLAN based on interfaces is configured, you can view that the configuration of DHCP policy VLAN based on interfaces is correct.

```
[Quidway-vlan2] display this
#
vlan 2
 policy-vlan dhcp-port GigabitEthernet 0/0/2 priority 2
#
```

## 7.4 Configuring Generic DHCP Policy VLAN

This section describes how to configure Generic DHCP Policy VLAN

### [7.4.1 Establishing the Configuration Task](#)

### [7.4.2 Configuration Procedure](#)

### [7.4.3 Checking the Configuration](#)

## 7.4.1 Establishing the Configuration Task

### Applicable Environment

When hosts that do not apply DHCP policy VLAN based on MAC addresses or DHCP policy VLAN based on interfaces access the network for the first time, you need to configure generic DHCP policy VLAN on the S-switch so that the hosts can obtain valid IP addresses.

### Pre-configuration Tasks

Before configuring generic DHCP policy VLAN, complete the following tasks:

- Configuring the default VLAN for the interface that connects to the newly added host on the S-switch

### Data Preparation

To configure generic DHCP policy VLAN, you need the following data.

| No. | Data  |
|-----|---|
| 1   | ID of the VLAN to which the DHCP server belongs |

## 7.4.2 Configuration Procedure

## Context

Do as follows on the S-switch.

## Procedure

**Step 1** Run:

```
system-view
```

The system view is displayed.

**Step 2** Run:

```
interface interface-type interface-number
```

The view of the interface that connects to the newly added host on the S-switch is displayed.

**Step 3** Run:

```
port hybrid untagged vlan { { vlan-id1 [ to vlan-id2 ] }&<1-10> | all }
```

The interface is added to the specified VLANs, ensuring that frames from the VLANs pass through the interface in untagged mode.

**Step 4** Run:

```
vlan vlan id
```

The view of the VLAN to which the DHCP server belongs is displayed.

**Step 5** Run:

```
policy-vlan dhcp-generic [ priority priority ]
```

The generic DHCP policy VLAN is configured.

----End

## 7.4.3 Checking the Configuration

Run the following command to check the previous configuration.

| Action  | Command             |
|---|---------------------|
| Check the configuration of the S-switch in the VLAN view. | <b>display this</b> |

Run the **display this** command in the VLAN view of the S-switch where generic DHCP policy VLAN is configured, you can view that the configuration of generic DHCP policy VLAN is correct.

```
[Quidway-vlan2] display this
#
vlan 2
 policy-vlan dhcp-generic priority 2
#
```

## 7.5 Maintaining DHCP Policy VLAN

This section describes how to maintain DHCP policy VLAN.

[7.5.1 Monitoring the Running Status](#)

## 7.5.1 Monitoring the Running Status

To check the running status of DHCP policy VLAN, run the following **display** command in the corresponding VLAN view.

| Action                                       | Command             |
|--|---------------------|
| Check the configuration of DHCP policy VLAN. | <b>display this</b> |

## 7.6 Configuration Examples

This section provides several configuration examples of DHCP policy VLAN.

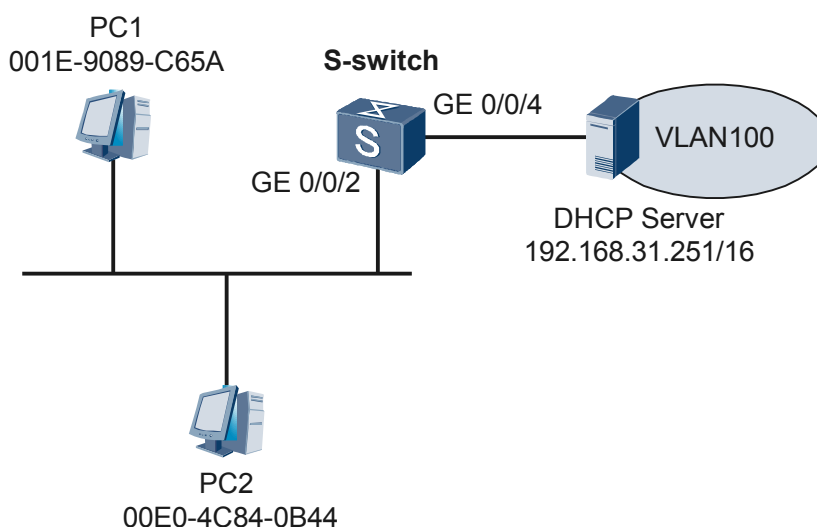
[7.6.1 Example for Configuring DHCP Policy VLAN Based on MAC Addresses](#)[7.6.2 Example for Configuring DHCP Policy VLAN Based on Interfaces](#)

### 7.6.1 Example for Configuring DHCP Policy VLAN Based on MAC Addresses

#### Networking Requirements

As shown in [Figure 7-1](#), on the S-switch, GE 0/0/2 connects to PC1 and PC2 that access the network for the first time; GE 0/0/4 connects to the DHCP server that belongs to VLAN 100. The MAC address of PC1 is 001E-9089-C65A; the MAC address of PC2 is 00E0-4C84-0B44.

**Figure 7-1** Networking for configuring DHCP policy VLAN based on MAC addresses



## Configuration Roadmap

The configuration roadmap is as follows:

1. Determine to which VLAN the DHCP server belongs.
2. Configure DHCP policy VLAN based on MAC addresses.

## Data Preparation

To complete the configuration, you need the following data:

- MAC address of the newly added host

## Configuration Procedure

1. Configure the S-switch.

# Configure GE 0/0/2 and GE 0/0/4 on the S-switch as a hybrid interface, and configure frames from VLAN 100 to pass through GE 0/0/2 in untagged mode.

```
<Quidway> system-view
[Quidway] interface gigabitethernet 0/0/2
[Quidway-GigabitEthernet0/0/2] port hybrid untagged vlan 100
[Quidway-GigabitEthernet0/0/2] quit
[Quidway] interface gigabitethernet 0/0/4
[Quidway-GigabitEthernet0/0/4] port hybrid untagged vlan 100
[Quidway-GigabitEthernet0/0/4] quit
```

# Configure DHCP policy VLAN based on MAC addresses.

```
<Quidway> system-view
[Quidway] vlan 100
[Quidway-vlan100] policy-vlan dhcp-mac 001E-9089-C65A priority 5
[Quidway-vlan100] policy-vlan dhcp-mac 00E0-4C84-0B44 priority 5
[Quidway-vlan100] quit
```

2. Verify the configuration.

# Ping the DHCP server from PC1 and PC2. The ping operations are successful.

```
C:\>ping 192.168.31.251
```

Pinging 192.168.31.251 with 32 bytes of data:

```
Reply from 192.168.31.251: bytes=32 time=126ms TTL=255
Reply from 192.168.31.251: bytes=32 time=2ms TTL=255
Reply from 192.168.31.251: bytes=32 time=2ms TTL=255
Reply from 192.168.31.251: bytes=32 time=2ms TTL=255
```

```
Ping statistics for 192.168.31.251:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 2ms, Maximum = 126ms, Average = 33ms
```

## Configuration Files

The following lists the configuration file of the S-switch.

```
#
interface GigabitEthernet0/0/2
 port hybrid untagged vlan 100
interface GigabitEthernet0/0/4
 port hybrid untagged vlan 100
#
vlan 100
 policy-vlan dhcp-mac 001e-9089-c65a priority 5
 policy-vlan dhcp-mac 00e0-4c84-0b44 priority 5
```

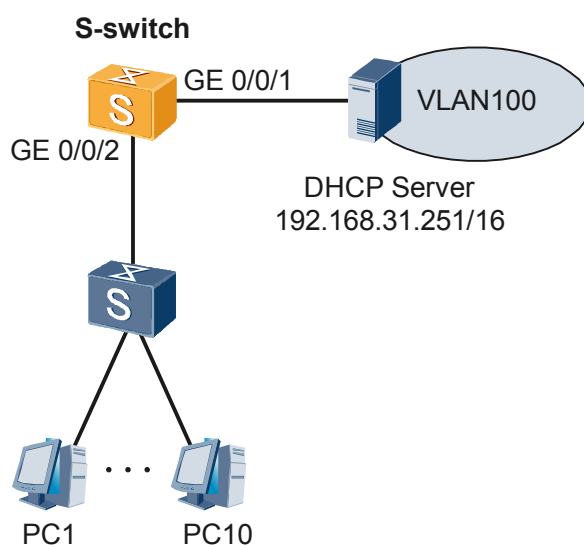
```
#
return
```

## 7.6.2 Example for Configuring DHCP Policy VLAN Based on Interfaces

### Networking Requirements

As shown in [Figure 7-2](#), on the S-switch, GE 0/0/2 connects to an access switch; GE 0/0/1 connects to the DHCP server that belongs to VLAN 100; the access switch connects to 10 hosts.

**Figure 7-2** Networking for configuring DHCP policy VLAN based on interfaces



### Configuration Roadmap

The configuration roadmap is as follows:

1. Determine to which VLAN the DHCP server belongs.
2. Configure DHCP policy VLAN based on interfaces.

### Data Preparation

To complete the configuration, you need the following data:

- Number of the S-switch interface that connects to the downstream access switch

### Configuration Procedure

1. Configure the S-switch.

# Configure GE 0/0/1 and GE 0/0/2 on the S-switch as hybrid interfaces, and configure frames from VLAN 100 to pass through GigabitEthernet 0/0/2 in untagged mode.

```
<Quidway> system-view
[Quidway] interface gigabitethernet 0/0/1
```

```
[Quidway-GigabitEthernet0/0/1] port link-type hybrid
[Quidway-GigabitEthernet0/0/1] port hybrid untagged vlan 100
[Quidway-GigabitEthernet0/0/1] quit
[Quidway] interface gigabitethernet 0/0/2
[Quidway-GigabitEthernet0/0/2] port link-type hybrid
[Quidway-GigabitEthernet0/0/2] port hybrid untagged vlan 100
[Quidway-GigabitEthernet0/0/2] quit

# Configure DHCP policy VLAN based on interfaces.

<Quidway> system-view
[Quidway] vlan 100
[Quidway-vlan100] policy-vlan dhcp-port gigabitethernet 0/0/2 priority 5
```

2. Verify the configuration.

# Ping the DHCP server from each host. The ping operations are successful.

```
C:\>ping 192.168.31.251

Pinging 192.168.31.251 with 32 bytes of data:

Reply from 192.168.31.251: bytes=32 time=126ms TTL=255
Reply from 192.168.31.251: bytes=32 time=2ms TTL=255
Reply from 192.168.31.251: bytes=32 time=2ms TTL=255
Reply from 192.168.31.251: bytes=32 time=2ms TTL=255

Ping statistics for 192.168.31.251:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 2ms, Maximum = 126ms, Average = 33ms
```

## Configuration Files

The following lists the configuration file of the S-switch.

```
#
interface GigabitEthernet0/0/1
 port hybrid untagged vlan 100
interface GigabitEthernet0/0/2
 port hybrid untagged vlan 100
#
vlan 100
 policy-vlan dhcp-port gigabitEthernet 0/0/2 priority 5
#
return
```