

Table of Contents

Chapter 1 IP Address Configuration	1-1
1.1 IP Address Overview	1-1
1.1.1 IP Address Classification and Indications	1-1
1.1.2 Subnet and Mask	1-3
1.2 Configuring IP Address	1-3
1.2.1 Configuring the Hostname and Host IP Address	1-4
1.2.2 Configuring the IP Address of the VLAN Interface	1-4
1.3 Displaying and debugging IP Address	1-5
1.4 IP Address Configuration Example	1-5
1.5 Troubleshooting IP Address Configuration	1-6
Chapter 2 ARP Configuration	2-1
2.1 Introduction to ARP	2-1
2.2 Configuring ARP	2-2
2.2.1 Manually Adding/Deleting Static ARP Mapping Entries	2-2
2.2.2 Configuring the Dynamic ARP Aging Timer	2-3
2.2.3 Enabling/Disabling ARP the Checking Function of ARP Entry	2-3
2.3 Displaying and debugging ARP	2-3
Chapter 3 Resilient ARP Configuration	3-1
3.1 Overview of Resilient ARP	3-1
3.2 Resilient ARP Configuration	3-1
3.2.1 Enabling/Disabling Resilient ARP Function	3-1
3.2.2 Configuring Resilient ARP Packet-sending VLAN Interface	3-2
3.3 Displaying and Debugging Resilient ARP Configuration	3-2
3.4 Resilient ARP Configuration Example	3-3
Chapter 4 BOOTP Client Configuration	4-1
4.1 Overview of BOOTP Client	4-1
4.2 BOOTP Client Configuration	4-1
4.2.1 Configuring a VLAN Interface to Obtain the IP Address Using BOOTP	4-1
4.3 Debugging BOOTP Client	4-2
Chapter 5 DHCP Configuration	5-1
5.1 Overview of DHCP	5-1
5.1.1 Brief Introduction	5-1
5.1.2 DHCP Relay	5-2
5.2 DHCP Client Configuration	5-3
5.2.1 Configuring a VLAN Interface to Obtain IP Address Using DHCP	5-3
5.3 DHCP Relay Configuration	5-4

5.3.1 Configuring the IP address for the DHCP server	5-4
5.3.2 Configuring the DHCP Server Group Corresponding to VLAN Interfaces	5-5
5.3.3 Configuring the User Address Entry for the DHCP server group	5-5
5.3.4 Enabling/Disabling DHCP Security Feature on the VLAN interface	5-5
5.3.5 Enable/Disable to Define Update Interval for DHCP Security Entries	5-6
5.4 Displaying and Debugging DHCP Configuration	5-6
5.5 DHCP Relay Configuration Example	5-7
5.6 Troubleshooting DHCP Relay Configuration	5-8
Chapter 6 Access Management Configuration	6-1
6.1 Access Management Overview	6-1
6.2 Configuring Access Management	6-1
6.2.1 Enabling/Disabling Access Management Function	6-1
6.2.2 Configuring the Access Management IP Address Pool Based on the Port	6-1
6.2.3 Configuring Layer 2 isolation between ports	6-2
6.2.4 Enabling/Disabling Access Management Trap	6-3
6.3 Displaying and Debugging Access Management	6-3
6.4 Access Management Configuration Example	6-3
Chapter 7 UDP Helper Configuration	7-1
7.1 Overview of UDP Helper	7-1
7.2 UDP Helper Configuration	7-1
7.2.1 Enabling/disabling UDP Helper Function	7-1
7.2.2 Configuring UDP Port with Replay Function	7-1
7.2.3 Configuring the Relay Destination Server for Broadcast Packet	7-2
7.3 Displaying and Debugging UDP Helper Configuration	7-3
7.4 UDP Helper Configuration Example	7-3
Chapter 8 IP Performance Configuration	8-1
8.1 IP Performance Configuration	8-1
8.1.1 Configuring TCP Attributes	8-1
8.2 Displaying and debugging IP Performance	8-2
8.3 Troubleshooting IP Performance	8-2

Chapter 1 IP Address Configuration

1.1 IP Address Overview

1.1.1 IP Address Classification and Indications

IP address is a 32-bit address allocated to the devices which access into the Internet. It consists of two fields: net-id field and host-id field. There are five types of IP address. See the following figure.

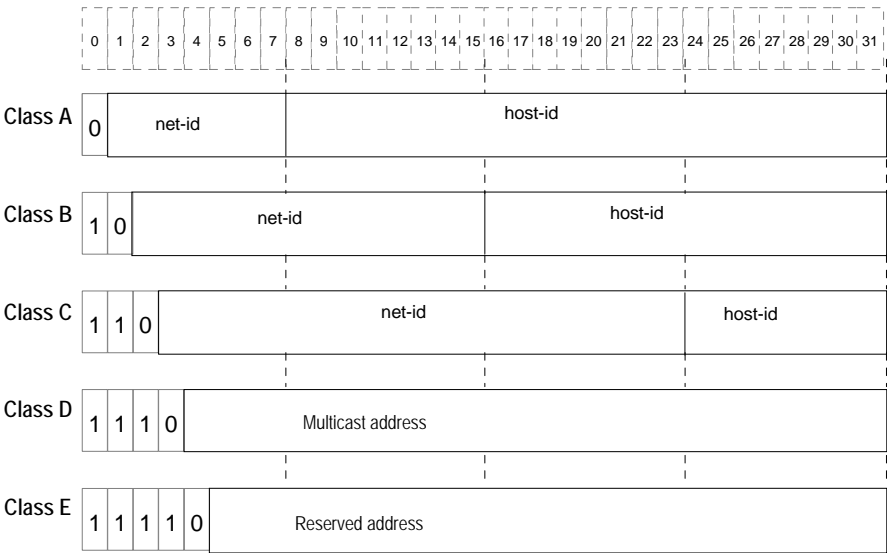


Figure 1-1 Five classes of IP address

Where, Class A, Class B and Class C are unicast addresses, while Class D addresses are multicast ones and class E addresses are reserved for special applications in future. The first three types are commonly used.

The IP address is in dotted decimal format. Each IP address contains 4 integers in dotted decimal notation. Each integer corresponds to one byte, e.g.10.110.50.101.

When using IP addresses, it should also be noted that some of them are reserved for special uses, and are seldom used. The IP addresses you can use are listed in the following table.

Table 1-1 IP address classes and ranges

Network class	Address range	IP network range	Note
A	0.0.0.0 to 127.255.255.255	1.0.0.0 to 126.0.0.0	<p>Host ID with all the digits being 0 indicates that the IP address is the network address, and is used for network routing.</p> <p>Host ID with all the digits being 1 indicates the broadcast address, i.e. broadcast to all hosts on the network.</p> <p>IP address 0.0.0.0 is used for the host that is not put into use after starting up.</p> <p>The IP address with network number as 0 indicates a specific host on the network, and this host can be the source end but not the destination end.</p> <p>Network ID with the format of 127.X.Y.Z is reserved for self-loop test and the packets sent to this address will not be output to the line. The packets are processed internally and regarded as input packets.</p>
B	128.0.0.0 to 191.255.255.255	128.0.0.0 to 191.254.0.0	<p>Host ID with all the digits being 0 indicates that the IP address is the network address, and is used for network routing.</p> <p>Host ID with all the digits being 1 indicates the broadcast address, i.e. broadcast to all hosts on the network.</p>
C	192.0.0.0 to 223.255.255.255	192.0.0.0 to 223.255.254.0	<p>Host ID with all the digits being 0 indicates that the IP address is the network address, and is used for network routing.</p> <p>Host ID with all the digits being 1 indicates the broadcast address, i.e. broadcast to all hosts on the network.</p>
D	224.0.0.0 to 239.255.255.255	None	Addresses of class D are multicast addresses.
E	240.0.0.0 to 255.255.255.254	None	The addresses are reserved for future use.
Other addresses	255.255.255.255	255.255.255.255	255.255.255.255 is used as LAN broadcast address.

1.1.2 Subnet and Mask

Nowadays, with rapid development of the Internet, IP addresses are depleting very fast. The traditional IP address allocation method wastes IP addresses greatly. In order to make full use of the available IP addresses, the concept of mask and subnet is proposed.

A mask is a 32-bit number corresponding to an IP address. The number consists of 1s and 0s. Principally, these 1s and 0s can be combined randomly. Generally, the mask is defined as the following: the bit value of the network number and subnet number is set to 1, and the bit value of the host number is set to 0. The mask divides the IP address into two parts: subnet address and host address. The bits 1s in the address and the mask indicate the subnet address and the other bits indicate the host address. If there is no sub-net division, then its sub-net mask is the default value and the length of "1" indicates the net-id length. Therefore, for IP addresses of classes A, B and C, the default values of corresponding sub-net mask are 255.0.0.0, 255.255.0.0 and 255.255.255.0 respectively.

The mask can be used to divide a Class A network containing more than 16,000,000 hosts or a Class B network containing more than 60,000 hosts into multiple small networks. Each small network is called a subnet. For example, for the Class B network address 138.38.0.0, the mask 255.255.224.0 can be used to divide the network into 8 subnets: 138.38.0.0, 138.38.32.0, 138.38.64.0, 138.38.96.0, 138.38.128.0, 138.38.160.0, 138.38.192.0 and 138.38.224.0 (Refer to the following figure). Each subnet can contain more than 8000 hosts.

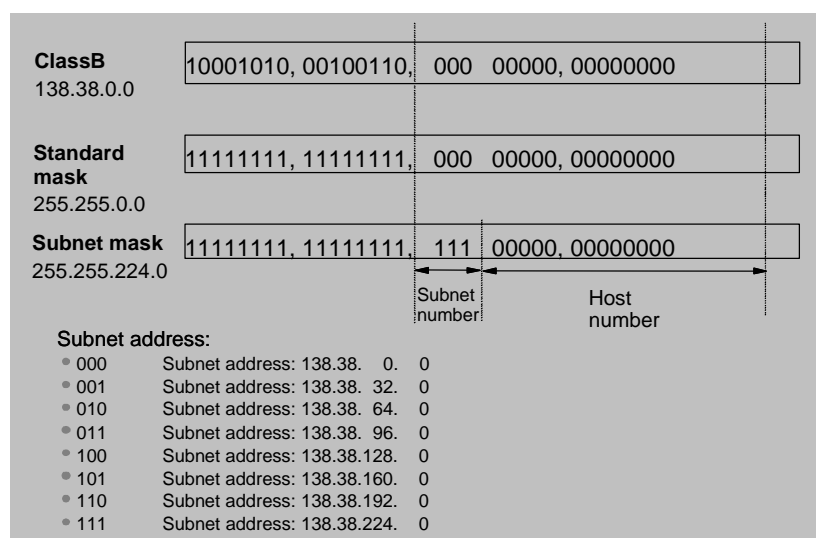


Figure 1-2 Subnet division of IP address

1.2 Configuring IP Address

Configure an IP address for VLAN interface in one of three ways:

- Using the IP address configuration command
- Allocated by BOOTP server
- Allocated by DHCP server

These three methods are mutually exclusive and a new configuration will replace the current IP address. For example, if you apply for an IP address using the **ip address bootp-alloc** command, the address allocated by BOOTP shall replace the currently-configured IP address.

This chapter just introduces how to configure an IP address with the IP address configuration command and the other two methods are to be discussed in the subsequent chapters.

The IP address configuration includes:

- Configuring the Hostname and Host IP Address
- Configuring the IP Address of the VLAN Interface

1.2.1 Configuring the Hostname and Host IP Address

The host name is corresponded to the IP address by using this command. When you use the applications like telnet, you can use the host name without having to memorize the IP address since the system translates it to the IP address automatically.

Perform the following configuration in System view.

Table 1-2 Configuring the host name and the corresponding IP address

Operation	Command
Configure the hostname and the corresponding IP address	ip host <i>hostname ip-address</i>
Delete the hostname and the corresponding IP address	undo ip host <i>hostname [ip-address]</i>

By default, there is no host name associated to any host IP address.

1.2.2 Configuring the IP Address of the VLAN Interface

You can configure an IP address for every VLAN interface of the switch. Generally, it is enough to configure one IP address for an interface. You can also configure five IP addresses for an interface at most, so that it can be connected to several subnets. Among these IP addresses, one is the primary IP address and all others are secondary.

Perform the following configuration in VLAN interface view.

Table 1-3 Configuring the IP address for a VLAN interface

Operation	Command
Configure IP address for a VLAN interface	ip address <i>ip-address</i> { <i>mask</i> <i>mask-length</i> } [sub]
Delete the IP address of a VLAN interface	undo ip address <i>ip-address</i> { <i>mask</i> <i>mask-length</i> } [sub]

By default, the IP address of a VLAN interface is null.

Note that the VLAN interface cannot be configured with the secondary IP address if its IP address is set to be allocated by BOOTP or DHCP.

1.3 Displaying and debugging IP Address

After the above configuration, execute **display** command in any view to display the IP addresses configured on interfaces of the network device, and to verify the effect of the configuration.

Table 1-4 Displaying and debugging IP address

Operation	Command
Display all hosts on the network and the corresponding IP addresses	display ip host
Display the configurations of each interface	display ip interface [<i>interface-type</i> <i>interface-number</i> brief]

1.4 IP Address Configuration Example

I. Networking requirements

Configure the IP address as 129.2.2.1 and sub-net mask as 255.255.255.0 for the VLAN interface 1 of the switch.

II. Networking diagram

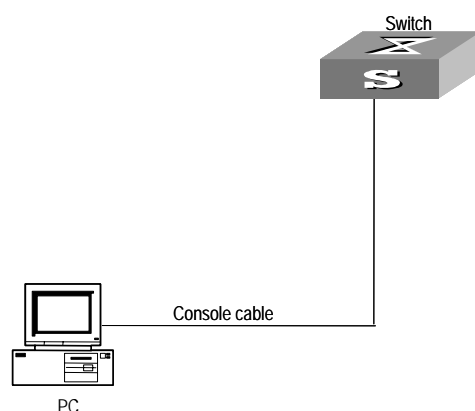


Figure 1-3 IP address configuration networking

III. Configuration procedure

Enter VLAN interface 1.

```
[Quidway] interface vlan-interface 1
```

Configure the IP address for VLAN interface 1.

```
[Quidway-vlan-interface1] ip address 129.2.2.1 255.255.255.0
```

1.5 Troubleshooting IP Address Configuration

Fault 1: The switch cannot ping through a certain host in the LAN.

Troubleshooting can be performed as follows:

- Check the configuration of the switch. Use **display arp** command to view the ARP entry table that the Switch maintains.
- Troubleshooting: First check which VLAN includes the port of the switch used to connect to the host. Check whether the VLAN has been configured with the VLAN interface. Then check whether the IP address of the VLAN interface and the host is on the same network segment.
- If the configuration is correct, enable the ARP debugging on the switch, and check whether the switch can correctly send and receive ARP packets. If it can only send but cannot receive the ARP packets, possibly errors occur on the Ethernet physical layer.

Chapter 2 ARP Configuration

2.1 Introduction to ARP

I. Necessity of ARP

An IP address cannot be directly used for communication between network devices because network devices can only identify MAC addresses. An IP address is only an address of a host in the network layer. To send the data packets transmitted through the network layer to the destination host, physical address of the host is required. So the IP address must be resolved into a physical address.

II. ARP implementation procedure

When two hosts on the Ethernet communicate, they must know the MAC addresses of each other. Every host will maintain the IP-MAC address translation table, which is known as ARP mapping table. A series of maps between IP addresses and MAC addresses of other hosts which were recently used to communicate with the local host are stored in the ARP mapping table. When a dynamic ARP mapping entry is not in use for a specified period of time, the host will remove it from the ARP mapping table so as to save the memory space and shorten the interval for switch to search ARP mapping table.

Suppose there are two hosts on the same network segment: Host A and Host B. The IP address of Host A is IP_A and the IP address of Host B is IP_B. Host A will transmit messages to Host B. Host A checks its own ARP mapping table first to make sure whether there are corresponding ARP entries of IP_B in the table. If the corresponding MAC address is detected, Host A will use the MAC address in the ARP mapping table to encapsulate the IP packet in frame and send it to Host B. If the corresponding MAC address is not detected, Host A will store the IP packet in the queue waiting for transmission, and broadcast it throughout the Ethernet. The ARP request packet contains the IP address of Host B and IP address and MAC address of Host A. Since the ARP request packet is broadcast, all hosts on the network segment can receive the request. However, only the requested host (i.e., Host B) needs to process the request. Host B will first store the IP address and the MAC address of the request sender (Host A) in the ARP request packet in its own ARP mapping table. Then Host B will generate an ARP reply packet into which, it will add MAC address of Host B, and then send it to Host A. The reply packet will be directly sent to Host A instead of being broadcast. Receiving the reply packet, Host A will extract the IP address and the corresponding

MAC address of Host B and add them to its own ARP mapping table. Then Host A will send Host B all the packets standing in the queue.

Normally, dynamic ARP executes and automatically searches for the resolution from the IP address to the Ethernet MAC address without the administrator.

2.2 Configuring ARP

The ARP mapping table can be maintained dynamically or manually. Usually, the manually configured mapping from the IP addresses to the MAC addresses is known as static ARP. The user can display, add or delete the entries in the ARP mapping table through relevant manual maintenance commands.

The static ARP configuration includes:

- Manually adding/deleting static ARP Mapping Entries
- Configuring the dynamic ARP aging timer
- Enabling/disabling ARP the checking function of ARP entry

2.2.1 Manually Adding/Deleting Static ARP Mapping Entries

You can configure static ARP mapping items either in system view or Ethernet port view. In system view, you can configure global static ARP mapping entries, or configure static ARP mapping entries for the designated egress port; while in Ethernet port view, you may set the current port as the egress port of static ARP.

Perform the following configuration in System view or Ethernet port view.

Table 2-1 Manually adding/deleting static ARP mapping Entries

Operation	Command
Manually add a static ARP mapping entry (System view)	arp static <i>ip-address mac-address</i> [<i>vlan-id</i> { <i>interface-type interface-number</i> <i>interface-name</i> }]
Manually add a static ARP mapping entry (Ethernet port view)	arp static <i>ip-address mac-address vlan-id</i>
Manually delete a static ARP mapping entry (System view or Ethernet port view)	undo arp <i>ip-address</i>

By default, the ARP mapping table is empty and the address mapping is obtained through dynamic ARP.

Note that:

- Static ARP map entry will be always valid as long as the switch works normally. But if the VLAN corresponding ARP mapping entry is deleted, the ARP mapping entry will be also deleted. The valid period of dynamic ARP map entries will last only 20 minutes by default.
- The parameter *vlan-id* must be the ID of a VLAN that has been created by the user, and the Ethernet port specified behind this parameter must belong to the VLAN.
- The aggregation port or port with LACP enabled cannot be set as the egress port of static ARP.

2.2.2 Configuring the Dynamic ARP Aging Timer

For purpose of flexible configuration, the system provides the following commands to assign dynamic ARP aging period. When the system learns a dynamic ARP entry, its aging period is based on the current value configured.

Perform the following configuration in system view.

Table 2-2 Configuring the dynamic ARP aging timer

Operation	Command
Configure the dynamic ARP aging timer	arp timer aging <i>aging-time</i>
restore the default dynamic ARP aging time	undo arp timer aging

By default, the aging time of dynamic ARP aging timer is 20 minutes.

2.2.3 Enabling/Disabling ARP the Checking Function of ARP Entry

You can use the following command to control the device whether to learn the ARP entry where the MAC address is multicast MAC address.

Perform the following configuration in system view.

Table 2-3 Enabling/Disabling ARP the checking function of ARP entry

Operation	Command
Enable the checking of ARP entry, that is, the device does not learn the ARP entry where the MAC address is multicast MAC address	arp check enable
Disable the checking of ARP entry, that is, the device learns the ARP entry where the MAC address is multicast MAC address	undo arp check enable

By default, the checking of ARP entry is enabled, that is, the device does not learn the ARP entry where the MAC address is multicast MAC address.

2.3 Displaying and debugging ARP

After the above configuration, execute **display** command in any view to display the running of the ARP configuration, and to verify the effect of the configuration. Execute **debugging** command in user view to debug ARP configuration. Execute **reset** command in user view to clear ARP mapping table.

Table 2-4 Displaying and debugging ARP

Operation	Command
Display ARP mapping table	display arp [<i>ip-address</i> [dynamic static] [{ begin include exclude } <i>text</i>]]
Display the current setting of the dynamic ARP map aging timer	display arp timer aging
Reset ARP mapping table	reset arp [dynamic static interface { <i>interface-type</i> <i>interface-number</i> <i>interface-name</i> }]
Enable ARP information debugging	debugging arp packet
Disable ARP information debugging	undo debugging arp packet

Chapter 3 Resilient ARP Configuration

3.1 Overview of Resilient ARP

To support resilient networking in IRF applications, redundant links are required between the IRF fabric and other devices. But if intra-fabric connections are broken and original fabric is spitted, these redundant links may cause a situation where the network connects to two or more layer 3 devices of the same configuration and they run the same routing function. To eliminate this situation, you can resort to resilient ARP mechanism, which can immediately detect if there are layer 3 devices of the same configuration existing in the network. If yes, it can remain only one as Layer 3 device and turn others to Layer 2 ones.

Resilient ARP state machine may be in one of the six states: Initialize, LisentForL3Master, L3Master, L3Slave, L2Master and L2Slave. L3Master state machine sends regularly the Resilient ARP messages to notify other IRF fabrics that its home fabric is in Layer 3 state.

Resilient ARP mechanism can implement state transition by sending/receiving the Resilient ARP messages regularly, so as to determine if a device serves as Layer 3 or Layer 2 one.

3.2 Resilient ARP Configuration

Resilient ARP configuration includes:

- Enabling/disable resilient ARP function
- Configuring resilient ARP packet-sending VLAN interface

3.2.1 Enabling/Disabling Resilient ARP Function

After resilient ARP is enabled, the system can make proper processing based on current state to ensure there is only one Layer 3 device, while others as Layer 2 ones.

Perform the following configuration in system view.

Table 3-1 Enabling/disabling resilient ARP function

Operation	Command
Enable resilient ARP function	resilient-arp enable
Disable resilient ARP function	undo resilient-arp enable

By default, resilient ARP function is enabled.

3.2.2 Configuring Resilient ARP Packet-sending VLAN Interface

It is required to configure the VLAN interface corresponding to the redundant links which connect the IRF fabric with other devices, to make resilient ARP normally function. Then if intra-fabric connections are broken, resilient ARP packets can be sent through these VLAN interfaces corresponding to the redundant links, to determine if the system works as layer 3 or layer 2 device.

You can use the following command to configure through which VLAN interface the resilient ARP packet is sent. The system provides default VLAN interface to send resilient ARP packets.

Perform the following configuration in system view.

Table 3-2 Configuring/deleting resilient ARP packet-sending VLAN interface

Operation	Command
Configure resilient ARP packet-sending VLAN interface	resilient-arp interface <i>vlan-interface</i> <i>vlan-id</i>
Delete resilient ARP packet-sending VLAN interface	undo resilient-arp interface <i>vlan-interface</i> <i>vlan-id</i>

By default, the system sends resilient ARP packets through VLAN interface 1.

Note that you only specify resilient ARP packet-sending VLAN interfaces, and any VLAN interface can receive resilient ARP packets.

3.3 Displaying and Debugging Resilient ARP Configuration

After the above configurations are completed, you can use the **display** command in any view to view the running of resilient ARP function and further to check configuration result.

You can also use the **debugging** command in user view to debug resilient ARP function.

Table 3-3 Displaying and debugging resilient ARP configuration

Operation	Command
Display resilient ARP state information	display resilient-arp [<i>unit</i> <i>unit-id</i>]

Enable resilient ARP debugging	debugging resilient-arp { packet state error all }
Disable resilient ARP debugging	undo debugging resilient-arp { packet state error all }

3.4 Resilient ARP Configuration Example

I. Networking requirement

There are four units, numbered respectively as Unit 1 through Unit 4, in the IRF network. Unit 1 and Unit 3 are connected to the switch in link aggregation mode. Resilient ARP runs on the IRF fabric to avoid packet forwarding problems between the switch and fabric when the network has two Layer 3 units, if the links between unit 1 and unit 3, between unit 2 and unit 4 are disconnected. MD5 authentication is enabled for the sake of security. The ports of Unit 1 and Unit 3, connecting the switch, belong to VLAN 2.

II. Networking diagram

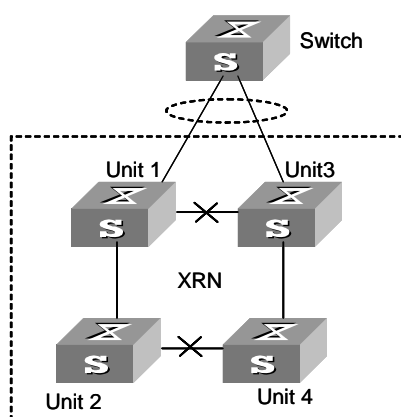


Figure 3-1 Networking for resilient ARP configuration

III. Configuration procedure

Enable resilient ARP function.

```
[Quidway] resilient-arp enable
```

Set VLAN interface 2 to send resilient ARP packets.

```
[Quidway] resilient-arp interface vlan-interface 2
```

Chapter 4 BOOTP Client Configuration

4.1 Overview of BOOTP Client

BOOTP client can request the server to allocate an IP address to it using BOOTP (bootstrap protocol). These two major processes are included on the BOOTP client:

- Sending BOOTP Request message to the server
- Processing BOOTP Response message returned from the server

In obtaining IP address using BOOTP, BOOTP client sends the server the BOOTP Request message. Upon receiving the request message, the server returns the BOOTP Response message. BOOTP client then can obtain the allocated IP address from the received response message.

The BOOTP message is based on UDP, so retransmission mechanism in the event of timeout is used to guarantee its reliable transmission. BOOTP client also starts a retransmission timer when it sends the request message to the server. If the timer expires before the return of the response message from the server, the request message will be retransmitted. The retransmission occurs every five seconds and the maximum number of retransmission is 3, that is, the message shall not be retransmitted after the third time.

4.2 BOOTP Client Configuration

BOOTP client configuration includes:

- Configuring a VLAN interface to obtain the IP address using BOOTP

4.2.1 Configuring a VLAN Interface to Obtain the IP Address Using BOOTP

Perform the following configuration in VLAN interface view.

Table 4-1 Configuring a VLAN interface to obtain the IP address using BOOTP

Operation	Command
Configure VLAN interface to obtain IP address using BOOTP	ip address bootp-alloc
Remove the configuration	undo ip address bootp-alloc

By default, the VLAN interface cannot use BOOTP to get IP address.

4.3 Debugging BOOTP Client

After the above configuration, verify the effect of the configuration.

Execute **debugging** command in user view to debug BOOTP client.

Table 4-2 Debugging BOOTP client

Operation	Command
Disable/enable hot backup debugging of BOOTP client	[undo] debugging dhcp irf xha

Chapter 5 DHCP Configuration

5.1 Overview of DHCP

5.1.1 Brief Introduction

With expansion of network size and complication of network structure, network configuration becomes more and more complex. It is often the case that computers change physical positions frequently (portable computers and wireless networks for example) and that computers exceed the IP addresses available. Dynamic host configuration protocol (DHCP) has been developed right for this situation. DHCP is in client/server structure, with DHCP client dynamic requesting configuration information, while DHCP server returning configuration information base on the specific policies.

A typical DHCP application often contains a DHCP server and several clients (desktop and laptop PCs). See the following figure.

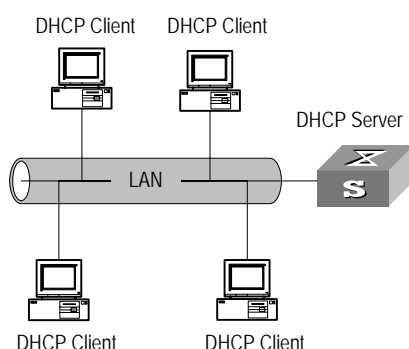


Figure 5-1 Typical DHCP application

To obtain valid dynamic IP addresses, DHCP client exchanges different types of information with the server at different stages. One of the following three situations may occur:

- 1) DHCP client logs into the network for the first time

When DHCP client logs into the network for the first time, its communication with the DHCP server includes these four stages:

- Discover stage, the stage when the DHCP client looks for the DHCP server. The client broadcasts the DHCP_Discover message and only the DHCP server can respond.

- Offer stage, the stage when the DHCP server allocates the IP address. After receiving the DHCP_Discover message from the client, the DHCP server chooses an IP address still available in IP address pool for the client, and sends to the client the DHCP_Offer message containing the leased IP address and other settings.
- Select stage, the stage when the client selects the IP address. If several DHCP servers send DHCP_Offer messages to the client, the client only accepts the first received one and then broadcasts DHCP_Request messages respectively to those DHCP servers. The message contains the information of IP address request from the selected DHCP server.
- Acknowledge stage, the stage when the DHCP server acknowledges the IP address. When receiving the DHCP_Request message from the client, the DHCP server sends the DHCP_ACK message containing the allocated IP address and other settings back to the client. Then the DHCP client binds its TCP/IP components to the NIC (network interface card).

Other DHCP servers not selected still can allocate their IP addresses to other clients later.

2) DHCP client logs into the network for a second time

When DHCP client logs into the network for a second time, its communication with the DHCP server includes these stages:

- When the DHCP client logs into the network at the first time, then at later login the client only needs to broadcast the DHCP_Request message containing the IP address obtained last time, other than the DHCP_Dscover message.
- After the reception of the DHCP_Request message, the DHCP server returns the DHCP_ACK message if the requested IP address is still not allocated, to indicate the client to continue use of the IP address.
- If the requested IP address becomes unavailable (for example, having been allocated to another client), the DHCP server returns the DHCP_NAK message. After receiving the DHCP_NAK message, the client sends the DHCP_Discover message to request another new IP address.

3) DHCP client extends its IP lease period

There is time limit for the IP addresses leased to DHCP clients. The DHCP server shall withdraw the IP addresses when their lease period expires. If the DHCP client wants to continue use of the old IP address, it has to extend the IP lease.

In practice, the DHCP client, by default, shall originate the DHCP_Request message to the DHCP server right in the middle of the IP lease period, to update the IP lease. If the IP address is still available, the DHCP server responds with the DHCP_ACK message, notifying the client that it has got the new IP lease.

The DHCP client implemented on the switch supports automatic IP lease update.

5.1.2 DHCP Relay

The earlier DHCP applied only to the case where DHCP clients and server(s) were in the same subnet, and it did not support trans-segment networking. To achieve dynamic address configuration, you have to configure a DHCP server for each subnet. Obviously, it is not economical. Introduction of DHCP relay has solved this problem: the clients in a LAN can communicate with DHCP servers in other subnet through DHCP relay, to eventually get valid IP addresses. Then DHCP clients of multiple different networks can share a DHCP server, which saves networking cost, as well as facilitating centralized management. A typical DHCP relay application is as shown in the figure below.

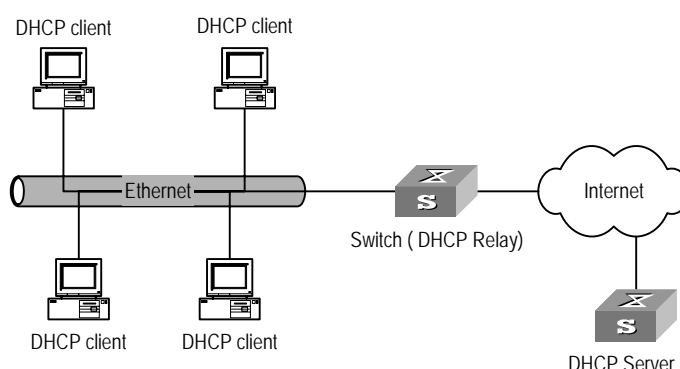


Figure 5-2 Typical DHCP relay application

DHCP Relay works on this principle:

- When the DHCP client starts and initializes DHCP, it broadcasts the request message to the local network.
- If there is a DHCP server on the local network, it can begin DHCP configuration without requiring DHCP relay function. If not, the network device with DHCP relay function which is connected with the local network, upon receiving the broadcast message, shall make proper processing and forward the message to the DHCP server of the designated network.
- The DHCP server makes proper configuration based on the information from the client and returns configuration information back to the client through DHCP relay.

In fact, several such interaction processes may be needed to complete a DHCP relay configuration.

5.2 DHCP Client Configuration

DHCP client configuration include:

- Configuring a VLAN interface to obtain IP address using DHCP

5.2.1 Configuring a VLAN Interface to Obtain IP Address Using DHCP

Perform the following configuration in VLAN interface view.

Table 5-1 Configuring a VLAN interface to obtain IP address using DHCP

Operation	Command
Configure VLAN interface to obtain IP address using DHCP	ip address dhcp-alloc
Remove the configuration	undo ip address dhcp-alloc

By default, the unit does attempt to obtain an IP address by DHCP on VLAN 1.

5.3 DHCP Relay Configuration

Note:

When the switch is in a stack, before configuring DHCP relay on the switch, you must ensure that the UDP-Helper is enabled.

DHCP relay configuration includes:

- Configuring the IP address for the DHCP server
- Configuring the DHCP server group corresponding to VLAN interfaces
- Configuring the user address entry for the DHCP server group
- Enabling/disabling DHCP security feature on the VLAN interface
- Enabling/disabling to Define Update Interval for DHCP Security Entries

5.3.1 Configuring the IP address for the DHCP server

To enhance reliability, you can set two DHCP servers on a network segment, making a DHCP server group. These two servers can be specified as the primary or the backup on themselves..

Perform the following configuration in System view.

Table 5-2 Configuring the IP address for the DHCP server

Operation	Command
Configure IP address for DHCP server	dhcp-server <i>groupNo</i> ip <i>ip_address1</i> [<i>ip_address2</i>]

Delete all DHCP server IP addresses (set the IP addresses of DHCP servers to 0)	undo dhcp-server groupNo
---	---------------------------------

By default, the corresponding IP address of the DHCP Server is not configured.

5.3.2 Configuring the DHCP Server Group Corresponding to VLAN Interfaces

Perform the following configuration in VLAN interface view.

Table 5-3 Configuring the DHCP server group corresponding to VLAN interfaces

Operation	Command
Configure DHCP server group corresponding to VLAN interfaces	dhcp-server groupNo
Delete DHCP server group	undo dhcp-server

By default, no DHCP server corresponds to VLAN interfaces.

You can just configure new correspondence between DHCP server group and VLAN interfaces, without deleting the existing correspondence. Only the last configuration is in effect if you configure the correspondence for several times.

5.3.3 Configuring the User Address Entry for the DHCP server group

To make the valid user with fixed IP address in the VLAN configured with DHCP Relay pass the address validity check of DHCP security feature, you must add a static address entry which indicates the correspondence between an IP address and an MAC address.

If another illegal user configures a static IP address which is in conflict with the fixed IP address of a valid user, the switch with DHCP Relay function enabled can identify the valid user and reject the illegal user's request for binding the IP address with the MAC address.

Perform the following configuration in system view.

Table 5-4 Configuring the user address entry for the DHCP server group

Operation	Command
Configure user address entry for DHCP server group	dhcp-security static ip_address mac_address

Delete the user address entry in the DHCP server group	undo dhcp-security { <i>ip_address</i> all dynamic static }
--	---

Note that only S3900-EI series support the configuration in S3900 series switches.

5.3.4 Enabling/Disabling DHCP Security Feature on the VLAN interface

Enabling DHCP security features will start address validity check on VLAN interface while disabling DHCP security features will cancel address validity check.

Perform the following configuration in VLAN interface view.

Table 5-5 Enabling/disabling DHCP security feature on the VLAN interface

Operation	Command
Enable DHCP security feature on VLAN interface	address-check enable
Disable DHCP security feature on VLAN interface	address-check disable

By default, DHCP security feature is disabled on the VLAN interface.

Note that only S3900-EI series support the configuration in S3900 series switches.

5.3.5 Enable/Disable to Define Update Interval for DHCP Security Entries

The dhcp-security table records the mapping of between dynamic IP addresses and MAC addresses on the DHCP relay and the mapping between the user-defined static IP addresses and MAC addresses. Regular update is required if there are dynamic IP entries in the dhcp-security table.

Please perform the following configuration in system view.

Table 5-6 Enable/disable to define an update interval for DHCP security entries

Operation	Command
Enable to define an update interval for DHCP security entries	dhcp-security tracker { <i>interval</i> auto }
Disable to define an update interval for DHCP security entries	undo dhcp-security tracker [<i>interval</i>]

Note that only S3900-EI series support the configuration in S3900 series switches.

5.4 Displaying and Debugging DHCP Configuration

After the above configuration, execute **display** command in any view to display the running of the DHCP configuration, and to verify the effect of the configuration. Execute **debugging** command in user view to debug DHCP configuration.

Table 5-7 Displaying and debugging DHCP configuration

Operation	Command
Display configuration information of DHCP server group	display dhcp-server <i>groupNo</i>
Display configuration information about the DHCP Server group corresponding to the VLAN interface	display dhcp-server interface vlan-interface <i>vlan-id</i>
Display all address information of the valid user address table for the DHCP server group	display dhcp-security [<i>ip_address</i> dynamic static tracker] [unit <i>unit-id</i>]
Display address allocation information of DHCP client	display dhcp client [verbose]
Enable/disable DHCP client debugging	[undo] debugging dhcp client { all error event packet }
Enable/disable DHCP Client hot backup debugging	[undo] debugging dhcp irf xha
Enable/disable DHCP relay debugging	[undo] debugging dhcp-relay

5.5 DHCP Relay Configuration Example

I. Networking requirements

The segment address for DHCP Client is 10.110.0.0, which is connected to a port in the VLAN2 on the switch. The IP address of DHCP Server is 202.38.1.2. The DHCP packets should be forwarded via the switch with DHCP Relay enabled. DHCP Client can get IP address and other configuration information from DHCP Server.

II. Networking diagram

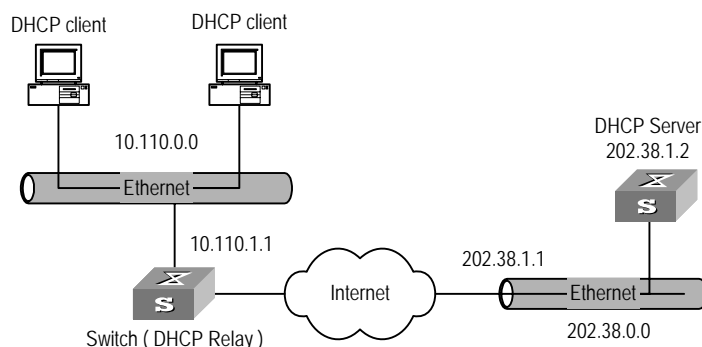


Figure 5-3 Networking diagram of configuring DHCP relay

III. Configuration procedure

Configure the group number of DHCP Server as 1 and the IP address as 202.38.1.2.

```
[Quidway] dhcp-server 1 ip 202.38.1.2
```

Associate the VLAN interface 2 with DHCP Server group 1.

```
[Quidway] interface vlan 2
```

```
[Quidway-Vlan-interface2] dhcp-server 1
```

Configure the IP address of the VLAN interface 2, which must be in the same segment as DHCP Client.

```
[Quidway-Vlan-interface2] ip address 10.110.1.1 255.255.0.0
```

To allocate IP address successfully for DHCP Client, you need to make necessary configuration on DHCP Server, which varies, depending on device type.

5.6 Troubleshooting DHCP Relay Configuration

Fault 1: The user cannot apply for IP address dynamically.

Troubleshoot: Perform the following procedures:

- Firstly, use the **display dhcp-server groupNo** command to check if the IP address of the corresponding DHCP Server has been configured.
- Secondly, use the **display vlan** and **display ip interface vlan-interface** commands to check if the VLAN and the corresponding interface IP address have been configured.
- Then make sure to ping the configured DHCP Server to ensure that the link is connected.
- Ping the IP address of the VLAN interface of the switch to which the DHCP user is connected from the DHCP Server to make sure that the DHCP Server can

correctly find the route of the network segment the user is on. If the ping execution fails, check if the default gateway of the DHCP Server has been configured as the address of the VLAN interface that it locates on.

If there is no problem found in the last two steps, use the **display dhcp-server groupNo** command to view what packet has been received. If you only see the Discover packet and there is no response packet (DHCP_OFFER messages), it means the DHCP Server has not sent the message to the switch. In this case, you shall check if the DHCP Server has been configured properly. If the numbers of request and response packets are normal, enable the **debugging dhcp-relay** in User view and then use the **terminal debugging** command output the debugging information to the console. In this way, you can view the detailed information of all DHCP packets on the console during applying for the IP address, thereby conveniently locating the problem.

Chapter 6 Access Management Configuration

6.1 Access Management Overview

In actual networking, the ports in a switch which access different subscribers belong to the same VLAN and they cannot communicate to each other, for the purpose of security, simplicity and saving VLAN resources. Different ports have different IP addresses and only the subscriber with the IP address allowed to pass the port can be accessed to the external network through the port. You can achieve this purpose using the functions binding switch port with IP address and port layer-2 isolating.

6.2 Configuring Access Management

Access management configuration includes:

- Enabling/Disabling access management function
- Configuring the access management IP address pool based on the physical port
- Configuring Layer 2 isolation between ports
- Enabling/Disabling access management trap

6.2.1 Enabling/Disabling Access Management Function

You can use the following command to enable access management function. Only after the access management function is enabled will the access management features (IP and port binding) take effect.

Perform the following configuration in system view.

Table 6-1 Enabling/Disabling access management function

Operation	Command
Enable access management function	am enable
Disable access management function	undo am enable

By default, the system disables the access management function.

6.2.2 Configuring the Access Management IP Address Pool Based on the Port

You can use the following command to set the IP address pool for access management on a port. The packet whose source IP address is in the specified pool is allowed to be forwarded on Layer 3 via the port of the switch.

Perform the following configuration in Ethernet port view.

Table 6-2 Configuring the access management IP address pool based on the port

Operation	Command
Configure the access management IP address pool based on the port	am ip-pool <i>address-list</i>
Cancel part or all of the IP addresses in the access management IP address pool of the port	undo am ip-pool { all <i>address-list</i> }

By default, the IP address pools for access management on the port are null and all the packets are permitted through.

Note that if the IP address pool to be configured contains the IP addresses configured in the static ARP at other ports, then the system prompts you to delete the static ARP to make the later binding effective.

6.2.3 Configuring Layer 2 isolation between ports

You can add a port to an isolation group using the following commands, and achieves port-to-port isolation between this port and other ports of this group, that is, Layer 2 forwarding between the isolated ports is not available.

Perform the following configuration in Ethernet port view.

Table 6-3 Configuring Layer 2 isolation between ports

Operation	Command
Add a port to the isolation group	port isolate
Remove a port from the isolation group	undo port isolate

By default, a port is not in an isolation group, namely Layer 2 forwarding is achievable between this port and other ports.

Note that:

- 1) One unit only supports one isolation group. That is, a port in an isolation group on a unit is isolated only from ports within this group, while not isolated from ports in isolation groups on other units.
- 2) The port isolation feature is synchronous on the same unit within an aggregation group, see the following details:
 - When a port in an aggregation group is added in or removed from an isolation group, then all the other ports of this aggregation group on the same unit are automatically added in or removed from this isolation group.
 - In the same aggregation group, the port isolation feature on one unit is consistent.
 - A port is removed from an aggregation group with its isolation feature not change.
 - If a port of an aggregation group is isolated on unit 1, then you can achieve the port-to-port isolation between this aggregation group and all the ports of the isolation group on unit 1.
 - If all the ports on unit 1 of this aggregation group are removed from this aggregation group, then the isolation feature of this aggregation group is disabled, that is, the port-to-port isolation mentioned above is unavailable.

6.2.4 Enabling/Disabling Access Management Trap

You can enable the access management trap function using the following commands. When this function is enabled, the trap information of access management is delivered to the console for the purpose of monitoring.

Perform the following configuration in System view.

Table 6-4 Enabling/Disabling access management trap

Operation	Command
Enable access management trap	am trap enable
Disable access management trap	undo am trap enable

By default, the access management trap is disabled.

6.3 Displaying and Debugging Access Management

After the above configuration, execute **display** command in any view to display the current configurations of access management and port isolation information, and to verify the effect of the configuration.

Table 6-5 Displaying current configuration of access management

Operation	Command
Display the status of access management function and configuration of IP address pool	display am [<i>interface-list</i>]
Display port isolation information	display isolate port

6.4 Access Management Configuration Example

I. Networking requirements

Organization 1 is connected to the port 1 of the switch, and organization 2 to the port 2. The ports 1 and 2 belong to the same VLAN. The IP addresses ranging 202.10.20.1~202.10.20.20 can be accessed from the port 1 and those ranging 202.10.20.21~202.10.20.50 from the port 2. Organization 1 and organization 2 cannot communicate with each other.

II. Networking diagram

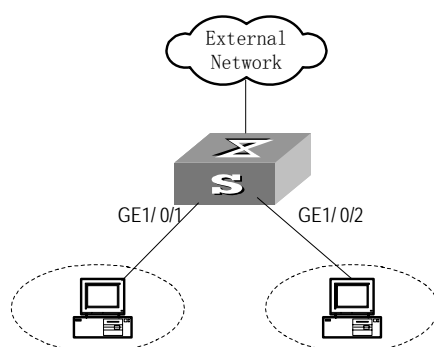


Figure 6-1 Networking diagram for port isolation configuration

III. Configuration procedure

Anable access management globally.

```
[Quidway] am enable
```

Configure the IP address pool for access management on port 1.

```
[Quidway] interface gigabitethernet1/0/1
```

```
[Quidway-GigabitEthernet1/0/1] am ip-pool 202.10.20.1 20
```

Add port 1 into isolation group.

```
[Quidway-GigabitEthernet1/0/1] port isolate
```

Configure the IP address pool for access management on port 2

```
[Quidway-GigabitEthernet1/0/1] interface gigabitethernet1/0/2  
[Quidway-GigabitEthernet1/0/2] am ip-pool 202.10.20.21 30
```

Add port 2 into isolation group.

```
[Quidway-GigabitEthernet1/0/2] port isolate
```

Chapter 7 UDP Helper Configuration

7.1 Overview of UDP Helper

The major function of UDP Helper is to relay-forward UDP broadcast packets, that is, it can convert UDP broadcast packets into unicast packets and send to the designated server, as a relay.

When UDP Helper starts, the switch can judge if to forward the UDP broadcast packets received at the port based on UDP port ID. If yes, the switch then modifies the IP address in the IP packet header and sends the packet to the designated destination server. Otherwise, it sends the packet to the upper layer module for further processing.

7.2 UDP Helper Configuration

UDP Helper configuration include:

- Enabling/disabling UDP Helper function
- Configuring UDP port with replay function
- Configuring the relay destination server for broadcast packets

7.2.1 Enabling/disabling UDP Helper Function

When UDP Helper function is enabled, you can configure the UDP ports where UDP function is required and the relay function is enabled at UDP ports 69, 53, 37, 137, 138 and 49. When the function is disabled. Relay function configured at all UDP ports, including the default six ports, shall be disabled.

Perform the following configuration in system view.

Table 7-1 Enabling/disabling UDP Helper function

Operation	Command
Enable UDP Helper function	udp-helper enable
Disable UDP Helper function	undo udp-helper enable

By default, UDP Helper function is disabled.

7.2.2 Configuring UDP Port with Replay Function

When UDP relay function is enabled, the system by default forwards the broadcast packets on the UDP ports listed in the following table. You can configure up to 256 UDP ports with relay function.

Table 7-2 Default UDP ports list

Protocol	UDP port ID
Trivial File Transfer Protocol (TFTP)	69
Domain Name System (DNS)	53
Time service	37
NetBIOS Name Service (NetBIOS-NS)	137
NetBIOS Datagram Service (NetBIOS-DS)	138
Terminal Access Controller Access Control System (TACACS)	49

Perform the following configuration in system view.

Table 7-3 Configuring a UDP port with replay function

Operation	Command
Configure a UDP port with replay function	udp-helper port { port dns netbios-ds netbios-ns tacacs tftp time }
Remove the configuration	undo udp-helper port { port dns netbios-ds netbios-ns tacacs tftp time }

Note that

- You must first enable UDP Helper function and then configure the UDP port with replay function. Otherwise, error information will appear.
- The parameters **dns** | **netbios-ds** | **netbios-ns** | **tacacs** | **tftp** | **time** respectively refer to the six default ports. You can configure the default UDP port in two ways: specifying port IDs and specifying the right parameters. For example, the **udp-helper port 53** command is equivalent to the **udp-helper port dns** command in function.
- The default UDP ports shall not be displayed when using the **display current-configuration** command. But its ID shall be displayed after its relay function is disabled.

7.2.3 Configuring the Relay Destination Server for Broadcast Packet

You can configure up to 20 relay destination servers for a VLAN interface. If a VLAN interface is configured with relay destination servers and UDP Helper function is enabled at it, then the broadcast packets of a designated UDP port received at the VLAN interface will be unicasted to the destination server.

Perform the following configuration in VLAN interface view.

Table 7-4 Configuring the relay destination server for broadcast packet

Operation	Command
Configure relay destination server for broadcast packet	udp-helper server <i>ip-address</i>
Delete relay destination server for broadcast packet	undo udp-helper server [<i>ip-address</i>]

Note that:

- The **undo udp-helper server** command without any parameter deletes all destination servers configured on the interface.
- By default, no relay destination server for UDP broadcast packets is configured.

7.3 Displaying and Debugging UDP Helper Configuration

After the above configuration, execute **display** command in any view to display the running of UDP Helper destination server, and to verify the effect of the configuration. Execute **debugging** command in user view to debug UDP Helper configuration.

Table 7-5 Displaying and debugging UDP Helper configuration

Operation	Command
Display the destination server corresponding to VLAN interface	display udp-helper server [interface vlan-interface <i>vlan-id</i>]
Enable UDP Helper debugging	debugging udp-helper { event packet [receive send] }
Disable UDP Helper debugging	undo debugging udp-helper { event packet [receive send] }

7.4 UDP Helper Configuration Example

I. Networking requirement

The IP address of VLAN interface 2 on the switch is 10.110.1.1, which is connected with network segment 10.110.0.0. Set to relay-forward the broadcast packets with destination IP of all 1s and destination UDP port 55 in the network segment 10.110.0.0 to the destination server 202.38.1.2.

II. Networking diagram

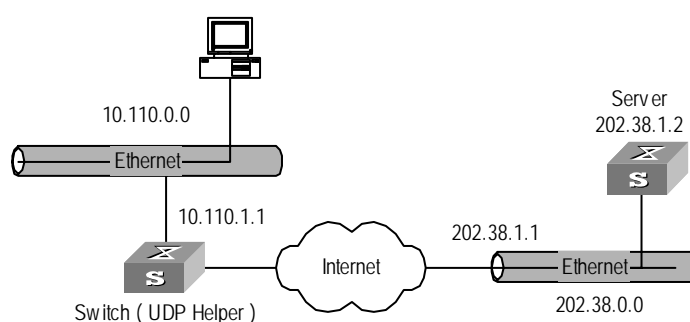


Figure 7-1 Networking for UDP Helper configuration

III. Configuration procedure

Enable UDP Helper function.

```
[Quidway] udp-helper enable
```

Set to relay-forward the broadcast packets with destination UDP port 55.

```
[Quidway] udp-helper port 55
```

Set the IP address of the destination server corresponding to VLAN interface 2 as 202.38.1.2.

```
[Quidway] interface vlan 2
```

```
[Quidway-Vlan-interface2] udp-helper server 202.38.1.2
```

Chapter 8 IP Performance Configuration

8.1 IP Performance Configuration

IP performance configuration includes:

- Configuring TCP attributes

8.1.1 Configuring TCP Attributes

TCP attributes that can be configured include:

- synwait timer: When sending the syn packets, TCP starts the synwait timer. If response packets are not received before synwait timeout, the TCP connection will be terminated. The timeout of synwait timer ranges 2 to 600 seconds and it is 75 seconds by default.
- finwait timer: When the TCP connection state turns from FIN_WAIT_1 to FIN_WAIT_2, finwait timer will be started. If FIN packets are not received before finwait timer timeout, the TCP connection will be terminated. Finwait timer ranges 76 to 3600 seconds. By default, finwait timer is 675 seconds.
- The receiving/sending buffer size of connection-oriented Socket is in the range from 1 to 32K bytes and is 8K bytes by default.

Perform the following configuration in System view.

Table 8-1 Configuring TCP attributes

Operation	Command
Configure timeout time for the synwait timer in TCP	tcp timer syn-timeout <i>time-value</i>
Restore the default timeout time of the synwait timer	undo tcp timer syn-timeout
Configure timeout time for the FIN_WAIT_2 timer in TCP	tcp timer fin-timeout <i>time-value</i>
Restore the default timeout time of the FIN_WAIT_2 timer	undo tcp timer fin-timeout
Configure the Socket receiving/sending buffer size of TCP	tcp window <i>window-size</i>
Restore the socket receiving/sending buffer size of TCP to default value	undo tcp window

By default, the TCP finwait timer is 675 seconds, the synwait timer is 75 seconds, and the receiving/sending buffer size of connection-oriented Socket is 8K bytes.

8.2 Displaying and debugging IP Performance

After the above configuration, execute **display** command in any view to display the running of the IP Performance configuration, and to verify the effect of the configuration. Execute **reset** command in user view to clear IP, TCP and UDP statistics information.

Table 8-2 Displaying and debugging IP performance

Operation	Command
Display TCP connection state	display tcp status
Display TCP connection statistics data	display tcp statistics
Display UDP statistics information	display udp statistics
Display IP statistics information	display ip statistics
Display ICMP statistics information	display icmp statistics
Display socket interface information of current system	display ip socket [socktype <i>sock-type</i>] [<i>task-id</i> <i>socket-id</i>]
Display the summary of the Forwarding Information Base	display fib
Display the FIB entries matching the destination IP address (range)	display fib <i>ip_address1</i> [{ <i>mask1</i> <i>mask-length1</i> } [<i>ip_address2</i> { <i>mask2</i> <i>mask-length2</i> }] longer] longer]
Display the FIB entries matching a specific ACL	display fib acl <i>number</i>
Display the FIB entries which are output from the buffer according to regular expression and related to the specific character string	display fib { { begin include exclude } <i>text</i> }
Display the FIB entries matching the specific prefix list	display fib ip-prefix <i>listname</i>
Display the total number of FIB entries	display fib statistics [{ begin include exclude } <i>text</i>]
Reset IP statistics information	reset ip statistics
Reset TCP statistics information	reset tcp statistics
Reset UDP statistics information	reset udp statistics

8.3 Troubleshooting IP Performance

Fault: IP layer protocol works normally but TCP and UDP cannot work normally.

In the event of such a fault, you can enable the corresponding debugging information output to view the debugging information.

- Use the **terminal debugging** command to output the debugging information to the console.
- Use the command **debugging udp packet** to enable the UDP debugging to trace the UDP packet.

The following are the UDP packet formats:

UDP output packet:

Source IP address:202.38.160.1

Source port:1024

Destination IP Address 202.38.160.1

Destination port: 4296

- Use the **debugging tcp packet** command to enable the TCP debugging to trace the TCP packets.

Operations include:

```
[Quidway] terminal debugging
```

```
<Quidway> debugging tcp packet
```

Then the TCP packets received or sent can be checked in real time. Specific packet formats include:

TCP output packet:

Source IP address:202.38.160.1

Source port:1024

Destination IP Address 202.38.160.1

Destination port: 4296

Sequence number :4185089

Ack number: 0

Flag :SYN

Packet length :60

Data offset: 10