Table of Contents

Chapter 1 IP Address Configuration

1.1 IP Address Overview

IP addresses are unique 32-bit addresses assigned to hosts connected to Internet. An IP address is composed of two parts: network ID and host ID. Its structure enables convenient addressing on Internet. IP addresses are assigned by Network Information Center (NIC) of American National Defense Data Network.

IP address consists of the following fields:

- Network ID field (net-id), among which the former bits are called the category field (or category bits) used to distinguish the types of IP addresses.
- Host ID field (host-id). Since host number with all 1s or 0s has special usage, it is specified that the host number should not be all 1s or 0s.

For easy IP address management and convenient networking, IP address of Internet is divided into five classes. As shown in the following diagram:

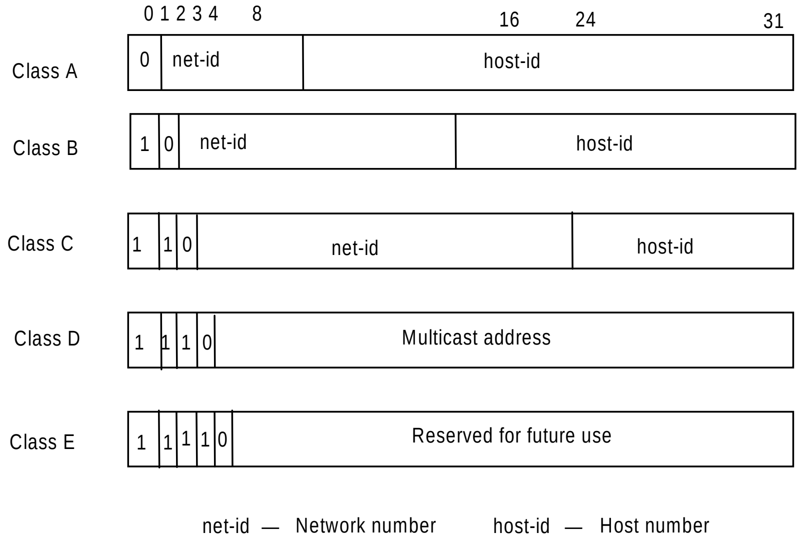


Figure 1-1 Classification of IP address

Address of class D is a multicast address, mainly used by IAB (Internet Architecture Board). Address of class E is reserved for future use. At present, most IP addresses are class A, class B and class C.

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	Description
A	0.0.0.0 to 127.255.255.255	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.
B	128.0.0.0 to 191.255.255.255	—
C	192.0.0.0 to 223.255.255.255	—
D	224.0.0.0 to 239.255.255.255	Addresses of class D are multicast addresses.
E	240.0.0.0 to 255.255.255.255	255.255.255.255 is a broadcast address, and the others are reserved for future use.

Important features of IP address:

- IP addresses are not in a hierarchical structure, which is different from the structure of telephone number. In other words, IP addresses cannot reflect any geographical information about the host position.
- When a host is connected to two networks at the same time (such as the host used as a router), it must have two IP addresses with different net-ids corresponding to two different networks. Such host is called multi-homed host.
- According to Internet concept, several LANs connected via transceiver or bridge are still in the same network, so these LANs have the same net-id.
- With respect to IP address, all networks with a net-ids are equal (no matter it is a small LAN or a huge WAN).

Since 1985, only the net-id of IP address is assigned by NIC, while the host-id is controlled by the enterprise. The IP address assigned to an enterprise is only a network ID: net-id. The specific host Ids, the host-ids for respective hosts, shall be assigned by the enterprise independently, so long as there is no repetition of host IDs within its network.

If there are many enterprise hosts widely scattered, the host IDs may be further divided into internal sub-nets to facilitate management. Note that the division of sub-nets is decided by the enterprise itself and the subnets cannot be seen from outside the enterprise. Seen from the outside, the enterprise only has one net-id. When an external packet enters this enterprise network, the internal router can route according to the sub-net number, and finally reach the destination host.

The following figure shows the sub-net classification of a Class B IP address, in which a sub-net mask consists of a string of continuous "1" s and a string of continuous "0" s.

The 1s corresponds to the network ID field and the sub-net number field, while the 0s correspond to the host ID field.

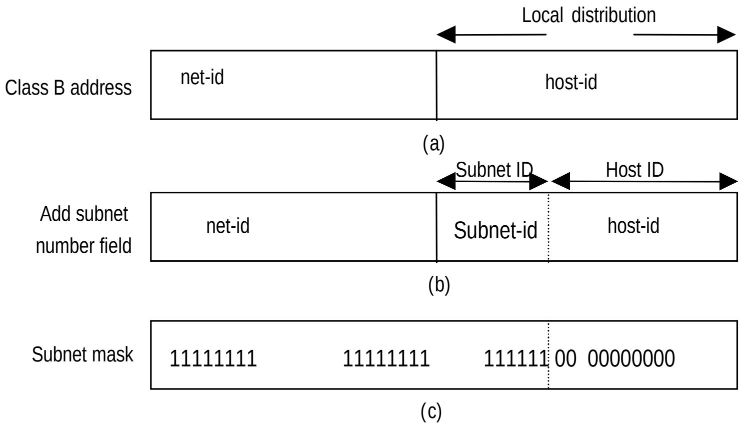


Figure 1-2 Sub-net classification of IP address

Classification of one more sub-net number field is at a price. For example, an IP address of class B originally consists of 65534 (2^{16}-2) host IDs. However, after a 6-bit-long sub-net field is classified, there may be at most 64 sub-nets. Each sub-net has 10-bit host ID, i.e., each sub-net has 1022 host IDs at most. There are 64 x 1022=65408 host IDs in total, 126 less than the sum before sub-net classification.

If there is no sub-net division in an enterprise, 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.

A router used to connect multiple sub-nets together will have multiple sub-net IP addresses.

The IP addresses mentioned above cannot be directly used in communication, because:

- 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 first resolved into a physical address.
- IP address is hard to remember, but a host domain name will be much easier to remember and is also more popular. So the host domain name must also be resolved into an IP address.

The following figure illustrates relations among host name, IP address and physical address.

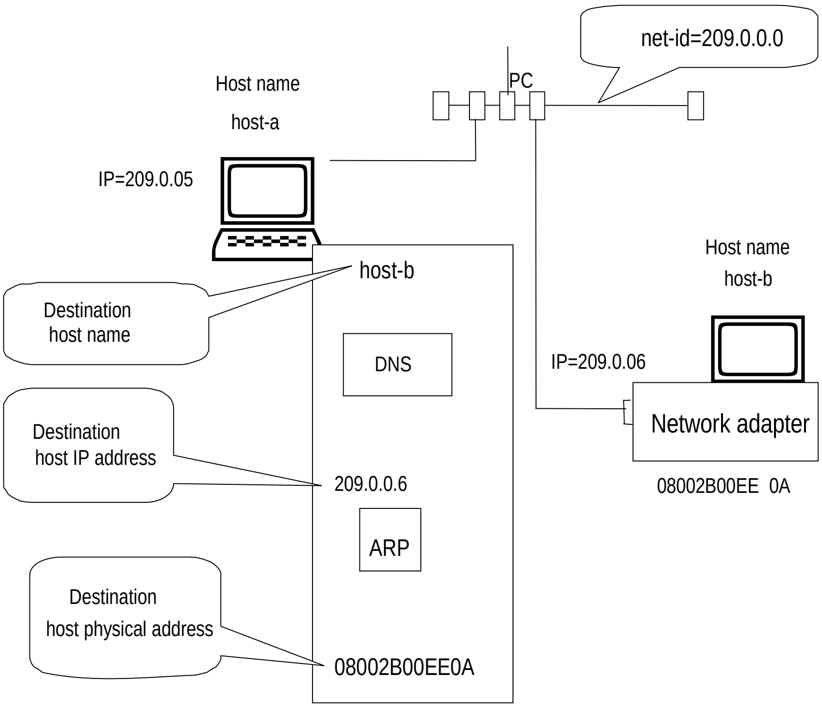


Figure 1-3 Relation between host name, IP address, and physical address

1.2 IP Address Configuration

IP address configuration includes:

- Assigning IP Addresses to an Interface
- Configuring IP Address Unnumbered for an Interface

1.2.1 Assigning IP Addresses to an Interface

Each interface of a router can have multiple IP addresses, among which one is the main IP address and the others are subordinate IP addresses (also called secondary IP addresses).

When assigning IP addresses to an interface, consider the following:

- A father interface and its subinterfaces must not reside on the same network segment.
- Peer interfaces must not reside on the same network segment.
- A main interface and a subordinate IP address can be in the same network segment.

I. Assigning a main IP address to an interface

Each interface can be assigned only one main IP address.

Perform the following configuration in interface view.

Table 1-2 Configure main IP address of an interface

Operation	Command
Configure main IP address of an interface	**ip address** *ip-address net-mask*

A mask identifies the netid boundary of an IP address. Suppose an Ethernet interface is assigned the IP address 129.9.30.42 with the mask of 255.255.0.0. Logic AND the IP address with the mask; then you can know that the Ethernet interface is assigned to the network segment 129.9.0.0.

Your main IP address configuration can overwrite the existing one, if there is any.

By default, no main IP address is assigned to any interface.

II. Configuring subordinate IP address of an interface

Besides the main IP address, several subordinate IP addresses can be configured on an interface. The purpose of assigning subordinate IP addresses is to have the same interface located in different sub-nets, to create network routes with the same interface as the output port, and set up connection via the same interface to multiple sub-nets.

Perform the following configuration in interface view.

Table 1-3 Configure a subaddress on an interface

Operation	Command
Configure a subaddress on an interface.	**ip address** *ip-address net-mask* **sub**

By default, no subaddress is configured.

You can configure up to 32 addresses on an interface, including the main IP address and subaddresses.

⚠ **Caution:**

For an interface that is configured to allocate IP addresses through BOOTP, DHCP, or PPP negotiation, you cannot define subaddresses.

III. Deleting IP addresses on an interface

Perform the following configuration in interface view.

Table 1-4 Delete IP addresses on the interface

Operation	Command
Delete IP addresses on the interface.	**undo ip address** [*ip-address net-mask* [**sub**]]

To delete all IP addresses on the interface, execute this command without specifying any argument.

To delete the main IP address, use the **undo ip address** *ip-address net-mask* command.

To delete subordinate addresses, use the **undo ip address** *ip-address net-mask* **sub** command.

Before you can delete the main IP address, you must delete all subordinate addresses.

IV. Setting negotiable attribute of an IP address for an interface

If a PPP-encapsulated interface is not assigned an IP address while its peer has been assigned one, you may configure PPP address negotiation to have it accept the address assigned by the peer. For example, when accessing the Internet through an ISP, you may use the **ip address ppp-negotiate** command to accept the addresses assigned by the ISP.

Perform the following configuration in interface view.

Table 1-5 Set negotiable attribute of IP address for an interface

Operation	Command
Set negotiable attribute of IP address for an interface	**ip address ppp-negotiate**
Cancel negotiable attribute of IP address for an interface	**undo ip address ppp-negotiate**

By default, the system does not allow to negotiate the interface IP address. For detailed configuration information about PPP interface address negotiation, refer to the section related to PPP protocol in the “Link Layer Protocol” part of this manual.

Caution:

- Because PPP supports IP address negotiation, IP address negotiation of an interface can be set only when the interface is encapsulated with PPP. When the PPP link is down, the IP address originated from negotiation will be deleted.
- If the interface has original address, then after setting IP address of the interface to negotiable, the original IP address will be deleted.
- After setting IP address of an interface to negotiable, it is unnecessary to configure IP address for the interface, as negotiation will automatically originate an IP address.
- After setting IP address of an interface to negotiable, if the interface is set to negotiable again, then the IP address originated from the original negotiation will be deleted, and the interface obtains IP address through the re-negotiation.
- The interface will have no address after the negotiation address is deleted.

1.2.2 Configuring IP Address Unnumbered for an Interface

I. Introduction to IP Address Unnumbered

The main purpose of borrowing IP address is to save IP address resource.

If an interface has no IP address, it can neither generate any route nor forward any packet. "IP Address Unnumbered" is used when you want to use an interface with no IP address. In such case, an IP address will be borrowed from another interface. If the lending interface has multiple IP addresses, then only the main one can be borrowed. However, if the lending interface has no IP address, then the IP address of the borrowing interface is 0.0.0.0. This function is implemented through the command **ip address unnumbered**.

The following should be noted:

- The borrower cannot be an Ethernet interface.
- The address of the lending interface cannot be an unnumbered address.
- The lending interface can lend its address to multiple interfaces.
- The address of Loopback interface can be borrowed by other interfaces, but it cannot borrow the addresses of other interfaces.

Because the borrowing interface has no IP address of its own, and cannot route, two static routes need to be configured manually to connect routers together. Refer to the configuration examples for the specific configuration procedure.

⚠ **Caution:**

After configuring an IP address unnumbered for a tunnel interface, you must configure an IP address for the peer interface of the tunnel and ensure that the subnet mask is 32 bits in length.

II. IP Address Unnumbered configuration task list

The configuration of IP Address Unnumbered can be performed in the interface view. Serial interfaces encapsulated with PPP, HDLC, Frame Relay, SLIP and Tunnel interface can borrow the IP addresses of the Ethernet interface and other kinds of interfaces.

IP Address Unnumbered configuration includes:

- Activating/deactivating IP address unnumbered

III. Activating/deactivating IP address unnumbered

Perform the following task in the interface view to activate/deactivate IP address unnumbered.

Table 1-6 Configure IP address unnumbered

Operation	Command
Activate IP address unnumbered	**ip address unnumbered interface** *interface-type interface-number*
Deactivate IP address unnumbered	**undo ip address unnumbered**

By default, IP address unnumbered is disabled.

1.2.3 Displaying and Debugging IP Address

After the above configuration, execute display command in any view to display the running of the IP Address, and to verify the effect of the configuration.

Table 1-7 Display and debug IP address

Operation	Command
Display IP-related information about the specified or all interfaces	**display ip interface** [*interface-type interface-number*]
Display IP-related summary about the specified or all interfaces	**display ip interface brief** [*interface-type interface-number*]

1.2.4 Displaying and Debugging IP Address Unnumbered

After the above configuration, execute display command in any view to display the running of the IP Address unnumbered, and to verify the effect of the configuration.

Table 1-8 Display and debug IP Address Unnumbered

Operation	Command
Display information of IP Address Unnumbered	**display interface** [*interface-type* [*interface-number*]]

1.2.5 IP Address Configuration Example

I. Network requirements

To configure IP addresses for a router's serial interface, it is required that the main IP address is 129.2.2.1, and the subordinate IP address is 129.1.3.1.

II. Network diagram

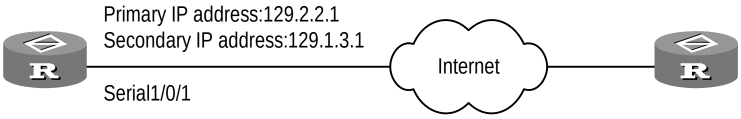


Figure 1-4 Configure the main and subordinate IP address for a router's interface

III. Configuration procedure

# Configure the main and subordinate IP address for router's interface serial1/0/1.

```
[Quidway] interface serial 1/0/1
[Quidway-Serial1/0/1] ip address 129.2.2.1 255.255.255.0
[Quidway-Serial1/0/1] ip address 129.1.3.1 255.255.255.0 sub
```

1.2.6 IP Address Unnumbered Configuration Example

I. Network requirements

Suppose the headquarters of a company is in Beijing, with one subsidiary in Shenzhen and Shanghai respectively and one office in Wuhan. Its networking diagram is shown in the following figure. R is the headquarters router, which connects the subsidiaries and office routers R1, R2 and R3 through PSTN. The four routers R, R1, R2 and R3 each have a serial port for dialing and one Ethernet interface to connect with local network.

II. Network diagram

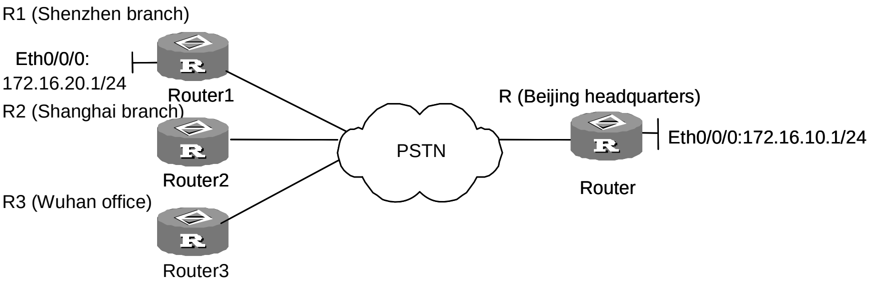


Figure 1-5 Network diagram for IP address unnumbered configuration

III. Configuration procedure

1) Configure headquarters router R

```
[Quidway-Ethernet1/0/0] ip address 172.16.10.1 255.255.255.0
```

# Borrow IP address of Ethernet.

```
[Quidway-Serial2/0/0] ip address unnumbered interface ethernet 1/0/0
[Quidway-Serial2/0/0] link-protocol ppp
```

# Configure routing to Ethernet segment of Shenzhen router R1.

```
[Quidway] ip route-static 172.16.20.0 255.255.255.0 172.16.20.1
```

# Configure the interface routing to Shenzhen router R1 serial interface.

```
[Quidway] ip route-static 172.16.20.0 255.255.255.0 serial2/0/0
```

2) Configure router R1 at Shenzhen branch

```
[Quidway-Ethernet1/0/0] ip address 172.16.20.1 255.255.255.0
```

# Borrow IP address of Ethernet.

```
[Quidway-Serial2/0/0] ip address unnumbered interface ethernet 1/0/0
[Quidway-Serial2/0/0] link-protocol ppp
```

# Configure routing to Ethernet segment on Beijing headquarters router R, this routing is default routing.

```
[Quidway] ip route-static 0.0.0.0 0.0.0.0 172.16.10.1
```

# Configure interface routing to serial interface of Beijing router R.

```
[Quidway] ip route-static 172.16.10.1 255.255.255.255 serial2/0/0
```

1.2.7 Troubleshooting IP Address Configuration

A router is a network interconnection device. So when IP address for an interface is configured, networking requirements and sub-net classification should be known. Normally, the following rules should be observed:

- The main IP address of a router Ethernet interface must be in the same network segment with the LAN to which this Ethernet interface is connected.

- Serial interface IP addresses of the routers at both ends of WAN must be in the same network segment.

Fault 1: the router cannot **ping** through a certain host in LAN

Troubleshooting:

- First check if the IP address configuration of the router's Ethernet interface and the host in LAN are in the same network segment
- If the configuration is correct, enable ARP debugging on the router, and check if the router can correctly send and receive ARP packets. If it can only send but cannot receive ARP packets, then possibly errors occur on the Ethernet physical layer.

Chapter 2 ARP Configuration

2.1 Dynamic/Static ARP Configuration

2.1.1 Introduction to Dynamic ARP

ARP (Address Resolution Protocol) is mainly used for resolution from IP address to Ethernet MAC address. Normally, dynamical ARP is used to resolve the mapping relation from the IP address to the Ethernet MAC address. The resolution is completed automatically without interference of the administrator.

In the implementation of VRP the system creates or updates ARP entries when receiving an ARP message compliant with one of the following conditions:

- The source IP address is a non-broadcast address located in the same segment attached to the receiving interface, the destination IP address is the same as the IP address of the interface.
- The source IP address is a non-broadcast address located in the same segment attached to the receiving interface, the destination IP address is the VRRP virtual IP address on the interface.
- The destination IP address is included in the NAT address pool on the receiving interface.

In addition, if one ARP entry has existed for the source IP address, the system updates the entry.

2.1.2 Brief Introduction to Static ARP

Static ARP applies to:

- Bind packets destined to an address beyond this segment to a network adapter, so that they can be forwarded through this gateway.
- Filter out invalid IP addresses by binding them to a MAC address that does not exist.

2.1.3 Static ARP Configuration

The static ARP configuration includes:

- Manually add/delete static ARP mapping table item.

Perform the following task in the system view.

Table 2-1 Manually add/delete static ARP mapping table item

Operation	Command
Manually add static ARP mapping table item	**arp static** *ip-address ethernet-address* [*vpn-instance-name*]
Manually delete static ARP mapping table item	**undo arp** *ip-address* [*vpn-instance-name*]

While the lifetime of dynamic ARP mappings is only 20 minutes, static ARP mappings never age out.

The ARP table on the router can accommodate up to 2048 static entries.

By default, address mappings are obtained through dynamic ARP.

2.1.4 Dynamic ARP Configuration

I. Enabling/disabling ARP entry check (optional)

You can enable or disable the device to learn the ARP entries with broadcast MAC addresses.

Perform the following configuration in system view.

Table 2-2 Enable/disable ARP entry check

Operation	Command
Enable ARP entry check to have the device not learn the ARP entries with broadcast MAC addresses.	**arp check enable**
Disable ARP entry check to have the system learn the ARP entries with broadcast MAC addresses.	**undo arp check enable**

By default, ARP entry check is enabled. The device does not learn the ARP entries with broadcast MAC addresses.

II. Enabling/disabling ARP request in the scope of natural network segments (optional)

ARP request is usually restricted only in subnets, but you are allowed to enable ARP request in the scope of natural segments.

Perform the following configuration in system view.

Table 2-3 Enable/disable ARP request in the scope of natural network segments

Operation	Command
Enable ARP request in the scope of natural segments.	**naturemask-arp enable**
Disable ARP request in the scope of natural segments.	**undo naturemask-arp enable**

By default, ARP request in the scope of natural network segments is not supported.

III. Setting the aging timer for dynamic ARP entries

Perform the following configuration in system view.

Table 2-4 Set the aging timer for dynamic ARP entries

Operation	Command
Set the aging timer for dynamic ARP entries	**arp timer aging** *minutes*
Restore the default setting of the aging timer for dynamic ARP entries	**undo arp timer aging**

By default, the aging timer for dynamic ARP entries is set to 20 minutes.

2.1.5 Displaying and Debugging ARP

After the above configuration, execute the **display** command in any view to display the running of the ARP configuration, and to verify the effect of the configuration.

Execute the **debugging** command in user view for the debugging of ARP configuration.

Table 2-5 Display and debug ARP

Operation	Command
Show ARP mapping table	**display arp** [**static** | **dynamic** | **all**]
Display the aging timer for dynamic ARP entries (only for the AR46 Series)	**display arp timer aging**
Clear the ARP entries in the ARP mapping table	**reset arp** [**all** | **dynamic** | **static** | **interface** *interface-type interface-number*]
Enable ARP information debugging	**debugging arp packet**
Disable ARP information debugging	**undo debugging arp packet**

2.2 Proxy ARP Configuration

2.2.1 Introduction

You can assign physically distributed computers and routers to the same network segment by assigning them IP addresses in the same network segment. Proxy ARP allows them to communicate with each other as they would in the same physical network.

The late 1980s witnessed an explosive growth of LANs along with the development of network applications. A good example is that even the Ethernet of a university could be connected to as many as hundreds of hosts. This increased the likelihood of collisions on the Ethernet. In addition, to implement new applications, a LAN must be expanded, for example, by using repeaters to connect new computers. This however, might cause overload and decrease network performance because of presence of heavy collisions. To solve the problem, proxy ARP was thus introduced.

2.2.2 Application Environments for Proxy ARP

Proxy ARP functions to connect two networks that are physically separated but on the same IP network segment at the same.

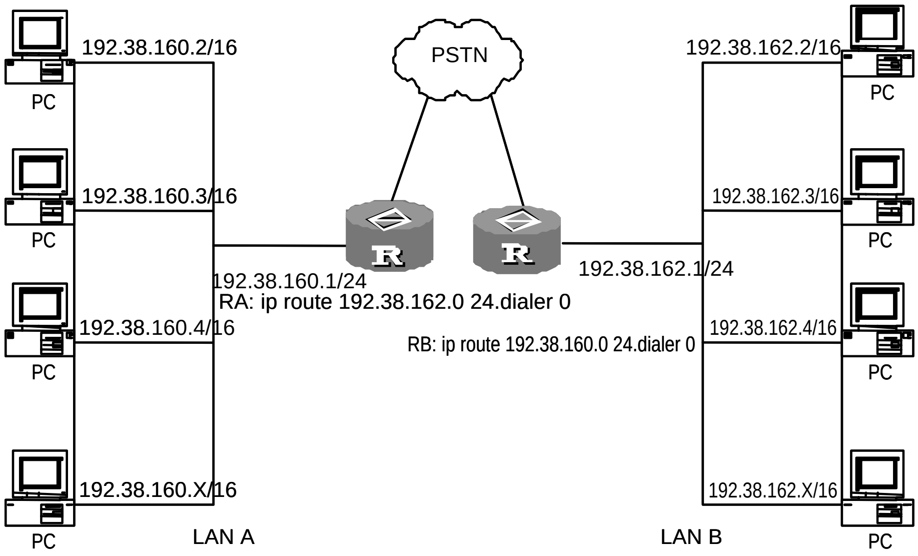


Figure 2-1 Application environment for proxy ARP

The scenario in the above figure illustrates that:

- LAN A and LAN B are connected each to an Ethernet interface on a router.
- All hosts on the LANs belong to network segment 192.38.0.0, with LAN using 192.38.160.0 and LAN B using 192.38.162.0.
- For both LANs, the host mask is 16 bits. As the result, all hosts on the LANs consider that they are located on the network segment 192.38.0.0.

- On the two routers, the involved interfaces are assigned to the 192.38.0.0 segment and enabled with proxy ARP.
- The two routers are connected through PSTN and each configured with a static route to the network segment of the opposite end.

Assume that the IP address of Host A on LAN A is 192.38.160.2, and the IP address of Host B on LAN B is 192.38.162.2. The following is how ARP works when Host A accesses Host B:

- Host A sends an ARP request for reaching Host B.
- Router A receives the request and looks up its routing table. If finding a routing entry, 192.38.162.0 for example, for reaching Host B, the router sends back an ARP response with its own MAC address included.
- After receiving the ARP response, Host A sends IP packets to Router A.
- After receiving the IP packets, Router A forwards them to Router B.
- Router B forwards the received IP packets to Host B.

To send responses to Host A, Host B undergoes the same procedure.

Thus, these two physically separated hosts can access each other as they would on the same physical network.

2.2.3 Configuring Proxy ARP

Perform the following configuration in Ethernet interface view.

Table 2-6 Enable/disable proxy ARP

Operation	Command
Enable proxy ARP function	**arp-proxy enable**
Disable proxy ARP function	**undo arp-proxy enable**

By default, proxy ARP is disabled.

2.3 Gratuitous ARP Configuration

2.3.1 Introduction to Gratuitous ARP

A network device can check for IP address conflicts with other devices by sending gratuitous ARP messages.

When the network device broadcasts a gratuitous ARP message, it sets both the source and destination IP addresses to local addresses, and sets the source MAC address to a local MAC address. Every receiving device checks the IP addresses in the received gratuitous ARP message and sends back an ARP response if detecting an address conflict.

In addition, by sending gratuitous ARP messages, a network device can update its current hardware address to the caches on other devices if a hardware address change has occurred for example, after the device reconnected to the network with a new interface card. As ARP requests are broadcast, this update involves all devices on the network.

The following are characteristics of gratuitous ARP packets:

- Both source and destination IP addresses are local addresses, and their source MAC addresses are local MAC addresses.
- If a device finds that the IP addresses carried in a received gratuitous packet are in conflict with the address of its own, it returns an ARP response to the sending device.

2.3.2 Enabling the Address Learning Function of Gratuitous ARP

Perform the following configuration in system view.

Table 2-7 Enable the address learning function of gratuitous ARP

Operation	Command
Enable the address learning function of gratuitous ARP	**gratuitous-arp-learning enable**
Disable the learning function of gratuitous ARP	**undo gratuitous-arp-learning enable**

By default, the address learning function of gratuitous ARP is disabled.

2.3.3 Responding to the ARP Requests from Other Network Segments

Perform the following configuration in system view.

Table 2-8 Respond to the ARP requests from other network segments

Operation	Command
Enable the system to respond to the ARP requests from other network segments	**gratuitous-arp-sending enable**
Disable the system to respond to the ARP requests from other network segments	**undo gratuitous-arp-sending enable**

By default, the router does not respond to the ARP requests received from other network segments.

2.3.4 Sending Gratuitous ARP Message Periodically and Setting the Sending Interval

Perform the following configuration in Ethernet interface view, Ethernet subinterface view, Gigabit Ethernet interface view, Gigabit Ethernet subinterface view, bridge template view, VLAN interface view or virtual Ethernet interface view.

Table 2-9 Send gratuitous ARP message periodically and set the sending interval

Operation	Command
Enable the interface to send gratuitous ARP message periodically and set the sending interval	**arp send-gratuitous-arp** *seconds*
Disable the interface from sending gratuitous ARP message periodically	**undo arp-gratuitous-arp**

By default, the interface does not send gratuitous ARP message periodically.

2.3.5 Mapping between WAN Interface IP Address and Link Layer Protocol Address

In a router, you shall maintain both the mapping from an Ethernet interface IP address to an MAC address, and that from a WAN interface IP address to a link layer protocol address. Namely there are the following types:

- On an interface encapsulated with X.25, the mapping between an IP address and X.121 address is maintained by the command **x25 map ip**.
- On an interface encapsulated with Frame Relay, mapping between an IP address and a virtual circuit number (DLCI) is maintained by the command **fr map ip**.

The above mapping tables are also called second routing, which is essential to the normal working of the router. For details, refer to related chapters in "Link Layer Protocol" of this manual.

2.4 Authorized ARP Configuration

2.4.1 Introduction to Authorized ARP

Authorized address resolution protocol (authorized ARP) enables the DHCP server or other modules to automatically add authorized ARP entries to the ARP table based on certain conventions. Allowing only static entries and entries with IP addresses from the DHCP server to be added to the ARP table, authorized ARP can stop a DHCP server learning dynamically from illegal ARP responses, making illegal clients unable to access the Internet. Authorized ARP also provides a probing mechanism called ARP ping. It can identify a log-off DHCP client and notify the DHCP Server of that. By deploying authorized ARP, you can achieve both enhanced network security and quick detection of a client going down.

🕮 **Note:**

- Currently, authorized ARP can only be implemented on a router with the DHCP server function enabled.
- Currently, authorized ARP supports only the scenario that the DHCP server and DHCP clients are on the same segment.

2.4.2 Basic Concepts

- ARP cache

Each host has an ARP cache, in which the recently learned mappings between the IP addresses and hardware addresses are kept. By default, the lifetime of each entry in the cache is 20 minutes.

During ARP translation, the ARP cache is searched at first. If no match is found, the ARP table is searched.

- ARP table

An ARP table keeps the mappings between IP addresses and physical addresses. A mapping can be generated dynamically, statically, or by any other way. Each device maintains an ARP table.

The fields of the ARP table are IF index, physical address, IP address, and type.

- ARP ping

The aging of authorized ARP is implemented by a mechanism called ARP ping. By periodically sending an ARP request to the IP address of a client recorded in an authorized ARP entry, ARP ping can detect whether the client is down. Whenever receiving an ARP response, whether the response is triggered by ARP ping or not, authorized ARP refreshes the aging time of the entry. ARP ping provides the DHCP server an initiative client status inquiry mechanism, enabling the DHCP server to detect offline clients in a shorter period of time and release the resources assigned to them.

- Authorized ARP entry

Authorized ARP entry is a kind of special entry. An authorized ARP entry is also added into the ARP table of the device, and has the features of the static ARP entry and the dynamic ARP entry. An authorized ARP entry has a higher priority than a dynamic ARP entry for the same mapping; a new authorized ARP entry overrides a dynamic ARP entry, while a new dynamic ARP entry cannot override an authorized ARP entry.

At the same time, an authorized ARP entry has a lower priority than a static ARP entry for the same mapping; a new authorized ARP entry cannot override a static ARP entry, while a new static ARP entry overrides an authorized ARP entry.

The aging mechanism of authorized ARP is similar to that of dynamic ARP; they determine whether an entry needs to be aged by recording and refreshing the aging time of the entry. The aging of an authorized ARP entry is implemented by ARP ping, which is independent of the aging of a dynamic ARP entry.

The default aging time of an authorized ARP entry is the time that three ARP ping operations takes when no responses are received. Since the ARP ping interval is 30 seconds, the default aging time of an authorized ARP entry is 90 seconds. If no response is received for an authorized ARP entry or if the DHCP server fails to update the entry by re-adding the entry for example, after 90 seconds elapse, the entry ages out. The DHCP server is then notified of this.

An authorized ARP entry can be removed manually or automatically by the DHCP server.

- ARP security

For the sake of security, authorized ARP provides the ARP security function to disable dynamic ARP learning. When you enable this function, only static ARP entries and authorized ARP entries are allowed to be populated into the ARP table, while dynamic ARP learning is prohibited.

ARP security is independent of authorized ARP, and can be employed independently.

2.4.3 Structure of the ARP Packet

ARP packets fall into two categories: ARP request and ARP response. The following table illustrates the structure of the ARP request and response. For an ARP request, the field of hardware address of the receiver (that is, the address the sender wants to obtain) is null, and all other fields are employed. An ARP response employs all the fields.

Hardware type (16 bits)	
Protocol type (16 bits)	
Length of the hardware address	Length of protocol address
Operator (16 bits)	
Hardware address of the sender	
IP address of the sender	
Hardware address of the receiver	
IP address of the receiver	

Figure 2-2 Structure of the ARP request and ARP response

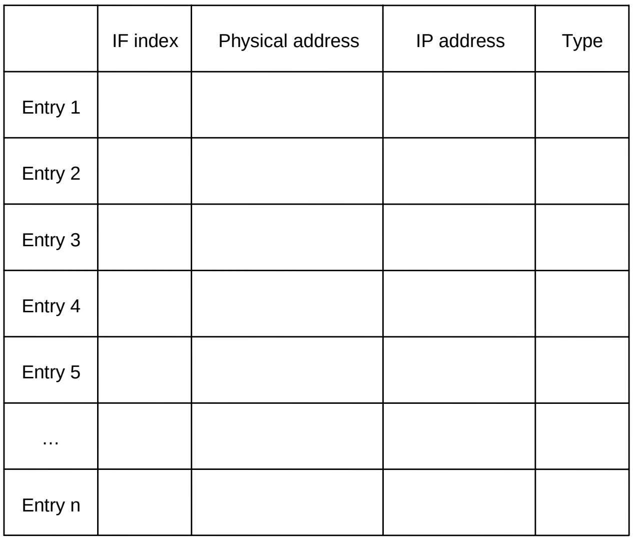
- Hardware type: Identifies the type of the hardware interface. The following table lists the valid values.

Table 2-10 Valid hardware interface types

Type	Description
1	Ethernet
2	Experimental Ethernet
3	X.25
4	Proteon ProNET
5	Chaos
6	IEEE802.X
7	ARC network

- Protocol type: Identifies the type of the protocol used by the sending device. In TCP/IP, it is usually EtherType.
- Length of the hardware address: Number of bytes in the hardware address.
- Length of protocol address: Number of bytes in the protocol address.
- Operator: Indicates whether the ARP packet is an ARP request or an ARP response. It can be 1 (for ARP request), 2 (for ARP response), 3 (for RARP request), or 4 (for RARP response).
- Hardware address of the sender: Hardware address of the sending device.
- IP address of the sender: IP address of the sending device.
- Hardware address of the receiver: Hardware address of the receiving device. In an ARP request, this field is null. In an ARP response, this field carries the hardware address of the receiver.
- IP address of the receiver: IP address of the receiving device.

2.4.4 ARP Table



	IF index	Physical address	IP address	Type
Entry 1				
Entry 2				
Entry 3				
Entry 4				
Entry 5				
…				
Entry n				

Figure 2-3 ARP table

- IF index: Physical interface or port on the device owning the physical address and IP address.
- Physical address: Physical address of the device, that is, the MAC address.
- IP address: IP address of the device.
- Type: Type of the entry, which can be 2 for an invalid entry, 3 for a dynamically learned entry, 4 for a statically configured entry, or 1 for an entry falling out of the previous three cases.

2.4.5 Fundamentals of Authorized ARP

The authorized ARP mechanism is a combination of the ARP mechanism and the DHCP mechanism. Currently, authorized ARP does not support DHCP relay. The following explains the operation of authorized ARP in a scenario with the DHCP clients and DHCP servers on the same segment:

1) A DHCP client broadcasts a DHCP_DISCOVER packet. When a DHCP server receives the broadcast packet, it responds with a DHCP_OFFER packet, in which the DHCP server fills the configuration parameters for the DHCP client.
2) If more than one DHCP server is present on the network and responds to the client, the client accepts the configuration parameters in the first received DHCP_OFFER packet and broadcasts a DHCP_REQUEST packet on the network. The DHCP_REQUEST packet contains the MAC address of the client and the IP address the client is ready to use.
3) After a DHCP server receives the DHCP_REQUEST packet of a client, it responds to the client with a DHCP_ACK packet. At the same time, the DHCP server adds an authorized ARP entry into the local ARP table, which contains the

MAC address and IP address of the client, and the interface owning the addresses.

4) Once an authorized ARP entry is added into the ARP table of the DHCP server, the ARP ping mechanism is initiated to implement the aging of the authorized ARP entry. That is, ARP ping periodically sends an ARP request to the IP address of the client recorded in the authorized ARP entry to determine whether the client is down. If ARP ping sends three ARP requests but receives no response, it considers that the client is down, and then removes the authorized ARP entry from the ARP table.

5) For the sake of security, authorized ARP provides the ARP security function. When you enable this function, only static ARP entries and authorized ARP entries are allowed to be populated into the ARP table, while dynamically learned ARP entries are prohibited. Therefore, if the DHCP server acts as the gateway for accessing the Internet, illegal hosts with fixed addresses will not be able to access the Internet.

2.4.6 Configuring Authorized ARP

I. Configuration Prerequisites

Before configuring authorized ARP, complete the following configurations:

- Enable the DHCP server function on the router acting as the DHCP server, and configure the DHCP server parameters such as address pool.
- Configure the clients to obtain IP addresses through DHCP.

II. Configuring Authorized ARP

The following tables describe the authorized ARP configuration tasks, which must be performed on the DHCP server.

1) Enable authorized ARP in system view

Table 2-11 Enable authorized ARP for DHCP interface address pools

Operation	Command	Description
Enter system view	**system-view**	—
Configure interfaces to operate in DHCP server mode and specify to allocate addresses from interface address pools	**dhcp select interface** { **interface** *interface-type interface-number* [**to** *interface-type interface-number*] | **all** }	Required
Enable authorized ARP for DHCP interface address pools	**dhcp server synchronize arp** { **interface** *interface-type interface-number* [**to** *interface-type interface-number* | **all** }	Required. By default, authorized ARP is not enabled.

Operation	Command	Description
Enter interface view	**interface** *interface-type interface-number*	Before creating an interface address pool, you must configure the IP addresses of the interfaces involved in the previous commands.
Configure the IP address of the interface	**ip address** *ip-address net-mask*	
Enable ARP security	**arp security**	Optional. By default, ARP security is disabled.
Configure the aging time of the authorized ARP entries	**arp security time-out** *seconds*	Optional. By default, the aging time of an authorized ARP entry is 90 seconds.

Note:

- This mode applies to scenarios where addresses from the interface address pools are assigned to clients.
- In this configuration mode, you can configure an interface range. Therefore, you can configure DHCP to support authorized ARP on multiple interfaces at the same time.

2) Enable authorized ARP in interface view

Table 2-12 Enable authorized ARP for DHCP interface address pools

Operation	Command	Description
Enter system view	**system-view**	—
Enter interface view	**interface** *interface-type interface-number*	—
Configure the IP address of the interface	**ip address** *ip-address net-mask*	—
Configure the interface to operate in DHCP server mode and specify to allocate addresses from interface address pools	**dhcp select interface**	Required
Enable authorized ARP for DHCP interface address pools	**dhcp server synchronize arp**	Required. By default, authorized ARP is not enabled.

Operation	Command	Description
Enable ARP security	**arp security**	Optional. By default, ARP security is disabled.
Configure the aging time of the authorized ARP entries	**arp security time-out** *seconds*	Optional. By default, the aging time of an authorized ARP entry is 90 seconds.

Note:

- This mode applies to scenarios where addresses from the interface address pools are assigned to clients.
- In this configuration mode, you may configure DHCP to support authorized ARP in interface view. Therefore, this mode is suitable when you want to configure a single interface to support authorized ARP.

3) Enable authorized ARP in DHCP global address pool view

Table 2-13 Enable authorized ARP for DHCP global address pools

Operation	Command	Description
Enter system view	**system-view**	—
Configure the interface to operate in DHCP server mode and specify to allocate addresses from global address pools	**dhcp select global** [**subaddress**] **|** **interface** *interface-type interface-number* [**to** *interface-type interface-number*] **|** **all** }	Required
Enter DHCP address pool view	**dhcp server ip-pool** *pool-name*	Required
Enable authorized ARP for global DHCP address pools	**synchronize arp**	Required. By default, authorized ARP is not enabled.
Exit to system view	**quit**	—
Enter interface view	**interface** *interface-type interface-number*	—
Enable ARP security	**arp security**	Optional. By default, ARP security is disabled.

Operation	Command	Description
Configure the aging time of the authorized ARP entries	**arp security time-out** *seconds*	Optional. By default, the aging time of an authorized ARP entry is 90 seconds.

🕮 **Note:**

This mode applies to scenarios where addresses from the global address pools are assigned to clients.

⚠ **Caution:**

- Only when you configure the ARP security function, can ARP ping start to work. If ARP ping is not working, an authorized ARP entry will never be removed, even if it has timed out.
- If an authorized ARP entry is in the ARP table already when you configure the **arp security** command, the aging time of the entry will be refreshed.
- If you configure the **arp security time-out** command directly without configuring the **arp security** command, the aging time configuration is accepted but takes no effect.

2.4.7 Authorized ARP Configuration Example

I. Network requirements

- DHCP clients obtain IP addresses through a DHCP server.
- The router with the DHCP server function enabled supports authorized ARP, and the aging time of the authorized ARP entries is 120 seconds.
- Ethernet interface Ethernet1/0/0 on the DHCP server, that is, the interface connected to the clients, has an IP address of 10.1.1.1/24. Ethernet interface Ethernet1/0/1, that is, the interface for accessing the Internet has an IP address of 10.1.2.1/24. The DHCP server is configured with global address pool 10.1.1.0/24.
- The DHCP server acts as the proxy gateway server for clients to access the Internet at the same time.

II. Network diagram

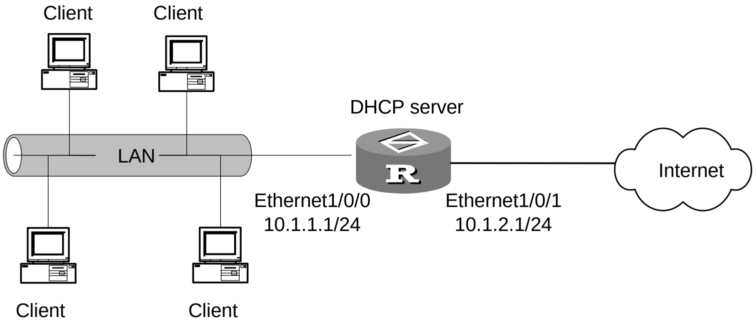


Figure 2-4 Network diagram for authorized ARP

III. Configuration procedure

# Enable DHCP.

```
[Quidway] dhcp enable
```

# Configure interfaces to operate in DHCP server mode, and assign IP addresses from a global address pool.

```
[Quidway] dhcp select global interface ethernet 1/0/0 to ethernet 1/0/1
```

# Configure the network parameters and address pool on the DHCP server.

```
<Quidway> system-view
[Quidway] interface ethernet 1/0/0
[Quidway-Ethernet1/0/0] ip address 10.1.1.1 255.255.255.0
[Quidway-Ethernet1/0/0] quit
[Quidway] interface ethernet 1/0/1
[Quidway-Ethernet1/0/1] ip address 10.1.2.1 255.255.255.0
[Quidway-Ethernet1/0/1] quit
[Quidway] dhcp server ip-pool 0
[Quidway-dhcp-pool-0] network 10.1.1.0 mask 255.255.255.0
```

# Enable authorized ARP for the DHCP global address pool.

```
[Quidway-dhcp-pool-0] synchronize arp
[Quidway-dhcp-pool-0] quit
```

# Enable ARP security, and configure an aging time of 120 seconds for authorized ARP entries.

```
[Quidway] interface ethernet 1/0/0
[Quidway-Ethernet1/0/0] arp security
[Quidway-Ethernet1/0/0] arp security time-out 120
[Quidway-Ethernet1/0/0] quit
```

2.5 ARP Entry Fixup Configuration

2.5.1 Introduction to ARP Entry Fixup

An attacker may send an ARP packet using a fake MAC address and the IP address of a device in a LAN to poison the cache of the corresponding gateway.

The dynamic ARP entry fixup feature can change the dynamic ARP entries of a gateway into fixed ARP entries to prevent such ARP attacks. In this way, the router will not change the ARP entries even if it is attacked.

2.5.2 Enabling ARP Entry Fixup

I. Fixing all the ARP entries on a device

Perform the following configuration in system view.

Table 2-14 Enable dynamic ARP entry fixup

Operation	Command	Description
Enable dynamic ARP entry fixup	**arp fixup**	Required

II. Fixing all the ARP entries on an interface

Perform the following configuration in interface view.

Table 2-15 Enable dynamic ARP entry fixup on an interface

Operation	Command	Description
Enable dynamic ARP entry fixup on an interface	**arp fixup**	Required

III. Adding a fixed ARP entry

Perform the following configuration in system view.

Operation	Command	Description
Add a fixed ARP entry	**arp fixed** *ip-address mac-address* [*vpn-instance-name*]	Required

2.5.3 Displaying and Maintaining ARP Entry Fixup Configuration

After the above configuration, execute the **display** command in any view to display the ARP entry fixup configuration for verification.

Execute the **reset** command in user view to clear fixed ARP entries.

Table 2-16 Display and maintain ARP entry fixup configuration

Operation	Command
Display fixed ARP entries	**display arp fixed**
Clear fixed ARP entries	**reset arp fixed**

Chapter 3 DNS Configuration

3.1 DNS Overview

TCP/IP not only provides IP address to specify devices, but also specially designs a kind of host naming mechanism called DNS (Domain Name System) in the form of character string. Adopting a hierarchical naming system, the DNS designates a meaningful name for the device in the Internet and associate the domain name with IP address with the help of the domain name resolution server. In this way, the user can use domain names that are easy to memorize and meaningful, and never needs to keep obscure IP addresses in mind.

There are two kinds of domain name resolutions, namely static domain name resolution and dynamic domain name resolution, which supplement each other in real application. On resolving a domain name, use the static resolution first. If it fails, use the dynamic resolution method. Some common domain names can be put into the static domain name resolution table to raise the domain name resolution efficiency greatly.

- Static resolution: To create the corresponding relationship between domain name and the IP address manually. When the client needs the IP address related to the domain name, it will search the specific domain name in the static domain name resolution table to obtain the corresponding IP address.
- Dynamic resolution: To receive the domain name resolution request lodged by the client with special domain name resolution server. The server first performs resolution within the local database. If it judges that the domain name does not belong to the local domain, it will forward the request to the upper level domain name resolution server until the resolution is finished. The resolution results, being either IP address or non-existed domain name, will be returned to the client.

3.2 Static Domain Name Resolution Configuration

3.2.1 Configuring Static Domain Name Resolution

The router performs static DNS by consulting a static DNS table containing domain name to IP address associations in common use. This table is similar to the hosts file on a Windows 9X OS. It allows users to use user-friendly hostnames rather than IP addresses to reach hosts.

Perform the following configuration in system view.

Table 3-1 Add or delete mapping entry in static domain name resolution table

Operation	Command
Add the mapping between domain name and IP address	**ip host** *hostname ip-address* [*port*]
Delete the mapping between domain name and IP address	**undo ip host** *hostname* [*ip-address*]

A hostname can be mapped to only one IP address and port number. The IP address assigned to a hostname will overwrite the previous one, if there is any.

📖 **Note:**

The port number specified in the **ip host** command is only used in reverse TELNET function.

3.2.2 Displaying and debugging domain name resolution table

After the above configuration, execute the **display** command in all views to display the running of domain name resolution table, and to verify the effect of the configuration.

Table 3-2 Display and debug domain name resolution table

Operation	Command
Display static domain name resolution table	**display ip host**

3.3 DNS Client Configuration

3.3.1 Introduction to the Architecture of DNS

IP addresses, 202.112.131.109 for example, are 32 bits long and as such are difficult for human beings to memorize. To make it easier to memorize addresses, most organizations replace IP addresses with domain names, that is, abbreviations or meaningful names, www.sina.com.cn for example. To map a domain name to an IP address, you need a resolver and a domain name system (DNS) server.

DNS is a distributed database that applies to TCP/IP application programs. It functions to resolve between hostnames and IP addresses and provide email routing information. In applications, access to the DNS server is provided by an address resolver. The DNS client can accomplish the function of a resolver by translating between IP addresses and domain names of hosts.

This is how DNS operates:

1) First, a user program sends a request to the DNS client.
2) Upon receipt of this request, the DNS client looks up the local database; if no match is found, it sends a query to the domain name server.
3) After receiving the response sent back by the domain name server, the DNS client resolves the response packet and based on the packet contents decides its operation.

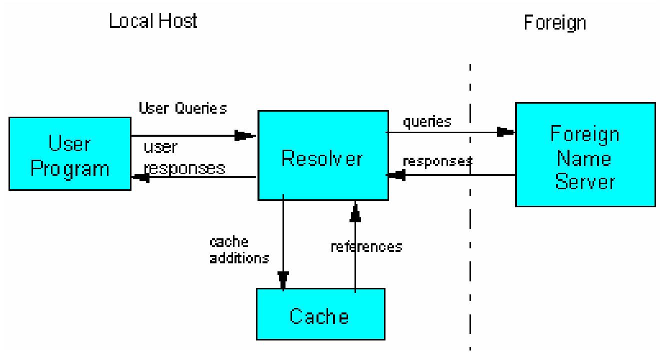


Figure 3-1 DNS system components

Figure 3-1 illustrates the process of DNS resolving:

1) The user program queries the resolver for a domain name or IP address.
2) Upon receipt of the query, the resolver first looks up the local cache. If the requested map entry is found, it directly replies. If not, it assembles a query packet appropriate to the query type, that is, whether IP address or domain name is needed. This packet can take TCP or UDP format, but in this program UDP is adopted.
3) Then, based on its DNS configuration, the resolver sends the query packet to port 53 on the default DNS server (the foreign name server in this scenario).
4) After receiving the response, the resolver resolves the response packet and replies to the user.

In this scenario, resolver and its cache are called DNS client and as a whole function to accept and respond to the DNS queries of user programs. Normally, the user program and resolver are on the same host whereas the foreign name server can be located on that same host or more likely on a different one.

3.3.2 Configuring the DNS Client

Following are the DNS client configuration tasks:

- Enable DNS resolving
- Configure IP address of the DNS server

- Configure the DNS domain name searching list

Where, you must enable DNS resolving and provide IP address of the DNS server. You need only to enable DNS resolving, however, if the interfaces on the device use IP addresses assigned by a DHCP client and the address of the DNS server and the domain name are included in the information that the DHCP server issues to the device.

I. Enabling DNS Resolving

To use the DNS client function, enable DNS resolving on the device first.

Perform the following configuration in system view.

Table 3-3 Enable/disable DNS resolving

Operation	Command
Enable DNS resolving.	**dns resolve**
Disable DNS resolving.	**undo dns resolve**

By default, DNS resolving is disabled.

II. Configuring IP Address of the DNS Server

To resolve domain names, the DNS client must know the domain server address where it can send queries.

Perform the following configuration in system view.

Table 3-4 Configure IP address of the DNS server

Operation	Command
Configure IP address of the DNS server.	**dns server** *ip-address*
Delete IP address of the DNS server.	**undo dns server** [*ip-address*]

By default, no IP address of DNS server is configured.

III. Configuring the DNS Domain Name Searching List

Some of the websites that you access may have the same domain name, such as sina.com.cn, huawei.com.cn, and sohu.com.cn.

To facilitate website searching of users, you can set a domain name to com.cn for example. Thus, to search for the IP address mapped with "sina.com.cn", a user only needs to enter the command **ping sina**. If no response is received, the DNS client sends a request to query the IP address mapped with “sina”.

You can configure a DNS domain name searching list by using the following command repeatedly.

Perform the following configuration in system view.

Table 3-5 Configure a DNS domain name

Operation	Command
Configure a DNS domain name.	**dns domain** *domain-name*
Delete one or all DNS domain names.	**undo dns domain** [*domain-name*]

Note:

RFC1034, however, uses a different searching approach: when you input the **ping sina** command, the DNS client first queries the IP address mapped to "sina". And if no response is received, it then queries the IP address mapped to "sina.com.cn".

3.3.3 Displaying and Debugging DNS Client Information

I. Displaying the DNS client information

Perform the following operation in any view.

Table 3-6 Display the DNS client information

Operation	Command
View whether DNS resolving is enabled	**display current-configuration**
Display the configurations of the DNS server	**display dns server** [**dynamic**]
Display the configurations of the DNS domain name searching list	**display dns domain** [**dynamic**]
Display contents of the dynamic domain name buffer	**display dns dynamic-host**
Display the domain name or IP address resolved from the specified IP address or domain name	**nslookup type** { **ptr** *ip-address* | **a** *domain-name* }

Note:

Execute the **display dns server dynamic** command to view DNS server addresses that are dynamically obtained through DHCP or by other means.

II. Clearing the domain name cache

The DNS client retains the result of each successful domain name resolution in its cache. If it receives the same resolving request later, it first looks up the cache for a match. And if no match is found, it sends a domain name resolving request to the DNS server.

You can clear the current cache using the following command.

Perform the following operation in user view.

Table 3-7 Clear the dynamic domain name cache

Operation	Command
Clear the dynamic domain name cache.	**reset dns dynamic-host**

III. Debugging the DNS client

Perform the following operation in user view.

Table 3-8 Debug the DNS client

Operation	Command
Enable DNS client debugging.	**debugging dns**
Disable DNS client debugging.	**undo debugging dns**

By default, DNS client debugging is disabled.

3.3.4 Typical DNS Configuration Example

I. Networking requirements

Enable DNS resolving on the router with the IP address 10.110.10.1. IP address of the DNS server is 10.110.66.66.

II. Network diagram

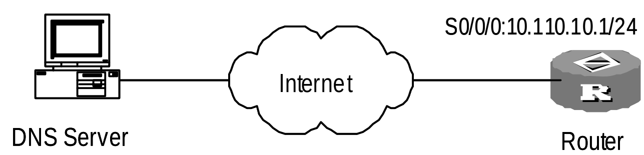


Figure 3-2 Network diagram

III. Configuration procedure

# Enable DNS resolving.

```
[Quidway] dns resolve
```

# Configure IP address of the DNS server.

```
[Quidway] dns server 10.110.66.66
```

# Configure IP address of the interface Serial0/0/0.

```
[Quidway] interface serial 0/0/0
[Quidway-Serial0/0/0] ip address 10.110.10.1 255.255.255.0
[Quidway-Serial0/0/0] quit
```

# Configure a static route to the DNS server.

```
[Quidway] ip route-static 10.110.66.66 serial0/0/0
```

3.3.5 Troubleshooting

Symptom: Domain name resolving failed.

Solution:

1) Check the software, making sure that:

- IP address of the domain name server is correctly configured.
- The device and the domain name server have routes between them.
- DNS resolving is enabled.

2) Check the hardware, making sure the network connection cable is in good condition and securely connected.

3.4 DNS Proxy Configuration

3.4.1 Introduction to DNS Proxy

DNS proxy is enabled on the router functioning as the gateway proxy for a LAN. It allows clients on the LAN to contact an external DNS server for service when accessing the Internet in case no internal DNS server is present.

3.4.2 Operational Mechanism of DNS Proxy

The following describes how DNS proxy operates:

1) The DNS client sends a DNS request to the DNS proxy, using the IP address of the DNS proxy as the destination address.
2) When the DNS proxy receives the request, it replaces the destination address with the IP address of a DNS server, and then forwards the request to the DNS server. When multiple DNS server addresses are available, the DNS proxy sends the request to the one configured first. If no response is received, the DNS client resends the request and the DNS proxy forwards this resent request to the second DNS server. This process continues until a response is received from a DNS server.
3) The DNS server sends a response back to the DNS proxy.

4) The DNS proxy replaces the source IP address in the received response with its own IP address and forwards the response to the DNS client.

Now, the DNS client can use the IP address carried in the received response to access the Internet.

3.4.3 Configuring DNS Proxy

I. Configuration prerequisites

Before configuring DNS proxy, make sure that

- IP addresses of DNS servers are available on the DNS proxy.
- The gateway enabled with DNS proxy is specified as the DNS server on the DNS client.
- The DNS client and the DNS server are reachable to the DNS proxy.

II. Configuring DNS proxy

Configure DNS proxy on the router functioning as the gateway.

Table 3-9 Configure DNS proxy

Operation	Command	Description
Enter system view	**system-view**	—
Enable DNS proxy	**dns-proxy enable**	Required

3.4.4 DNS Proxy Configuration Example

I. Network requirements

PCs on network segment 10.1.1.0/24 where no DNS server is present may obtain DNS service from an external DNS server, for example, the one with IP address 10.72.66.36/24. To this end, the gateway router must support DNS proxy.

II. Network diagram

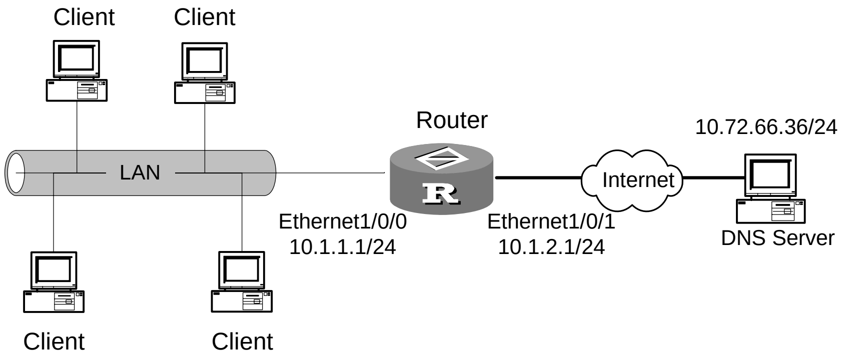


Figure 3-3 Network diagram for DNS proxy configuration

III. Configuration example

1) Configure the router

# Assign an IP address to interface Ethernet 1/0/0.

```
[Quidway] interface ethernet 1/0/0
[Quidway-Ethernet 1/0/0] ip address 10.1.1.1 255.255.255.0
```

# Configure NAT, allowing the client to access the Internet by using DNS proxy.

```
[Quidway] acl number 2000
[Quidway-acl-basic-2000] rule 0 permit source 10.1.1.0 0.0.0.255
[Quidway-acl-basic-2000] quit
[Quidway] interface ethernet 1/0/1
[Quidway-Ethernet1/0/1] ip address 10.1.2.1 255.255.255.0
[Quidway-Ethernet1/0/1] nat outbound 2000
[Quidway-Ethernet1/0/1] quit
```

# Enable DNS proxy.

```
[Quidway] dns-proxy enable
```

# Configure the IP address of the DNS server.

```
[Quidway] dns server 10.72.66.36
```

# Configure routing, ensuring that the DNS client and the router are reachable to each other.

```
Omitted
```

2) Configure the PC

Set gateway and DNS server addresses to 10.1.1.1.

Chapter 4 DDNS Configuration

4.1 Introduction to DDNS

Dynamic domain name service (DDNS) is to set up bindings between static domain names and dynamic IP addresses of the hosts using the domain names.

As shown in Figure 4-1, Server A is an HTTP or FTP server connected to Router A to gain access to the Internet. When Server A obtains IP address through DHCP or connects to the Internet through PPPoE, PPTP or L2TP, its IP address is dynamic, meaning its IP address may change each time the connection is initialized.

The DNS server providing service to Server A maintains a static domain name-to-IP address binding for Server A. As this binding does not alter as the IP address changes, Internet users cannot reach Server A by using its domain name once the server's IP address changes.

To help the DNS server maintain a binding between static domain name and dynamic IP address for Server A, you may use DDNS. This allows Internet users to reach Server A by its domain name despite the change of its IP address.

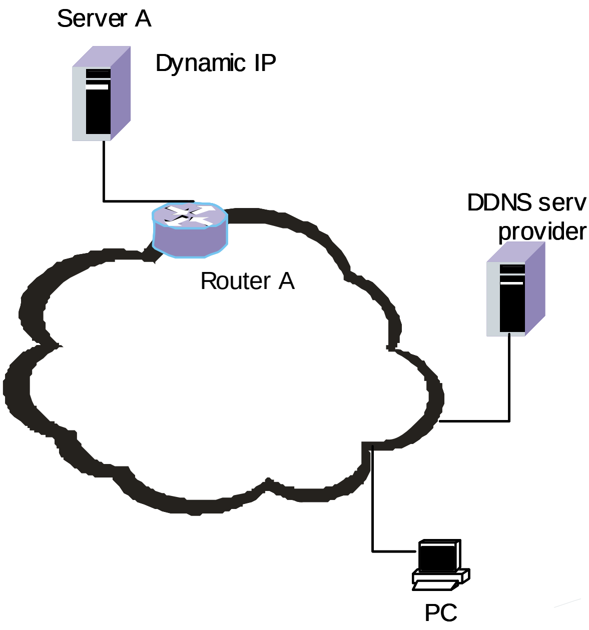


Figure 4-1 Network diagram for DDNS application

DDNS is divided into user side and service provider side.

- User side of DDNS

Usually, the user side of DDNS is a server providing HTTP, FTP, or other services. After the IP address of the server changes, the server needs to request the DDNS service provider to notify the DNS server of this. This is usually done by using a special client program provided by the DDNS service provider or through a specified HTTP page.

The domain name-to-IP address mapping update process does not follow a particular protocol; it varies by DDNS service provider.

- Service provider side of DDNS

After receiving an IP address update request from the user side, the DDNS service provider notifies the DNS server to update the involved domain name-to-IP address mapping.

At present, www.3322.org is the only DDNS service provider supported by Quidway Series Routers.

Quidway Series Routers implement the user side of DDNS. When DDNS users' IP addresses change, Quidway Routers can request www.3322.org to notify DNS servers to update domain name-to-IP address mappings.

4.2 Configuring DDNS

4.2.1 Configuration Prerequisites

Before configuring DDNS on your router, make sure that:

- The router can obtain DNS service.
- On the DNS server, a domain name-to-IP address mapping entry has created for the domain name of the DDNS service provider, which can be www.3322.org only at present.

This is to ensure that your router can access the DDNS service provider.

4.2.2 Configuring DDNS

Table 4-1 Configure DDNS

Operation	Command	Description
Enter system view	**system-view**	—
Set 3322.org as the DDNS service provider and enter its view	**ddns-server 3322.org**	—
Set parameters for accessing the DDNS service provider	Refer to section 4.2.3 "Configuring Parameters for Accessing the DDNS Service Provider"	Required

Operation	Command	Description
Configure a domain name whose domain name-to-IP address mapping on DNS needs update by using the service of the DDNS service provider	**ddns domainname** *name*	Required
Request the DDNS service provider to notify the DNS server that the bound IP address of the domain name specified by the **ddns domainname** command has changed	**ddns refresh**	Required

4.2.3 Configuring Parameters for Accessing the DDNS Service Provider

Table 4-2 Configure parameters for accessing the DDNS service provider

Operation	Command	Description
Enter system view	**system-view**	—
Set 3322.org as the DDNS service provider and enter its view	**ddns-server 3322.org**	—
Set the user name used for accessing the DDNS service provider	**ddns username** *name*	Required
Set the password used for accessing the DDNS service provider	**ddns password** *password*	Required
Set the interface used for accessing the DDNS service provider	**ddns source-interface** *interface-type interface-number*	Required

4.2.4 DDNS Configuration Example

I. Network requirements

As shown in the following figure, Server A obtains IP address dynamically through DHCP service of Router A. It provides the WWW service at www.abc123.com to Internet users.

II. Network diagram

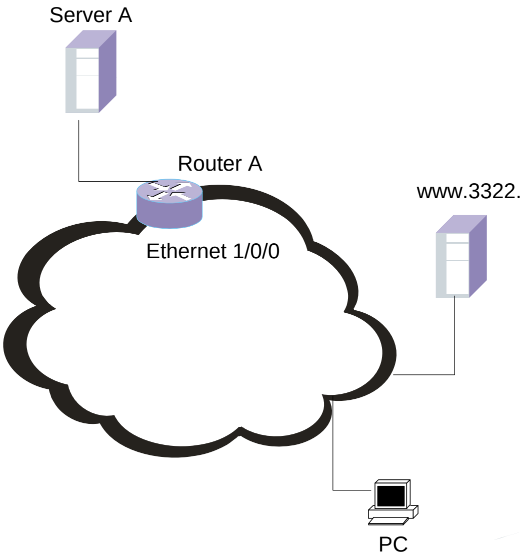


Figure 4-2 Network diagram for DDNS application

III. Configuration procedure

# Enter system view.

```
<Quidway> system-view
```

# Set 3322.org as the DDNS service provider and enter its view.

```
[Quidway] ddns-server 3322.org
```

# Set the user name used for accessing the DDNS service provider to user.

```
[Quidway-ddns-3322.org] ddns username user
```

# Set the password used for accessing the DDNS service provider to pass.

```
[Quidway-ddns-3322.org] ddns password pass
```

# Set the interface used for visiting the DDNS service provider to Ethernet 1/0/0.

```
[Quidway-ddns-3322.org] ddns source-interface ethernet 1/0/0
```

# Configure domain name www.abc123.com, allowing its domain name-to-IP address mapping on DNS to be updated by using the service of the DDNS service provider.

```
[Quidway-ddns-3322.org] ddns domainname www.abc123.com
```

# Request the DDNS service provider to notify the DNS server that the bound IP address of domain name www.abc123.com has changed.

```
[Quidway-ddns-3322.org] ddns refresh
```

Chapter 5 URPF Configuration

5.1 URPF Overview

5.1.1 Introduction to URPF

Unicast Reverse Path Forwarding (URPF) serves as a safeguard against source address based network attacks.

In source address spoofing attacks, attackers create a series of packets with forged source addresses. For applications using IP address based authentication method, this type of attack allows unauthorized users to access the system in the name of other users. Even the response packets cannot reach the attackers; it is disruptive to the attacked target.

There are generally two types of URPF check: strict check and loose check. It also supports ACL and default route check.

5.1.2 URPF Check Procedure

The URPF check procedure is as follows:

1) The router checks the source address of a packet for validity. If the source address is an invalid host address, the router will directly discard it.
2) If the source address can be found in the FIB of the router and the outgoing interface in the forwarding entry is the same as the incoming interface of the packet, the router will do:

- If the forwarding entry is a default route, the router will forward the packet only if the **allow-default-route** keyword is specified. If the **allow-default-route** keyword is not specified, the router will go to step 5 for an ACL check.
- If the forwarding entry is not a default route, the router will pass the URPF check.

3) If the source address can be found in the FIB but the outgoing interface in the forwarding entry is different from the incoming interface of the packet, the router will do:

- For **strict** check, the router goes to step 5 for an ACL check directly.
- For **loose** check, the processing is the same as in step 2).

4) If the source address cannot be found not in the FIB, or the found forwarding entry is Blackhole or Reject, the router goes to Step 5 for ACL check.
5) The router performs ACL check in the following way:

- If an ACL is configured, the router filters the packet according to the ACL rule.

If the ACL rule permits the packet to pass, the packet can pass.

If the ACL rule rejects the packet to pass, the router discards it.

- If no ACL is configured, the router will directly discard the packet.

📖 **Note:**

URPF does not support fast forwarding. If a fast forwarding table exists, the result of a URPF check does not take effect. Thus, even a packet fails to pass URPF check, it is forwarded all the like.

5.2 URPF Configuration

Perform the following configuration in interface view.

Table 5-1 Enable/disable URPF check

Operation	Command
Enable URPF check	**ip urpf** { **strict** | **loose** } [**allow-default-route**] [**acl** *acl-number*]
Disable URPF check	**undo ip urpf**

By default, URPF check is disabled.

5.3 URPF Display and Debugging

Perform the following configuration in user view.

Table 5-2 Enable URPF discarded packets debugging

Operation	Command
Enable URPF discarded packets debugging	**debugging ip urpf discards** [**interface** *interface-type interface-number*]
Disable URPF discarded packets debugging	**undo debugging ip urpf discards** [**interface** *interface-type interface-number*]

Chapter 6 IP Accounting Configuration

6.1 Introduction to IP Accounting

IP Accounting counts inbound and outbound IP packets on the router. These IP packets include those sent and forwarded normally as well as those denied by the firewall.

The statistics of the IP Accounting provide information about source and destination IP addresses, protocol number, packet sum, and byte sum. The statistics are sorted into different tables for display depending on whether IP packets pass the firewall and whether they match IP accounting rules.

Each IP accounting rule consists of an IP address and its mask. The rule list records network segment addresses, which are the results of ANDing IP addresses with their masks. An IP packet is sorted as follows:

- If the source or destination IP address of the IP packet matches a network segment address in the rule list, the packet is recorded in an interior hash table as a valid packet (a packet not filtered out by the firewall) matching the rule. Otherwise, the packet is recorded in an exterior hash table as a valid packet not matching the rule.
- If the packet is filtered out by the firewall configured on the interface when it reaches a router, it is recorded in the firewall-denied hash table as an invalid packet.

6.2 IP Accounting Configuration

To configure IP accounting, first enable it, and then specify one or more types of packets to be counted on an interface. After that, the router can start counting IP packets.

6.2.1 Preparations for IP Accounting Configurations

You have assigned an IP address and mask to the interface, on which packets are to be counted. In addition, a firewall is configured on the interface.

6.2.2 IP Accounting Configuration Tasks

The following sections describe IP accounting configuration tasks:

Table 6-1 IP accounting configuration tasks

Operation	Command	Description
Enter system view	**system-view**	—
Enable IP accounting	**ip count enable**	Required
Set an aging time	**ip count timeout** *minutes*	Optional (720 minutes by default)
Set the maximum length of the interior hash table	**ip count interior-threshold** *number*	Optional (512 by default)
Set the maximum length of the exterior hash table	**ip count exterior-threshold** *number*	Optional (0 by default)
Add IP accounting rules	**ip count rule** *ip-address net-mask*	Required. If no rule is set, no packet matches rules.
Enter interface view	**interface** *interface-type interface-number*	Required
Specify the type of packets to be counted on the interface	**ip count** [**firewall-denied**] { **inbound-packets | outbound-packets** }	Required.
Display the IP accounting rule list	**display ip count rule**	You may execute the **display** command in any view.
Display IP accounting information	**display ip count** { **inbound-packets | outbound-packets** } { **interior | exterior | firewall-denied** }	Execute the **display** command in any view.

Caution:

- If the IP accounting function is configured on interfaces but no IP accounting rule exists, you must set the length of the exterior hash table to be greater than zero by using the **ip count exterior-threshold** *number* command. If the *number* argument is set to 50, the IP Accounting may count up to 50 IP packets with different combinations of source and destination.
- The IP packets with the same source and destination are counted in the same entry. For legitimate IP packets, they are further classified and then saved by protocol number. For illegitimate packets, no further classification is performed; their protocol information is omitted, and only packet sum and byte sum are recorded.
- You may configure up to 32 IP accounting rules.

6.2.3 IP Accounting Configuration Example

I. Network requirements

As shown in Figure 6-1, the router is connected to two hosts through Ethernet ports. Count the IP packets from PC1 to PC2, with the aging time for table entries as 24 hours.

II. Network diagram

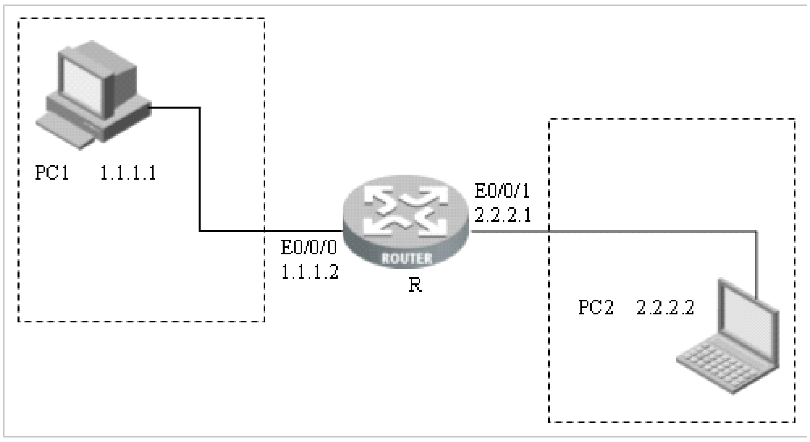


Figure 6-1 Network diagram for IP accounting configuration

III. Configuration procedure

# Enable IP accounting.

```
[Quidway] ip count enable
```

# Enter system view, and configure an IP accounting rule.

```
[Quidway] ip count rule 1.1.1.1 24
```

# Configure the aging time as 1,440 minutes (24 hours).

```
[Quidway] ip count timeout 1440
```

# Set the maximum length of the interior hash table to 100.

```
[Quidway] ip count interior-threshold 100
```

# Set the maximum length of the exterior hash table to 20.

```
[Quidway] ip count exterior-threshold 20
```

# Enter the interface view of Ethernet 0/0/0; assign the interface an IP address and configure the IP Accounting to count both inbound and outbound IP packets on it.

```
[Quidway] interface ethernet 0/0/0
[Quidway-Ethernet0/0/0] ip address 1.1.1.2 24
[Quidway-Ethernet0/0/0] ip count inbound-packets
[Quidway-Ethernet0/0/0] ip count outbound-packets
[Quidway-Ethernet0/0/0] quit
```

# Enter the view of Ethernet 0/0/1 and assign it an IP address.

```
[Quidway] interface ethernet 0/0/1
[Quidway-Ethernet0/0/1] ip address 2.2.2.1 24
```

# Configure static routes on PC1 and PC2 for them to reaching each other. Ping PC2 on PC1.

# Display IP accounting information.

```
[Quidway] display ip count inbound-packets interior
 Inbound packets information in interior list:
  SrcIP          DstIP          Protocol  Pkts        Bytes
  1.1.1.1        2.2.2.2        ICMP      4           240
[Quidway] display ip count outbound-packets interior
 Outbound packets information in interior list:
  SrcIP          DstIP          Protocol  Pkts        Bytes
  2.2.2.2        1.1.1.1        ICMP      4           240
```

Note:

The two hosts can be replaced by other types of network devices such as routers.

6.3 Displaying and Maintaining IP Accounting Configuration

Execute the **display** commands in any view to display IP accounting configuration.

Table 6-2 Display and maintain IP accounting configuration

Operation	Command	Description
Display configuration information	**display this**	You can execute the command in system or interface view to view the configured commands.
Display the IP accounting rule list	**display ip count rule**	You can execute the command in any view.
Display IP accounting information	**display ip count** { **inbound-packets** | **outbound-packets** } { **interior** | **exterior** | **firewall-denied** }	You can execute the command in any view.

6.4 Tips for Configuration

- When configuring an interior or exterior hash table, you need to clear the table first and then make configuration if the number of the entries in the table is greater than the configured or default value.
- The interior or exterior hash table contains information about the IP packets counted after IP accounting rules are configured. After you configure an IP accounting rule, some original rule-incompliant packets may match the rule. After that, information about these packets is to be saved in the interior hash table. The exterior table, however, possibly contains information about the packets counted with the same address before the rule is configured. The entry for these packets in the exterior hash table will be removed when the aging time expires.

Chapter 7 UDP Helper Configuration

7.1 Introduction to UDP Helper

UDP Helper functions to relay UDP broadcast packets to the specified server after converting them to unicast packets.

With UDP Helper enabled, the router decides whether to forward a received UDP broadcast packet based on its port number. If forwarding is required, the router modifies the destination IP address in the IP header and then relays the packet to the specified destination server. If not, the router passes the packet to the upper layer module. When relaying a BOOTP/DHCP response message, the router broadcasts it if the client requests that a broadcast response is desired; if otherwise, the router unicasts it.

7.2 UDP Helper Configuration

UDP Helper configuration tasks are described in the following sections:

- Enabling/Disabling UDP Helper
- Specifying by UDP Port Number which UDP Broadcast
- Configuring Destination Server

7.2.1 Enabling/Disabling UDP Helper

You can enable UDP helper to have the router forward the received UDP broadcast packets. As soon as this function is enabled, the router forwards the broadcast packets with the UDP port number 69, 53, 37, 137, 138, or 49 by default. In addition to these port numbers, you can configure the router to forward the broadcast packets with the specified UDP port number. Disabling this function disables the router to forward the broadcast packets with one of these UDP port numbers (specified or default).

Perform the following configuration in system view.

Table 7-1 Enable/disable UDP Helper

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

By default, UDP Helper is disabled.

7.2.2 Specifying by UDP Port Number which UDP Broadcasts are forwarded

With UDP Helper enabled, the system by default unicasts the broadcast packets with the UDP ports listed in the following table. You can configure up to 256 UDP ports with UDP Helper.

Table 7-2 Default UDP ports

Protocol	UDP port number
Trivial file transfer protocol (TFTP)	69
Domain name system (DNS)	53
Time service	37
NetBIOS name server (NetBIOS-NS)	137
NetBIOS datagram server (NetBIOS-DS)	138
Terminal access controller access control system (TACACS)	49

Perform the following configuration in system view.

Table 7-3 Configure/disable the system to forward the UDP broadcasts with the specified UDP port number

Operation	Command
Configure the system to forward the UDP broadcasts with the specified UDP port number	**udp-helper port** { *port* | **dns** | **netbios-ds** | **netbios-ns** | **tacacs** | **tftp** | **time** }
Disable the system to forward the UDP broadcasts with the specified UDP port number	**undo udp-helper port** { *port* | **dns** | **netbios-ds** | **netbios-ns** | **tacacs** | **tftp** | **time** }

Note that:

- Before you can specify by UDP port number which UDP broadcasts are forwarded, you must enable UDP Helper.
- The **dns**, **netbios-ds**, **netbios-ns**, **tacacs**, **tftp**, and **time** keywords represents the six default ports. When specifying a default port, DNS for example, you can specify its port number 53 directly or specifying the keyword **dns**.
- When displaying the information about UDP helper, the **display current-configuration** command displays the default UDP port numbers only when they are disabled to use UDP Helper.

7.2.3 Configuring Destination Servers

After enabling UDP helper in system view, you can configure one or multiple (up to 20) servers on an Ethernet interface to have the UDP broadcasts received on the interface forwarded to the server or servers.

Perform the following configuration in Ethernet interface view.

Table 7-4 Configure/delete the server to which UDP broadcasts are forwarded

Operation	Command
Configure the destination server to which the UDP broadcasts received on the interface are forwarded	**udp-helper server** *ip-address*
Delete the destination server to which the UDP broadcasts received on the interface are forwarded	**undo udp-helper server** [*ip-address*]

By default, no destination server is available.

7.3 Displaying and Debugging the UDP Helper Configuration

After completing the above configuration tasks, execute the **display** command in any view to view the destination servers available with UDP Helper and to verify the effect of the configurations.

Execute the **debugging** command in user view to debug UDP helper.

Table 7-5 Display and debug UDP Helper

Operation	Command
Display the destination servers associated with the specified or all Ethernet interfaces	**display udp-helper server** [**interface** *number*]
Enable UDP Helper debugging	**debugging udp-helper** { **event** | **packet** [**receive** | **send**] }
Disable UDP Helper debugging	**undo debugging udp-helper** { **event** | **packet** [**receive** | **send**] }

Chapter 8 BOOTP Client Configuration

8.1 Introduction to BOOTP Client

The bootstrap protocol (BOOTP) adopts the client/server model where the BOOTP client requests the server for an IP address.

The following is how the BOOTP client obtains an IP address from the BOOTP server:

- The BOOTP client sends a BOOTP request.
- Upon receipt of the request, the BOOTP Server sends back a reply with the allocated IP address.
- The BOOTP client obtains the IP address.

BOOTP messages are encapsulated in UDP. To ensure transmission reliability, the timeout retransmission mechanism is adopted. When the BOOTP client sends a request, a retransmission timer starts. If no reply is received when the timer times out, the client retransmits the request. The retransmission occurs every five seconds and up to three transmission attempts are allowed.

8.2 BOOTP Client Configuration

BOOTP client configuration includes only one task, which is described in the following subsection.

8.2.1 Configuring an Ethernet Interface to Obtain IP Address Using BOOTP

Perform the following configuration in Ethernet interface view.

Table 8-1 Configure the Ethernet interface to obtain IP address using BOOTP

Operation	Command
Configure the Ethernet interface to obtain IP address using BOOTP	**ip address bootp-alloc**
Disable the Ethernet interface to obtain IP address using BOOTP	**undo ip address bootp-alloc**

By default, the Ethernet interface does not use BOOTP to obtain IP address.

8.3 Displaying and Debugging BOOTP Client Configuration

After completing the above configuration, execute the **display** command in any view to display and verify your BOOTP configuration.

Table 8-2 Display and debug the BOOTP client configuration

Operation	Command
Display BOOTP client information	**display bootp client** [**interface** *interface-type interface-number*]

Chapter 9 DHCP Configuration

9.1 DHCP Overview

9.1.1 Introduction to DHCP

We are in a world where the scales of networks are ever-growing and their configurations are more and more complex, computers (such as laptop computers and wireless networks) are likely to move, and the available IP addresses are far from adequate for the ever-increasing number of computers. Dynamic Host Configuration Protocol (DHCP) was introduced in such a background.

Like Bootstrap Protocol (BOOTP), DHCP adopts the client/server communications model. In this model, it is client that requests the server for configurations, such as the assigned IP address, subnet mask, and default GateWay (GW). The server will return the configuration information appropriate to the request in accordance with the configured policy. Both BOOTP and DHCP packets are encapsulated with UDP and in the structures that are highly similar.

BOOTP is running in a relatively static environment in which each host has a fixed network connection and, for each host, administrators configure a BOOTP file that will keep the same for a relatively long time.

Compared to BOOTP, DHCP is improved in two aspects. Firstly, DHCP allows computers to obtain all the desired configuration information by using only one message; secondly, it allows computers to rapidly and dynamically obtain IP addresses rather than statically specifying an address for each host.

9.1.2 IP address allocation in DHCP

1) IP address allocation policy

The time durations different types of hosts occupying IP addresses are different. For example, servers are more likely to use fixed IP addresses for a long time, some hosts perhaps need to use some dynamic IP addresses for a long period of time too, but some individuals only need to use temporarily assigned IP addresses for a short period of time.

Commensurate with these demands, a DHCP server provides three types of IP address allocation policies:

- Manual allocation, with which fixed IP addresses are assigned to a small amount of special hosts such as World Wide Web (WWW) servers.

- Auto-allocation, with which fixed IP addresses are assigned to some hosts connected to networks for the first time and these hosts are allowed to use the addresses for a long period of time.
- Dynamic allocation, with which some addresses are “leased” to client hosts. In this case, the clients need to request for new addresses upon the expiration of the leases. In fact, the addresses assigned to most client hosts are dynamic addresses.

2) IP address allocation order

A DHCP server selects an IP address for a client in the following order:

- The static IP address bound with the MAC address of the client in the database of the DHCP server.
- The client’s previous IP address, that is, the address requested in the “Requested IP Addr Option” carried in the DHCP_Discover packet sent by the client.
- A new address allocated from the server's DHCP pool of available addresses. This address is the one found first in the address pool.
- If the DHCP server does not find an available address, it will look outdated leased IP address and then conflicting IP address to find a valid one for assignment. If the attempt fails, the server will report error.

9.2 DHCP Server

9.2.1 Application environment for DHCP server

DHCP servers are well-suited to the network where:

- The network size is large, manual configuration is not an easy job, and it is hard to centralize the management on the entire network.
- The number of IP addresses available to the hosts on the network is far from adequate and it is impossible to assign a fixed IP address to each host. So the hosts, being too many, have to obtain dynamic IP addresses from a DHCP server in this case. In addition, limitation is placed on the number of concurrent users.
- On networks, most hosts are not assigned fixed IP addresses except of a few of them.

9.2.2 Fundamentals of DHCP server

As shown in the following figure, a typical DHCP application network usually comprises a DHCP server and multiple clients (such as PCs and laptop computers).

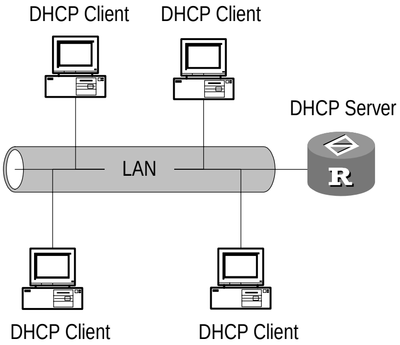


Figure 9-1 Network diagram for a DHCP server application

In order to obtain a valid dynamic IP address, a DHCP client should exchange different information with the server in different stages, three usual situations are:

1) First network access of DHCP client

In this case, the DHCP client should undergo four stages in order to set up a connection with a DHCP server.

- Discover stage where the DHCP client is searching for a DHCP server. In this stage, the client broadcast a DHCP_Discover packet on the network and only DHCP servers respond to it.
- Offer stage where DHCP servers offer IP addresses to the client. Upon receipt of the DHCP_Discover packet from the client, each DHCP server sends a DHCP_Offer packet carrying an unassigned IP address selected from its IP address pool to the client with other settings. To guarantee that the offered IP address is unique, each of them does an ARP probe before that.
- Selecting stage where the DHCP client picks one IP address out of all the offers. If the client receives offers from multiple DHCP servers, it only accepts the one reaching first. Then, it broadcasts a DHCP_Request packet containing the IP address, which was assigned and wrapped in the DHCP_Offer packet by DHCP server, to all the DHCP servers.
- Final check stage where the DHCP client checks the offered IP address. After receiving a DHCP_ACK packet, the client broadcasts an ARP packet destined to the offered IP address. If no response is received after a specified period of time, the client uses the IP address.
- Except for the selected DHCP server, all other DHCP servers can allocate their offered IP addresses to other requesting clients.

2) Non-first network access of DHCP client

If it is not the first time for the DHCP client to access the network, it should undergo the following procedure in order to set up a connection with a DHCP server.

- When a DHCP client that has a successful access record accesses the network again, it only needs to broadcast a DHCP_Request packet containing the IP address assigned to it the last time instead of sending a DHCP_Discover packet.

- Upon the receipt of the DHCP_Request packet, the DHCP server sends back a DHCP_ACK packet allowing the client to use the requested address if it is still unallocated.
- If the DHCP server has allocated that IP address to some other DHCP client or it is not available to the client for other reasons, the DHCP server sends back a DHCP_NAK packet. Upon the receipt of the packet, the client may send a new DHCP_Discover packet requesting a new IP address.

3) Renew the IP address lease

DHCP server takes back the dynamic IP address allocated to DHCP client when the lease expires. If DHCP client still wants to use this address, it should renew the IP address lease.

In practice, when the DHCP client starts or is at the half of the lease limit, it can send a DHCP_Request packet to DHCP server to complete lease renewal. If the current IP address is still valid, DHCP server returns DHCP_ACK packet to notify DHCP client that it has renewed the IP address lease.

4) Configure PC (Windows operating system for example)

Use the **ipconfig**/**release** command under DOS environment or run [winipcfg/release] at GUI (graphic user interface) to release an existing IP address. Then the user PC sends DHCP_Release packet to DHCP server. Use the **ipconfig /renew** command under DOS environment or run [winipcfg/renew] at GUI to request for new IP address. Now the user PC sends the DHCP_Discover packet to DHCP server.

You can also use the **ipconfig**/**renew** command on the user PC or run [winipcfg /renew] at GUI to renew the IP address lease.

The following figure presents the procedures described above:

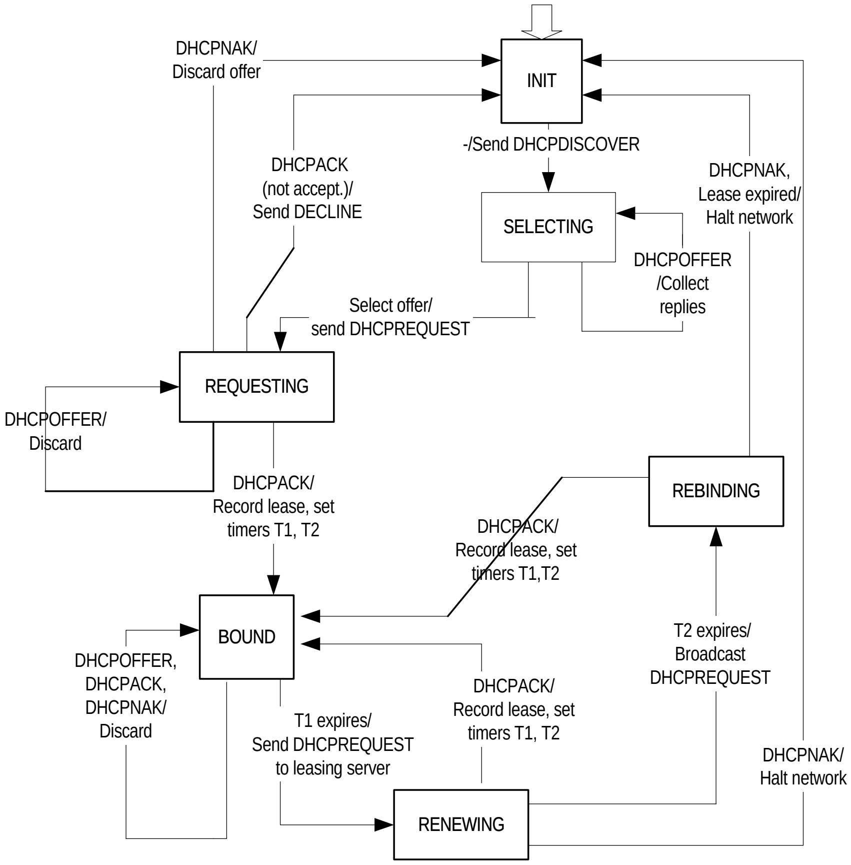


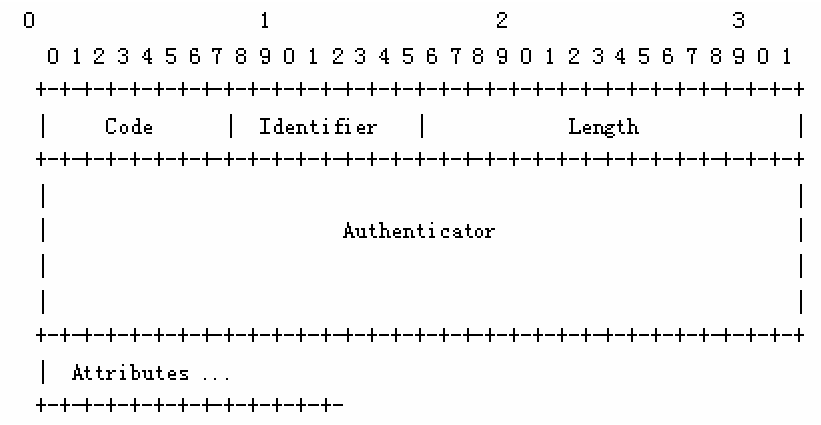
Figure 9-2 DHCP client state transit

9.2.3 Introduction to DHCP Accounting

DHCP accounting enables a DHCP server to notify the RADIUS server of the start or end of accounting when assigning or reclaiming a lease. The cooperation of the DHCP server and RADIUS server implements the network accounting function, and at the same time improves the network security to a certain degree.

I. Structure of the DHCP accounting packet

The interactive operations between the DHCP server and the RADIUS server are based on two types of packets: accounting start request and accounting stop request. The two types of packets have the similar structure, and the only difference lies in the Attributes field. The following figure illustrates the packet structure:



```
 0                   1                   2                   3
  0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
 |     Code      |  Identifier   |            Length             |
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
 |                                                               |
 |                         Authenticator                         |
 |                                                               |
 |                                                               |
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
 |  Attributes ...
 +-+-+-+-+-+-+-+-+-+-+-+-+-
```

Figure 9-3 Structure of the DHCP accounting packet

- Code: One byte for identifying the type of the DHCP accounting packet. A value of 4 indicates an accounting start request, while a value of 5 indicates an accounting stop request. If the Code field of an accounting packet is not valid, the packet is discarded.
- Identifier: One byte for matching requests and responses. The RADIUS server checks this field for duplicate requests from the same IP address and UDP port of a client.
- Length: Two bytes for identifying the length of the accounting packet.
- Authenticator: 16 bytes for identifying the information between the RADIUS server and client.

II. Fundamental of DHCP accounting

After you complete AAA authentication and RADIUS configuration on a router with the DHCP server function enabled, the DHCP server acts as a RADIUS client. For the authentication process of the DHCP server acting as a RADIUS client, refer to the “Introduction to the RADIUS Protocol” section of the "Security” part in this manual. The following describes only the interactive accounting operations between the DHCP server and the RADIUS server.

- After sending a DHCP_ACK packet with the IP configuration parameters to the DHCP client, the DHCP server sends an accounting start request to the specified RADIUS server. The RADIUS server processes the accounting start request, makes a record, and sends a response to the DHCP server.
- Once reclaiming a lease for some reason, the DHCP server sends an accounting stop request to the RADIUS server immediately. The RADIUS server processes the accounting stop request, stops the recording for the DHCP client, and sends a response to the DHCP server. A lease can be reclaimed for an expired lease, a release request from the DHCP client, a manual reclamation operation, an address pool removal operation, and the like.

- If the RADIUS server of the specified domain is unreachable for some reason, the DHCP server sends up to three DHCP accounting start requests (including the first sending attempt) at regular intervals. If the three start requests bring no response from the RADIUS server, the DHCP server does not send start requests any more.

9.2.4 Option 82 Support on the DHCP Server

Option 82 is a relay agent information option in the DHCP packet. When a request packet from a DHCP client travels through a DHCP relay on its way to the DHCP server, the DHCP relay inserts the option 82 field into the request packet. Option 82 includes many sub-options, but the DHCP server supports only sub-option 5 at present. When the DHCP relay adds the IP address of a segment into sub-option 5 of option 82, the DHCP server can assign an IP address or the configuration information according to option 82.

I. Basic concepts for option 82

1) Options

Options is a length-variable field in the DHCP packet for carrying information such as part of the lease information and packet type. It can include up to 255 options and must comprise at least one option.

2) Option 82

Option 82, also known as relay agent information option, is a part of the Options field of DHCP packet. According to RFC3046, option 82 lies before option 255 and after the other options. Option 82 can include up to 255 sub-options and must comprise at least one sub-option. Up to now, the frequently used sub-options in option 82 are sub-option 1, sub-option 2, and sub-option 5.

3) Sub-option 1

As a sub-option of option 82, sub-option 1 represents the agent circuit ID, namely Circuit ID. It holds the VLAN-ID and MAC address of the switch port for the DHCP client, which usually you must configure on the DHCP relay.

Generally, sub-option 1 and sub-option 2 must be used in conjunction to identify information about the DHCP source end.

4) Sub-option 2

Sub-option 2 is also a sub-option of option 82 and represents the remote agent ID, namely Remote ID. It holds the MAC address of the DHCP relay, which usually you must configure on the DHCP relay.

Generally, sub-option 1 and sub-option 2 must be used in conjunction to identify information about the DHCP source end.

5) Sub-option 5

Sub-option 5, another sub-option of option 82, represents link selection. It holds the IP address added by the DHCP relay, so that the DHCP server can assign an IP address on the same segment as the address.

Note:

Currently, DHCP from Huawei Technology implements only part of the functions of option 82: The DHCP server supports only sub-option 5 in option 82, and the DHCP relay supports only sub-options 1 and 2 in option 82.

II. Operating mechanism of option 82 support on the DHCP server

Sub-option 5 of option 82 for DHCP server operates on these principles:

- On a network with a DHCP relay, the DHCP relay forwards the DHCP request packet broadcasted by a DHCP client to the DHCP server.
- Upon receiving a request packet forwarded by the DHCP relay, the DHCP server determines whether sub-option 5 of option 82 is present in the packet. If the sub-option is present, the DHCP server looks up the local address pools, assigns an IP address on the same segment as that in sub-option 5 to the client, and responds with a packet with option 82.
- After receiving the response from the DHCP server, the DHCP relay strips off option 82 and forwards the resulted packet to the DHCP client.

III. Protocols and standards

The protocols related with option 82 for DHCP server include these:

- RFC2131 Dynamic Host Configuration Protocol
- RFC3527 Link Selection sub-option

9.2.5 BIMS Option Support on the DHCP Server

BIMS option for DHCP server enables a DHCP server to notify a DHCP client of the information about the branch intelligent management system (BIMS) server when assigning an IP address, making the DHCP client be able to use the BIMS server for software backup and upgrade after obtaining an IP address. The code of the BIMS option is 217.

I. Structure of the BIMS Option packet

The BIMS option is added into the Options field of a response generated by the DHCP server for a DHCP client. Since DHCP clients from different manufacturers process DHCP responses differently, the DHCP server adds the BIMS option to both

DHCP_OFFER and DHCP_ACK packets. The structure of the BIMS option packet is as follows:

```
 Code       Len      IP:port:sharekey
 +-------+------+------+------+------+------+--...-+------+
 |  217  |   N  |  i1  |  i2  |  i3  |  i4  | …|  iN  |
 +-------+------+------+------+------+------+--...-+------+
```

Figure 9-4 Structure of the BIMS option packet

The BIMS option packet has a structure similar to those of other option packets. It also contains the Code field for identifying the number of the option and the Len field for identifying the length of the option packet.

The i1 to iN fields mainly carry the IP address, protocol port, and shared key of the BIMS server, which are represented by a string. For example, if the IP address of the BIMS server is 192.168.1.1, the port number is 80, and the shared key is abcdefg, then these fields carry the string of 192.168.1.1.80.abcdefg.

II. Fundamental of BIMS Option for DHCP Server

1) A DHCP client sends a request to the DHCP server for an IP address and configuration parameters.
2) When receiving a request, the DHCP server checks the locally configured address pools. You can enable the BIMS option feature for a global address pool or interface address pool of the DHCP server. If the address to be assigned to the client is from an address pool for which BIMS option is enabled, the DHCP server encapsulates the IP address, protocol port, and shared key of the BIMS server together with the IP configuration parameters in the response.
3) When receiving the response with the BIMS option information from the DHCP server, the DHCP client resolves the BIMS option information to obtain the IP address, protocol port, and shared key of the BIMS server. After that, the client periodically sends connection requests to the BIMS server for software backup and upgrade.

9.2.6 Introduction to Option 184

Option 184 is an RFC reserved option, and the information it carries can be customized. 3Com defines four proprietary sub-options for this option, enabling the DHCP server to encapsulate the information required by a DHCP client in the response packet to the client. The four sub-options of option 184 mainly carry information about voice. The following lists the sub-options and the carried information:

- Sub-option 1: IP address of the network call processor (NCP-IP).
- Sub-option 2: IP address of the alternate server (AS-IP).

- Sub-option 3: Voice VLAN configuration.
- Sub-option 4: Fail-over call routing.

I. Meanings of the sub-options for option 184

- NCP-IP

The NCP-IP sub-option carries the IP address of the network call processor (NCP). When used in option 184, this sub-option must be the first sub-option, that is, sub-option 1.

The IP address of the NCP server carried by sub-option 1 of option 184 is intended for identifying the server acting as the network call controller and used for application download.

- AS-IP

The AS-IP sub-option carries the IP address of the alternate server (AS), and is the second sub-option of option 184, that is, sub-option 2. The AS-IP sub-option takes effect only when sub-option 1 (that is, the NCP-IP sub-option) is defined.

The alternate NCP server identified by sub-option 2 of option 184 acts as the backup of the NCP server and is used only when the IP address carried by the NCP-IP sub-option is unreachable or invalid.

- Voice VLAN configuration

The voice VLAN configuration sub-option carries the ID of the voice VLAN and the flag indicating whether the voice VLAN identification function is enabled. This sub-option is the third sub-option of option 184, that is, sub-option 3.

The sub-option 3 of option 184 comprises two parts, which carry the previously mentioned two items respectively. A flag value of 0 indicates that the voice VLAN identification function is not enabled, in which case the information carried by the VLAN ID part will be neglected. A flag value of 1 indicates that the voice VLAN identification function is enabled.

- Fail-over call routing

The fail-over call routing sub-option carries the IP address for fail-over call routing and the associated dial number. This sub-option is the fourth sub-option of option 184, that is, sub-option 4.

The IP address for fail-over call routing and the dial number in sub-option 4 of option 184 refer to the IP address and dial number of the session initiation protocol (SIP) peer. When the NCP server and alternate NCP server (if configured) are unreachable, a SIP user can use the configured IP address and dial number of the peer to establish a connection and communicates with the peer SIP user.

📖 **Note:**

For the configurations specifying to add sub-option 2, sub-option 3, and sub-option 4 in the response packets to take effect, you must configure the DHCP server to add sub-option 1.

II. Operational mechanism of using option 184 on DHCP server

The DHCP server encapsulates the information for option 184 to carry in the response packets sent to the DHCP clients. Supposing that the DHCP clients are on the same segment as the DHCP server, the operational mechanism of option 184 support on DHCP server is as follows:

1) A DHCP client sends to the DHCP server a request packet carrying option 55, which indicates the client requests the configuration parameters of option 184.
2) The DHCP server checks the request list in option 55 carried by the request packet, and then adds the sub-options of option 184 in the Options field of the response packet sent to the DHCP client.

📖 **Note:**

Only when the DHCP client specifies in option 55 of the request packet that it requires option 184, does the DHCP server add option 184 in the response packet sent to the client.

9.2.7 DHCP Address Allocation Support of WAN Interfaces

The traditional DHCP client function can only be implemented on Ethernet interfaces, while all the current functions of DHCP server, DHCP relay, and DHCP client can be implemented on WAN interfaces encapsulating PPP, HDLC, or FR. The DHCP-enabled WAN interfaces include synchronous/asynchronous serial interface and E1 interface.

The following describes the operational procedure of the DHCP server and DHCP client based on the encapsulated link layer protocol.

I. Enabling DHCP address allocation on a WAN interface encapsulating PPP

With PPP encapsulated and DHCP enabled, an interface starts with PPP negotiation, and after achieving negotiation success, performs DHCP packet interaction. The following lists the detailed procedure:

1) After the LCP negotiation over the PPP link succeeds, the local client (the DHCP client) sends a DHCP-Discover request packet to the peer (the DHCP server), which the DHCP server discards.
2) During IPCP negotiation, the local client uses the IP address of another interface or an address that is all 0s to negotiate with the peer. After the IPCP negotiation succeeds, the DHCP client broadcasts the DHCP request packet over the PPP link. For the address allocation procedure, refer to section 9.2.2 "Fundamentals of DHCP server".
3) After obtaining an IP address, the DHCP client fills the IP address to the corresponding WAN interface and notifies the PPP module that the local address has changed. Then, the local PPP module performs the IPCP negotiation again to notify the peer of the IP address change.

II. Enabling DHCP address allocation on a WAN interface encapsulating FR

The operational procedure of DHCP on an FR link is similar to that on Ethernet. However, since an FR interface may have multiple logical channels, when an FR interface is used as DHCP client to apply for an IP address, the following happen:

- If the FR interface is configured to allow dynamic address mapping, the DHCP client can broadcast the DHCP request packet directly to perform normal DHCP negotiation and obtain an IP address.
- If the FR interface is configured with static address mapping, the **broadcast** keyword must be configured at the same time, so that the DHCP request packet can be broadcasted over multiple logical channels and the DHCP client can obtain an IP address.

III. Enabling DHCP address allocation on a WAN interface encapsulating HDLC

When the link layer protocol is HDLC, once the DHCP client initiates a DHCP request, the DHCP server can assign an IP address to the client directly.

9.3 DHCP Relay

The early Dynamic Host Configuration Protocol (DHCP) is only applicable to the case where DHCP server and client are in the same sub-net, but not to the trans-segment case. To achieve dynamic host configuration, it is required to configure a DHCP server for every segment, as obviously uneconomical.

DHCP relay can solve this problem. With DHCP relay, the client in a LAN can communicate with the DHCP server in another sub-net and get IP address successfully. That is, DHCP clients in several sub-nets can share one DHCP server, as is significant for saving cost and centralized management.

You may use a host or router as a DHCP relay simply by running a DHCP relay agent program on it.

9.3.1 Principle of DHCP Relay

The following figure illustrates DHCP relay networking.

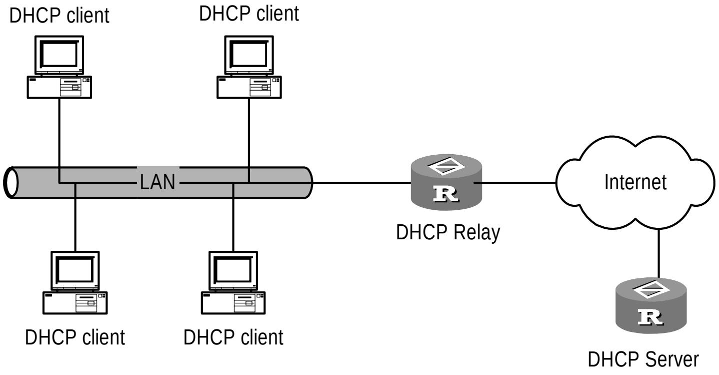


Figure 9-5 Network diagram for DHCP relay

DHCP relay works on this principle:

- When DHCP client starts and runs DHCP initialization, it sends configuration request packet to the local network.
- If there is a DHCP server in the network, it begins DHCP configurations without DHCP relay.
- If not, the local network processes the packet and forwards it to the specified DHCP server in another sub-net.
- The DHCP server undertakes configurations according to the information from the client and sends the configuration information through DHCP relay back to the client. Till now, dynamic configuration for the client ends is completed. In practice, multiple message exchange processes may be required to finish client configuration.

DHCP relay supports transparent transmission of DHCP broadcast messages and can transmit broadcast messages from DHCP client (or server) transparently to the DHCP server (or client) in another sub-net.

In real network, DHCP relay function is often implemented at a specific interface of a router. So you should configure IP relay address for the interface to specify a target DHCP server.

9.3.2 Option 82 Support on the DHCP Relay

Option 82 is a relay agent information option in the DHCP packet.

When a request packet with option 82 from a DHCP client reaches a DHCP relay on its way to the DHCP server, the DHCP relay may drop it, forward it with its option 82 information intact, or forward it with its original option 82 information replaced.

Option 82 provides many sub-options. Among them, only sub-option 1 and sub-option 2 are available on the DHCP relay. Option 82 allows the address information of the DHCP client and the DHCP relay such as MAC address and VLAN ID, to be recorded on the DHCP server. In conjunction with other software, it may implement DHCP address assignment restriction and accounting.

I. Operating mechanism of option 82 support on the DHCP relay

When obtaining an IP address through a DHCP relay, the DHCP client goes through four phases, discovery, offer, selecting, and final check, as it would directly through a DHCP server. This section however, describes only the operating mechanism of option 82 support on the DHCP relay.

The following is how option 82 support is operating on the DHCP relay:

1) The DHCP client broadcasts a request when it is initialized.
2) If no DHCP server is present on the local network, the DHCP relay connected to the network checks the packet for the option 82 field. If the packet does not carry the option 82 field, the DHCP relay inserts the option 82 field into the packet and forwards it with the MAC address and VLAN ID of the switch port connected to the DHCP client, and the MAC address of the DHCP relay itself. If the packet carries option 82 information, the DHCP relay does one of the following depending on the adopted strategy:

- Drop the packet.
- Forward the packet with its option 82 information intact.
- Forward the packet with its option 82 information being replaced with that of the DHCP relay.
- When the DHCP server receives the request, it records the option 82 information and then sends a response carrying DHCP configuration and option 82 information back to the DHCP relay.
- The DHCP relay sends the received response to the DHCP client with option 82 information removed.

Note:

To accommodate the DHCP request processing mechanisms of different DHCP relay vendors, the DHCP relay with option 82 support enabled inserts option 82 information into all DHCP requests, whether they are DHCP_DISCOVER or DHCP_Request.

II. Protocols and standards

The DHCP relay supports option 82 in compliance with the following protocols:

- RFC 2131 Dynamic Host Configuration Protocol (DHCP)
- RFC 3046 DHCP Relay Agent Information Option

9.4 DHCP Common Configuration

DHCP common configurations refer to those configurations suitable for both DHCP server and DHCP relay. The configuration tasks include

- Enable/disable DHCP services
- Configure pseudo-DHCP server detection

9.4.1 Enabling/Disabling DHCP

For both DHCP server and DHCP relay, DHCP configurations can take effect only after DHCP is enabled.

Perform the following configurations in the system view.

Table 9-1 Enable/disable DHCP

Operation	Command
Enable DHCP.	**dhcp enable**
Disable DHCP.	**undo dhcp enable**

By default, DHCP is enabled.

Note:

DHCP can operate normally only after you correctly set the system clock.

9.4.2 Configuring Pseudo-DHCP Server Detection

Pseudo-DHCP servers are unauthorized DHCP servers. Upon the request for IP address from a DHCP client, a pseudo-DHCP server might communicate with the client and may allocate incorrect IP address to the client.

You can configure pseudo-DHCP server detection to record IP address and interface information of DHCP server. Then the administrator can easily find and deal with the pseudo-DHCP server.

Perform the following configurations in system view.

Table 9-2 Configure pseudo-DHCP server detection

Operation	Command
Enable pseudo-DHCP server detection.	**dhcp server detect**
Disable pseudo-DHCP server detection.	**undo dhcp server detect**

By default, pseudo-DHCP server detection is disabled.

9.5 DHCP Server Configuration

DHCP server configuration tasks include

- Setting interfaces to operate in DHCP server mode
- Adding DHCP address pool
- Defining allocation mode of DHCP address pool
- Excluding IP address from auto allocation
- Defining IP address lease expiry limit
- Configuring domain name for DHCP client
- Configuring DNS (Domain Name Server) IP address for DHCP client
- Configuring NetBIOS IP address for DHCP client
- Defining NetBIOS node type for DHCP client
- Configuring DHCP customization items
- Configuring egress gateway router for DHCP client
- Configuring ping packet transfer in DHCP server
- Clearing DHCP information

Note:

Differences between global address pool and interface address pool:

- The global address pool is created with **dhcp server ip-pool** command in system view and it takes effect within the scope of this router.
- The interface address pool is established automatically when the Ethernet interface is configured with valid unicast IP address and the **dhcp select interface** command is configured; it is effective only in the interface. Its address segment range is the segment for the Ethernet interface. The commands related to interface address pool can be configured only when the interface address pool exists.

9.5.1 Setting Interfaces to Operate in DHCP Server Mode

When the router receives a DHCP packet with itself being the destination, the router handles the packet depending on the specified operating mode. When operating in DHCP server mode, the router forwards the packet to the local DHCP server; when operating in relay mode, the router forwards the packet to an external DHCP server.

Perform the following configuration in interface view to have the current interface operate in DHCP server mode.

Table 9-3 Set the current interface to operate in DHCP server mode

Operation	Command
Send DHCP packets to the local DHCP server and allocate addresses from the global address pool	**dhcp select global** [**subaddress**]
Send DHCP packets to the local DHCP server and allocate addresses from the interface address pool	**dhcp select interface**
Restore the default	**undo dhcp select**

Perform the following configuration in the system view to have the specified interfaces operate in DHCP server mode.

Table 9-4 Set multiple interfaces to operate in DHCP server mode

Operation	Command
Send DHCP packets to the local DHCP server and allocate addresses from the global address pool	**dhcp select global** [**subaddress**] { **interface** *interface-type interface-number* [**to** *interface-type interface-number*] **|** **all** }
Send DHCP packets to the local DHCP server and allocate addresses from the interface address pool	**dhcp select interface** { **interface** *interface-type interface-number* [**to** *interface-type interface-number*] **|** **all** }
Resets the default	**undo dhcp select** { **interface** *interface-type interface-number* [**to** *interface-type interface-number* **|** **all** }

By default, **dhcp select global** applies. Currently DHCP server is available on following interfaces:

- Ethernet interface (subinterface)
- Virtual Ethernet interface
- Synchronous/asynchronous serial interface encapsulated with PPP, HDLC, or frame relay
- E1 interface

🕮 **Note:**

- To use interface address pools for address allocation, you must configure the **dhcp select interface** command.
- The **subaddress** keyword allows the DHCP server to assign a DHCP client an IP address from the subaddress segment of the Ethernet interface. This IP address is selected from the global address pool corresponding to the subaddress segment. When subaddress allocation is enabled, the Ethernet interface on the DHCP server must be assigned a subaddress and the specified global address pool must reside in the same segment with the subaddress, otherwise the IP address is assigned to the client from the primary address segment of the Ethernet interface.
- Currently subaddress allocation is available only on Ethernet interface and Virtual Ethernet interface.
- If both DHCP Server and DHCP Client are enabled on an interface, subaddress allocation will fall into confusion. Therefore, avoid enabling both of them on an interface.

9.5.2 Adding Global DHCP Address Pool

DHCP server allocates IP addresses from the address pool. When DHCP client originates DHCP requests to DHCP server, the server will choose a proper address pool and select a free IP address, which, along with other parameters (for example DNS IP address, address lease limit), is sent to the client. With VRP, a DHCP server by far can be configured with 128 global address pools.

The address pools in DHCP server is in tree structure: the native segment address as root, sub-net addresses as branch, addresses bound to the clients as leaf nodes. This structure guarantees configuration inheritance: the sub-net (son node) inherits the configurations of the native segment (father node); the client (grandson node) inherits the configurations of the sub-net. For those common parameters, for example domain name, you can just configure them at the native segment or sub-net. You can view the structure of the address pools with the **display dhcp server tree** command. The order for those address pools at the same level is defined by creation time.

Perform the following configurations in the system view.

Table 9-5 Add global DHCP address pool

Operation	Command
Adds DHCP address pool or enter DHCP address pool view	**dhcp server ip-pool** *pool-name*
Deletes DHCP address pool	**undo dhcp server ip-pool** *pool-name*

By default, no global DHCP address pool is created.

9.5.3 Defining Allocation Mode of DHCP Address Pool

You can select static address binding or dynamic address binding accordingly, but you can only choose one of them for a given DHCP address pool.

For dynamic address allocation mode, you should specify address range. Static address binding can be deemed as a special DHCP address pool with only one address.

I. Configuring static address binding for global address pool

Some DHCP clients may require a fixed IP address, i.e., binding the client MAC address or identifier to an IP address. Then when the DHCP client with this MAC address or identifier requests for an IP address, DHCP server will find and allocate the bound IP address to the client.

Perform the following configurations in the DHCP address pool view.

Table 9-6 Configure static address binding

Operation	Command
Configure static IP address binding	**static-bind ip-address** *ip-address* [**mask** *netmask*]
Delete static IP address binding	**undo static-bind ip-address**
Configure static client MAC address or identifier binding	**static-bind** { **mac-address** *mac-address* **|** **client-identifier** *client-identifier* }
Delete static client MAC address or identifier binding	**undo static-bind** { **mac-address |** **client-identifier** }

By default, no binding is configured and the client MAC address/identifier is set as Ethernet.

Note:

The command **static-bind ip-address** must be used along with the **static-bind** { **mac-address | client-identifier**} command. If you use the commands repeatedly, the new configuration will overwrite the previous one.

Only one static binding that contains a MAC address or identifier can be configured.

II. Configuring static address binding for interface address pool

Perform the following configurations in Ethernet interface (or subinterface) view.

Table 9-7 Configure static address binding for interface address pool

Operation	Command
Configure a static address binding for the address pool of the current interface	**dhcp server static-bind ip-address** *ip-address* { **mac-address** *mac-address* | **client-identifier** *client-identifier* }
Delete a static address binding	**undo dhcp server static-bind** { **ip-address** *ip-address* | **mac-address** *mac-address* | **client-identifier** *client-identifier* }

Among all the bindings of an interface, each IP address, MAC address, and client identifier must be unique. In addition, the client identifier and the corresponding MAC address are mutually exclusive, that is, an IP address can only be bound to a MAC address or client identifier, but not both.

III. Configuring dynamic address allocation

For the dynamic addresses (including permanent ones or those lease limit dynamic ones), you should configure them with address pool range. Currently only one address segment can be set to an address pool, which is defined by the mask.

Perform the following configurations in the DHCP address pool view.

Table 9-8 Configure IP address range for dynamic allocation

Operation	Command
Configure IP address range for dynamic allocation	**network** *ip-address* [**mask** *netmask*]
Delete dynamic IP address range	**undo network**

By default, no DHCP address pool is available for dynamic allocation.

If you use the command repeatedly, the new configurations will overwrite the previous ones.

9.5.4 Excluding IP Address from Auto Allocation

In configuring address allocation by DHCP server, you should exclude those in-use IP addresses. Otherwise, one IP address may be allocated to two hosts, which will cause address conflict.

Perform the following configurations in the system view.

Table 9-9 Exclude IP address from auto allocation

Operation	Command
Forbid auto allocation of an IP address	**dhcp server forbidden-ip** *low-ip-address* [*high-ip-address*]
Allow auto allocation of the IP address	**undo dhcp server forbidden-ip** *low-ip-address* [*high-ip-address*]

By default, all addresses in the DHCP address pool will be automatically allocated.

Using this command repeatedly, you can exclude multiple IP addresses from being allocated.

9.5.5 Defining IP Address Lease Expiry Limit

DHCP server can assign different lease duration limit for different address pools, but the same lease duration limit for the addresses in the same address pool.

Address lease duration limit cannot be renewed automatically.

The system provides different configuration modes for different types of address pools.

I. Global DHCP address pool

Perform the following configurations in the DHCP address pool view.

Table 9-10 Configure lease expiry limit for global DHCP address pool

Operation	Command
Configures expiry limit for dynamic IP address lease	**expired** { **day** *day* [**hour** *hour* [**minute** *minute*]] | **unlimited** }
Resets the lease expiry limit to the default value	**undo expired**

II. Interface DHCP address pool

Perform the following configurations in Ethernet interface (or subinterface) view.

Table 9-11 Configure lease expiry limit for interface DHCP address pool

Operation	Command
Configures expiry limit for dynamic IP address lease	**dhcp server expired** { **day** *day* [**hour** *hour* [**minute** *minute*]] | **unlimited** }
Resets the lease expiry limit to the default value	**undo dhcp server expired**

III. Multiple interface DHCP address pools

You can also configure lease limit for DHCP address pool on multiple interfaces at one blow.

Perform the following configurations in the system view.

Table 9-12 Configure lease expiry limit for DHCP address pool on multiple interfaces

Operation	Command
Configures expiry limit for dynamic IP address lease	**dhcp server expired** { **day** *day* [**hour** *hour* [**minute** *minute*]] | **unlimited** } { **interface** *interface-type interface-number* [**to** *interface-type interface-number* | **all** }
Resets the lease expiry limit to the default value	**undo dhcp server expired** { **interface** *interface-type interface-number* [**to** *interface-type interface-number* | **all** }

By default, an IP address lease expires after one day.

🕮 **Note:**

For some DHCP configuration items, the system provides different configuration modes for different types of DHCP address pools. You can configure these items respectively in the global DHCP address pool, interface DHCP address pool and multiple interface DHCP address pools.

These configuration tasks include: Configuring domain name for DHCP client, configuring DNS IP address for DHCP client, configuring NetBIOS IP address for DHCP client, defining NetBIOS node type for DHCP client and configuring DHCP customization items.

Currently, the leasing valid period specified by this command cannot exceed the year of 2106.

9.5.6 Configuring Domain Names for DHCP Clients

On a DHCP server, you may configure domain names that DHCP clients should use when obtaining the DNS service on a per-address pool basis.

Perform the following configuration in DHCP address pool view to configure the global DHCP address pool.

Table 9-13 Configure DHCP client domain name in global DHCP address pool

Operation	Command
Configures a domain name to DHCP client	**domain-name** *domain-name*
Delete the domain name to DHCP client	**undo domain-name**

Perform the following configurations in Ethernet interface (or subinterface) view to configure the interface DHCP address pool.

Table 9-14 Configure domain name to DHCP client in interface DHCP address pool

Operation	Command
Configures a domain name to DHCP client	**dhcp server domain-name** *domain-name*
Delete the domain name to DHCP client	**undo dhcp server domain-name**

Perform the following configurations in the system view to configure multiple interface DHCP address pools.

Table 9-15 Assign domain name to DHCP client in multiple interface DHCP address pools

Operation	Command
Configures a domain name to DHCP client	**dhcp server domain-name** *domain-name* { **interface** *interface-type interface-number* [**to** *interface-type interface-number*] **|** **all** }
Delete the domain name to DHCP client	**undo dhcp server domain-name** { **interface** *interface-type interface-number* [**to** *interface-type interface-number* **|** **all** }

By default, no domain name is allocated to DHCP client.

9.5.7 Configuring DNS IP Address for DHCP Client

When the host accesses the Internet through domain name, it should translate the domain name into IP address, which is implemented by Domain Name System (DNS). To access DHCP client successfully into the Internet, DHCP server ought to assign DNS IP address at the time allocating IP address to the client.

A maximum of eight DNS addresses by far can be configured in a DHCP address pool.

Perform the following configurations in the DHCP address pool view to configure global DHCP address pool.

Table 9-16 Configure DNS IP address in global DHCP address pool

Operation	Command
Configures a DNS IP address to DHCP client	**dns-list** *ip-address* [*ip-address*]
Delete the DNS IP address to DHCP client	**undo dns-list** { *ip-address* | **all** }

Perform the following configurations in Ethernet interface (or subinterface) view to configure interface DHCP address pool.

Table 9-17 Configure DNS IP address in interface DHCP address pool

Operation	Command
Configure a DNS IP address to DHCP client	**dhcp server dns-list** *ip-address* [*ip-address*]
Delete the DNS IP address to DHCP client	**undo dhcp server dns-list** { *ip-address* | **all** }

Perform the following configurations in the system view to configure multiple interface DHCP address pools.

Table 9-18 Configure DNS IP address in multiple interface DHCP address pools

Operation	Command
Add a DNS server to the DNS server list of the DHCP client	**dhcp server dns-list** *ip-address* [*ip-address*] { **interface** *interface-type interface-number* [**to** *interface-type interface-number* | **all** }
Remove the specified DNS server from the DNS server list of the DHCP client	**undo dhcp server dns-list** { *ip-address* | **all** } { **interface** *interface-type interface-number* [**to** *interface-type interface-number* | **all** }

By default, no IP address of DNS server is configured.

9.5.8 Configuring NetBIOS IP Address for DHCP Client

For those clients running on Microsoft operating system, WINS (Windows Internet Naming Service) server is required to translate host name into IP address for the hosts using NetBIOS protocol. So most Windows client may require WINS settings.

A maximum of eight NetBIOS addresses currently can be configured in a DHCP address pool.

Perform the following configurations in the DHCP address pool view to configure global DHCP address pool.

Table 9-19 Configure NetBIOS IP address in global DHCP address pool

Operation	Command
Configures a NetBIOS address to DHCP client	**nbns-list** *ip-address* [*ip-address*]
Deletes the NetBIOS address to DHCP client	**undo nbns-list** { *ip-address* **|** **all** }

Perform the following configurations in Ethernet interface (or subinterface) view to configure interface DHCP address pool.

Table 9-20 Configure NetBIOS IP address to DHCP client in interface

Operation	Command
Configures a NetBIOS address to DHCP client	**dhcp server nbns-list** *ip-address* [*ip-address*]
Deletes the NetBIOS address to DHCP client	**undo dhcp server nbns-list** { *ip-address* **|** **all** }

Perform the following configurations in the system view to configure multiple interface DHCP address pools.

Table 9-21 Configure NetBIOS IP address to DHCP client in multiple interface DHCP address pools

Operation	Command
Configures a NetBIOS address to DHCP client	**dhcp server nbns-list** *ip-address* [*ip-address*] { **interface** *interface-type interface-number* [**to** *interface-type interface-number*] **|** **all** }
Deletes the NetBIOS address to DHCP client	**undo dhcp server nbns-list** { *ip-address* **|** **all** } { **interface** *interface-type interface-number* [**to** *interface-type interface-number*] **|** **all** }

By default, no NetBIOS IP address is configured to DHCP client.

9.5.9 Defining NetBIOS Node Type for DHCP Client

Mapping must be established between the host name and IP address when DHCP client uses NetBIOS protocol for communications over Wide Area Network (WAN). In terms of mapping establishment mode, NetBIOS node can be divided as

- b-node: b here stands for broadcast, that is, the node gets mapping through broadcast.
- p-node: p here stands for peer-to-peer. The node gets mapping by communicating with the NetBIOS server.

- m-node: m here stands for mixed. It is the p-node embraces part of the broadcast attributes.
- h-node: h here stands for hybrid. It is b-node for which peer-to-peer communication is available.

Perform the following configurations in the DHCP address pool view to configure DHCP address pool.

Table 9-22 Define NetBIOS node type in global DHCP address pool

Operation	Command
Defines NetBIOS node type for DHCP client	**netbios-type** { **b-node** | **h-node** | **m-node** | **p-node** }
Resets NetBIOS node type to the default value	**undo netbios-type**

Perform the following configurations in Ethernet interface (or subinterface) view to configure interface DHCP address pool.

Table 9-23 Define NetBIOS node type in interface DHCP address pool

Operation	Command
Defines NetBIOS node type for DHCP client	**dhcp server netbios-type** { **b-node** | **h-node** | **m-node** | **p-node** }
Resets NetBIOS node type to the default value	**undo dhcp server netbios-type**

Perform the following configurations in the interface view to configure multiple interface DHCP address pools.

Table 9-24 Define NetBIOS node type in multiple interface DHCP address pools

Operation	Command
Defines NetBIOS node type for DHCP client	**dhcp server netbios-type** { **b-node** | **h-node** | **m-node** | **p-node** } { **interface** *interface-type interface-number* [**to** *interface-type interface-number*] | **all** }
Resets NetBIOS node type to the default value	**undo dhcp server netbios-type** { **interface** *interface-type interface-number* [**to** *interface-type interface-number*] | **all** }

By default, h-node is configured for DHCP client.

9.5.10 Configuring DHCP Customization Items

With further development of DHCP technology, new optional configuration items may arise. Then you can add in custom way these items into DHCP server attribute table.

Perform the following configurations in the DHCP address pool view to configure global DHCP address pool.

Table 9-25 Configure DHCP customization items

Operation	Command
Adds DHCP customization items	**option** *code* { **ascii** *ascii-string* **|** **hex** *hex-string* **|** **ip-address** *ip-address* }
Deletes DHCP customization items	**undo option** *code*

Perform the following configurations in Ethernet interface (or subinterface) view to configure interface DHCP address pool.

Table 9-26 Configure DHCP customization items

Operation	Command
Adds DHCP customization items	**dhcp server option** *code* { **ascii** *ascii-string* **|** **hex** *hex-string* **|** **ip-address** *ip-address* }
Deletes DHCP customization items	**undo dhcp server option** *code*

Perform the following configurations in the interface view to configure multiple interface DHCP address pools.

Table 9-27 Configure DHCP customization items

Operation	Command
Adds DHCP customization items	**dhcp server option** *code* { **ascii** *ascii-string* **|** **hex** *hex-string* **|** **ip-address** *ip-address* } { **interface** *interface-type interface-number* [**to** *interface-type interface-number*] **|** **all** }
Deletes DHCP customization items	**undo dhcp server option** *code* { **interface** *interface-type interface-number* [**to** *interface-type interface-number*] **|** **all** }

9.5.11 Configuring Egress Gateway Router for DHCP Client

DHCP client must use an egress gateway for data transmission and receiving when accessing the server or host with the IP address not in the segment.

Perform the following configurations in the DHCP address pool view.

Table 9-28 Configure egress gateway router for DHCP client

Operation	Command
Configures egress gateway router for DHCP client	**gateway-list** *ip-address* [*ip-address*]
Deletes the egress gateway router	**undo gateway-list** { *ip-address* **|** **all** }

By default, no egress gateway router is configured to DHCP client.

A maximum of eight egress gateway addresses currently can be configured in a DHCP.

Note:

To configure multiple egress gateway addresses, give out the ip-address parameter one by one.

9.5.12 Configuring ping Packet Transfer in DHCP Server

To prevent IP address conflict, DHCP server will check whether an address has been allocated before allocating it to the client.

You can initiate IP address check with the command **ping**. If no response is sent back, then continue to send ping packets till the maximum ping packets allowed are sent. If there is still no response sent back with the preset time limit, then you can conclude that this IP address is free. This ensures the client a unique IP address.

Perform the following configurations in the system view.

Table 9-29 Configure ping packet transfer in DHCP server

Operation	Command
Configures maximum number of ping packet for transfer in DHCP server	**dhcp server ping packets** *number*
Resets the maximum number of ping packet to the default value	**undo dhcp server ping packets**
Configures time limit to receive ping response	**dhcp server ping timeout** *milliseconds*
Resets time limit to receive ping response to the default value	**undo dhcp server ping timeout**

By default, two ping packets can be transferred and 500 milliseconds are set for DHCP server to receive ping response.

The DHCP server detects address collisions by sending pings, while the DHCP client does that by sending ARP packets.

9.5.13 Configuring DHCP Accounting

When DHCP accounting is enabled, the DHCP server sends accounting packets to the RADIUS accounting server in the specific domain when issuing and releasing leases.

After DHCP accounting is configured, the DHCP server issues leases with IP address, lease deadline and other configuration information to a user when the user applies for an IP address. After leases are issued, the server will intermediately inform the RADIUS accounting server in the specific domain to send a RADIUS START request; when for some reason, DHCP server leases are released (the reasons can be lease out of date, the receipt of the request from the user, manually deleting the lease, or manually delete address pool), the DHCP server will inform the RADIUS accounting server in the specific domain to send a RADIUS STOP accounting request.

In this case, the RADIUS server records information about use of IP addresses, but does not really perform accounting.

I. Configuration prerequisites

Before configuring DHCP accounting, perform the following configuration:

- Complete the related configuration on the DHCP server and client, ensuring that the DHCP server can assign IP addresses to clients.
- Complete the configuration related to domain and RADIUS accounting server. That is, configure the RADIUS scheme for the specified domain, and configure the RADIUS server in the RADIUS scheme.

For configuration of domain and RADIUS accounting server, refer to the “Security” part of this manual.

II. Configuring DHCP accounting in system view

Table 9-30 Configure DHCP accounting in system view

Operation	Command	Description
Enter system view	**system-view**	—
Configure the interfaces to work in DHCP server mode and assign addresses from specified interface address pools	**dhcp select interface** { **all** | **interface** *interface-type interface-number* [**to** *interface-type interface-number*] }	Required

Operation	Command	Description
Enable DHCP accounting for addresses from specified interface address pool and configure the domain for DHCP accounting	**dhcp server accounting domain** *domain-name* { **interface** *interface-type interface-number* [**to** *interface-type interface-number*] | **all** }	Required
Enter interface view	**interface** *interface-type interface-number*	To create interface address pools, you must configure IP addresses for the interfaces involved in the above commands.
Configure the IP address of the interface	**ip address** *ip-address net-mask*	

Note:

- This mode applies to the scenario that the DHCP server allocates IP addresses from interface address pools.
- In this mode, you can configure a range of subinterfaces, and therefore can enable DHCP accounting on multiple subinterfaces at a time.

III. Configuring DHCP accounting in interface view

Table 9-31 Configure DHCP accounting in interface view

Operation	Command	Description
Enter system view	**system-view**	—
Enter interface view	**interface** *interface-type interface-number*	Required
Configure the IP address of the interface	**ip address** *ip-address net-mask*	Required
Configure the interface to work in DHCP server mode and assign addresses from the interface address pools	**dhcp select interface**	Required
Enable DHCP accounting for addresses from the interface address pools and configure the domain for DHCP accounting	**dhcp server accounting domain** *domain-name*	Required

Note:

- This mode applies to the scenario where the DHCP server allocates IP addresses from interface address pools.
- In this mode, you can enable DHCP accounting in interface view. Therefore, this mode applies when you want to enable DHCP accounting on a single interface.

IV. Configuring DHCP accounting in global DHCP address pool view

Table 9-32 Configure DHCP accounting in global DHCP address pool view

Operation	Command	Description
Enter system view	**system-view**	—
Configure specified interfaces to work in DHCP server mode and assign addresses from the global DHCP address pool	**dhcp select global** [**subaddress**] { **all** | **interface** *interface-type interface-number* [**to** *interface-type interface-number*]}	Required
Enter DHCP address pool view	**dhcp server ip pool** *pool-name*	—
Configure the IP addresses for dynamic allocation	**network** *ip-address* [**mask** *netmask*]	—
Enable DHCP accounting for addresses in the DHCP address pool and configure the domain for DHCP accounting	**accounting domain** *domain-name*	By default, DHCP accounting is not enabled.

Note:

This mode applies to the scenario where the DHCP server allocates IP addresses from the global DHCP address pool.

9.5.14 Configuring BIMS Option Support on the DHCP Server

I. Configuration prerequisites

Before configuring the feature of BIMS option for DHCP server, complete the following tasks:

- Enable the DHCP server function and configure the address pools on the router.
- Configure the DHCP clients.
- Ensure that the DHCP clients, DHCP server, and BIMS server are reachable.

II. Configuring BIMS option

The following table describes the BIMS option configuration tasks.

Table 9-33 Configure BIMS option

Operation	Command	Description
Enter system view	**system-view**	—
Enable and configure BIMS option in system view	**dhcp server bims-server ip** *ip-address* **port** *port-number* **sharekey** *key* { **interface** *interface-type interface-number* [**to** *interface-type interface-number*] **|** **all** }	Required. These are three alternative ways of configuring BIMS options.
Enable and configure BIMS option in interface view	**dhcp server bims-server ip** *ip-address* [**port** *port-number*] **sharekey** *key* **undo dhcp server bims-server**	
Enable and configure BIMS option in global DHCP address pool view	**dhcp server ip-pool** *pool-name*	
	bims-server ip *ip-address* **port** *port-number* **sharekey** *key*	

Note:

- If you configure BIMS option for a global address pool, the DHCP server sends the BIMS option information together with the lease when assigning an IP address from the global address pool to a DHCP client.
- If you configure BIMS option for an interface, the DHCP server sends the BIMS option information together with the lease when assigning an IP address from the interface address pool to a DHCP client.
- If you specify the **all** keyword in the **dhcp server bims-server ip** command, the DHCP server sends the BIMS option information together with the lease when assigning an IP address from any of the interface address pools to a DHCP client.

9.5.15 Configuring Option 184 Support on the DHCP Server

You may configure suboptions of option 184 for the DHCP server in system view, interface view, or DHCP address pool view. Whichever view you select, you must configure interface address pools for involved interfaces.

I. Configuration prerequisites

Before configuring option 184 support on the DHCP server, make sure that:

- The network parameters, and address pool and address lease allocation policies are configured.
- The DHCP client is reachable to the DHCP server.

II. Configuring option 184 in system view

Table 9-34 Configure option 184 for the DHCP server in system view

Operation	Command	Description
Enter system view	**system-view**	—
Configure specified interfaces to operate in DHCP server mode and assign addresses from specified interface address pools	**dhcp select interface** { **all | interface** *interface-type interface-number* [**to** *interface-type interface-number*] }	Required
Configure suboption NCP-IP of option 184	**dhcp server voice-config ncp-ip** *ip-address* { **all | interface** *interface-type interface-number* [**to** *interface-type interface-number*] }	Required
Configure suboption AS-IP of option 184	**dhcp server voice-config as-ip** *ip-address* { **all | interface** *interface-type interface-number* [**to** *interface-type interface-number*] }	Optional This suboption is available only after you configure suboption NCP-IP.
Configure suboption Voice VLAN Configuration of option 184	**dhcp server voice-config voice-vlan** *vlan-id* { **enable | disable** } { **all | interface** *interface-type interface-number* [**to** *interface-type interface-number*] }	Optional This suboption is available only after you configure suboption NCP-IP.
Configure suboption Fail-Over Routing of option 184	**dhcp server voice-config fail-over** *ip-address dialer-string* { **all | interface** *interface-type interface-number* [**to** *interface-type interface-number*] }	Optional This suboption is available only after you configure suboption NCP-IP.
Enter interface view	**interface** *interface-type interface-number*	Repeat these two steps to assign IP address to each involved interface. Otherwise, your address pool creation may fail.
Assign an IP address to the interface	**ip address** *ip-address net-mask*	

📖 **Note:**

Configure option 184 in system view when the DHCP server uses interface address pools to assign addresses.

This approach allows you to configure option 184 on multiple interfaces at the same time.

III. Configuring option 184 in interface view

Table 9-35 Configure option 184 for the DHCP server in interface view

Operation	Command	Description
Enter system view	**system-view**	—
Enter interface view	**interface** *interface-type interface-number*	Required
Assign an IP address to the interface	**ip address** *ip-address net-mask*	Required
Configure the interface to operate in DHCP server mode and assign addresses from its address pool	**dhcp select interface**	Required
Configure suboption NCP-IP of option 184	**dhcp server voice-config ncp-ip** *ip-address*	Required
Configure suboption AS-IP of option 184	**dhcp server voice-config as-ip** *ip-address*	Optional This suboption is available only after you configure suboption NCP-IP.
Configure suboption Voice VLAN Configuration of option 184	**dhcp server voice-config voice-vlan** *vlan-id* { **enable** | **disable** }	Optional This suboption is available only after you configure suboption NCP-IP.
Configure suboption Fail-Over Routing of option 184	**dhcp server voice-config fail-over** *ip-address dialer-string*	Optional This suboption is available only after you configure suboption NCP-IP.

📖 **Note:**

Configure option 184 in interface view when the DHCP server uses an interface address pool to assign addresses.

This approach allows you to configure option 184 on a single interface.

IV. Configuring option 184 in DHCP global address pool view

Table 9-36 Configure option 184 for the DHCP server in global address pool view

Operation	Command	Description
Enter system view	**system-view**	—
Configure specified interfaces to operate in DHCP server mode and assign addresses from a global address pool	**dhcp select global** [**subaddress**] { **all** | **interface** *interface-type interface-number* [**to** *interface-type interface-number*] }	Required
Enter DHCP address pool view	**dhcp server ip pool** *pool-name*	Required
Configure an IP address range for dynamic address allocation	**network** *ip-address* [**mask** *netmask*]	Required
Configure suboption NCP-IP of option 184	**voice-config ncp-ip** *ip-address*	Required
Configure suboption AS-IP of option 184	**voice-config as-ip** *ip-address*	Optional This suboption is available only after you configure suboption NCP-IP.
Configure suboption Voice VLAN Configuration of option 184	**voice-config voice-vlan** *vlan-id* { **enable** | **disable** }	Optional This suboption is available only after you configure suboption NCP-IP.
Configure suboption Fail-Over Routing of option 184	**voice-config fail-over** *ip-address dialer-string*	Optional This suboption is available only after you configure suboption NCP-IP.

📖 **Note:**

Configure option 184 in DHCP global address pool view when the DHCP server uses a global address pool to assign addresses.

9.5.16 Configuring Option 82 Support on the DHCP Server

I. Configuration prerequisites

Before configuring option 82 support on the DHCP server, make sure that:

- The DHCP server function is enabled on your device and the network parameters of the device are configured.
- The network parameters, and address pool and address lease allocation policies are configured for the DHCP server.
- The DHCP server device is reachable.

For more information, refer to the part discussing DHCP.

II. Enabling option 82 support on the DHCP server

Table 9-37 Configure option 82 support on the DHCP server

Operation	Command	Description
Enter system view	**system-view**	—
Enable option 82 support on the DHCP server	**dhcp server relay information enable**	Required By default, option 82 support is enabled on the DHCP server.

9.5.17 Clearing DHCP Information

Use the **display dhcp server ip-in-use** command in any view to display dynamic address binding information of the address pool. You can delete the information using the corresponding command.

Use the **display dhcp server conflict** command in any view to display DHCP address conflict information. You can delete the information using the corresponding command.

Use the **display dhcp server statistics** command in any view to display DHCP server information. You can delete the information using the corresponding command.

Perform the following configurations in user view.

Table 9-38 Clear DHCP information

Operation	Command
Clear binding information of a specific IP address	**reset dhcp server ip-in-use ip** *ip-address*
Clear dynamic address binding information of the global address pool	**reset dhcp server ip-in-use pool** [*pool-name*]
Clear dynamic address binding information of the interface address pool	**reset dhcp server ip-in-use interface** [*interface-type interface-number*]
Clear binding information of all address pools	**reset dhcp server ip-in-use all**
Clear conflict information of a specific IP address	**reset dhcp server conflict** *ip-address*
Clear conflict information of all address pool	**reset dhcp server conflict all**
Clear statistical information in DHCP server	**reset dhcp server statistics**

9.6 DHCP Relay Configuration

DHCP relay configuration tasks include:

- Setting interfaces to operate in DHCP relay mode
- Specifying external DHCP server addresses
- Configuring DHCP server load sharing from DHCP relay
- Clearing DHCP relay information

9.6.1 Setting Interfaces to Operate in DHCP Relay Mode

When the router receives a DHCP packet with itself being the destination, the router handles the packet depending on the specified operating mode. When operating in DHCP server mode, the router forwards the packet to the local DHCP server; when operating in relay mode, the router forwards the packet to an external DHCP server.

Perform the following configuration in interface view to have the current interface operate in DHCP relay mode.

Table 9-39 Set the current interface to operate in DHCP relay mode

Operation	Command
Relay DHCP packets to an external DHCP server for address allocation	**dhcp select relay**
Restore the default	**undo dhcp select**

📖 **Note:**

These commands must be performed on an Ethernet interface (subinterface), virtual Ethernet interface, synchronous/asynchronous serial interface encapsulated with PPP, HDLC or frame relay, or E1 interface.

Perform the following configuration in the system view to have the specified interfaces operate in DHCP relay mode.

Table 9-40 Set multiple interfaces to operate in DHCP relay mode

Operation	Command
Relay DHCP packets to an external DHCP server for address allocation	**dhcp select relay** { **interface** *interface-type interface-number* [**to** *interface-type interface-number*] | **all** }
Resets the default	**undo dhcp select** { **interface** *interface-type interface-number* [**to** *interface-type interface-number*] | **all** }

By default, **dhcp select global** applies.

Currently DHCP relay is available on following interfaces:

- Ethernet interface (subinterface)
- Virtual Ethernet interface
- Synchronous/asynchronous serial interface encapsulated with PPP, HDLC, or frame relay
- E1 interface

📖 **Note:**

When a PC wants to obtain an IP address through the DHCP relay on an Ethernet subinterface on the router, the PC needs to connect to the router through a switch. In this case, you need to make proper link configuration on the switch beforehand.

9.6.2 Specifying External DHCP Servers

When receiving a DHCP broadcast, the interface with DHCP relay enabled relays the DHCP broadcast to the specified external DHCP server.

Perform the following configuration in interface view to specify an external DHCP server address to which the received DHCP broadcasts are to be forwarded.

Table 9-41 Specify an external DHCP server address on the current interface

Operation	Command
Specify an external DHCP server address on the current interface	**ip relay address** *ip-address*
Delete one or all external DHCP server addresses on the current interface	**undo ip relay address** { *ip-address* **|** **all** }

Perform the following configuration in system view to specify an external DHCP server address to which the DHCP broadcasts received on the specified interfaces are to be forwarded.

Table 9-42 Configure an external DHCP server address for multiple interfaces

Operation	Command
Specify an external DHCP server address for the interfaces in the specified range	**ip relay address** *ip-address* [**interface** *interface-type interface-number* [**to** *interface-type interface-number*] **|** **all**]
Remove an external DHCP server address for the interfaces in the specified range	**undo ip relay address** { *ip-address* **|** **all** } { **interface** *interface-type interface-number* [**to** *interface-type interface-number*] **|** **all** }

Note:

Since the packets sent by the DHCP client are broadcast in some stages, the corresponding interface must support broadcast.

Up to 20 external DHCP server addresses can be configured on an interface.

9.6.3 Configuring DHCP Server Load Sharing for DHCP Relay

You can use DHCP relay to configure several DHCP servers and share traffic load between them.

When multiple DHCP servers are configured, the DHCP Relay can distribute among them requests from the clients using the HASH algorithm and thus achieve load sharing.

Perform the following configurations in the system view.

Table 9-43 Configure DHCP server load sharing

Operation	Command
Configures DHCP server load sharing	**ip relay address cycle**
Cancel DHCP server load sharing	**undo ip relay address cycle**

By default, no load sharing between DHCP servers is available.

9.6.4 Configuring Option 82 Support on the DHCP Relay

I. Configuration prerequisites

Before configuring option 82 support on the DHCP relay, make sure that:

- The DHCP relay function is enabled on your device and the network parameters of the device are configured.
- The network parameters, and address pool and address lease allocation policies are configured for the DHCP relay.
- The DHCP relay device is reachable.

For more information, refer to the part discussing DHCP.

II. Configuring option 82 support on the DHCP relay

Table 9-44 Configure option 82 support on the DHCP relay

Operation	Command	Description
Enter system view	**system-view**	—
Enable option 82 support on the DHCP relay	**dhcp relay information enable**	Required
Configure a strategy for handling packets with option 82 on the DHCP relay	**dhcp relay information strategy** { **drop** | **keep** | **replace** }	Required By default, the DHCP relay uses the replace strategy when handling a request with option 82.

9.6.5 Clearing DHCP Relay Information

Use the command **display dhcp relay statistics** in any view to view DHCP relay information. The information can certainly be cleared out.

Perform the following configuration in user view.

Table 9-45 Clear DHCP relay information

Operation	Command
Clears DHCP relay information	**reset dhcp relay statistics**

9.7 DHCP Client Configuration

When configuring the DHCP client, you only need to perform one command to have an interface to get IP address from DHCP. Currently, DHCP is available only on the following interfaces:

- Ethernet interface or subinterface
- Synchronous/asynchronous serial interface encapsulated with PPP, HDLC, or frame relay
- E1 interface or ATM interface

Perform the following configurations in interface view.

Table 9-46 Configure DHCP client

Operation	Command
Enable DHCP client to get local IP address	**ip address dhcp-alloc**
Disable DHCP client	**undo ip address dhcp-alloc**

By default, DHCP client is disabled.

Note:

- After configured to obtain an IP address through DHCP, an interface cannot be configured with any subaddress. That is, the command **ip address dhcp-alloc** is in conflict with the command **ip address** *ip-address mask* **sub**, so you can only use one of them.
- When one interface on a DHCP client goes up after obtaining an IP address from a DHCP server configured with the **gateway-list** command, a default route entry appears in the routing table on the client, with the next hop being the gateway specified by the command. If the DHCP client obtains various gateway addresses and uses the Quidway series router, the DHCP client chooses the first address in the gateway-list in the DHCP Server address pool to add to the default route after it obtains the interface IP address and the interface is UP, for example,

```
[Quidway] display ip routing-table
Routing Table: public net
Destination/Mask   Protocol    Pre  Cost      Nexthop        Interface
0.0.0.0/0            DHCPDEF       255     0         23.23.0.2      Ethernet2/1.1
```

The default route priority is 255, cost is 0.

- When an interface with frame relay encapsulation is functioning as the DHCP client, the interface adopts frame relay dynamic address mapping or broadcast-mode frame relay static address mapping.

Currently, virtual Ethernet interfaces support DHCP server but not DHCP client.

9.8 Displaying and Debugging DHCP

When the aforementioned configurations are completed, use the **display** command in any view to show DHCP running status, for the purpose of checking configuration information.

Using the **debugging** command in user view, you can enable DHCP debugging.

I. Displaying and debugging DHCP server

Table 9-47 Display and debug DHCP

Operation	Command
Display free address information in DHCP address pool	**display dhcp server free-ip**
Display in-conflict DHCP address information	**display dhcp server conflict** { **ip** *ip-address* | **all** }
Display expired leases in DHCP address pool	**display dhcp server expired** { **ip** *ip-address* | **pool** [*pool-name*] | **interface** [*interface-type interface-number*] **all** }

Operation	Command
Display DHCP address binding information	**display dhcp server ip-in-use** { **all** | **ip** *ip-address* | **pool** [*pool-name*] | **interface** [*interface-type interface-number*] }
Display DHCP server information	**display dhcp server statistics**
Display tree architecture information about DHCP address pool	**display dhcp server tree** { **pool** [*pool-name*] | **interface** [*interface-type interface-number*] | **all** }
Enable DHCP server debugging	**debugging dhcp server** { **error** | **event** | **packet** | **all** }
Disable DHCP server debugging	**undo debugging dhcp server** { **event** | **packet** | **error** | **all** }
Delete the information of DHCP dynamic address binding	**reset dhcp server ip-in-use** [**ip** *ip-address* | **pool** [*pool-name*] | **interface** [*interface-type interface-num*] | **all**]
Delete the statistics of DHCP address conflict	**reset dhcp server conflict** { *ip-address* | **all** }
Delete the statistics of the DHCP server	**reset dhcp server statistics**

Note:

The lease information is not saved in the DHCP server's Flash when you execute the save command. So there is not any lease information in the configuration files when the system restarts or when you use the reset dhcp server ip-in-use command to delete the lease information. If a client requests lease renewal at this time, the system will not permit it but require the client to apply for the IP address again.

II. Displaying and debugging DHCP relay

Table 9-48 Display and debug DHCP relay

Operation	Command
Display the IP information of the interface of DHCP relay	**display ip interface** [*interface-type interface-number*]
Display the statistics of DHCP relay	**display dhcp relay statistics**
Display the DHCP relay address of the interface	**display dhcp relay address** { **interface** *interface-type interface-num* | **all** }

Operation	Command
Display IP-to-MAC address associations for DHCP clients obtaining IP addresses through the DHCP relay	**display dhcprelay-security**
Enable the DHCP relay debugging	**debugging dhcp relay** { **all** | **error** | **event** | **packet** [**client mac** *mac-address*] }
Disable the DHCP relay debugging	**undo debugging dhcp relay** { **all** | **error** | **event** | **packet** [**client mac** *mac-address*] }

III. Displaying and debugging DHCP client

Table 9-49 Display and debug DHCP client

Operation	Command
Display the statistics of DHCP client	**display dhcp client** [**verbose**]
Enable the DHCP client debugging	**debugging dhcp client** { **error** | **event** | **packet** | **all** }
Disable the DHCP client debugging	**undo debugging dhcp client** { **error** | **event** | **packet** | **all** }

9.9 DHCP Configuration Examples

9.9.1 DHCP Server Configuration Example

There are two types of DHCP networking modes: one is that both DHCP server and DHCP client are in the same sub-net and they exchange signals using DHCP. The second is that DHCP server and DHCP client are in different sub-nets, which requires DHCP relay agent to achieve IP address allocation. The configuration details are the same in both networking modes.

I. Network requirements

DHCP server allocates dynamic IP address to DHCP client which is in the same sub-net. The address pool segment 10.1.1.0/24 is divided into two sub-segments: 10.1.1.0/25 and 10.1.1.128/25. The two Ethernet interface of DHCP server are with the addresses 10.1.1.1/25 and 10.1.1.129/25.

For the segment 10.1.1.0/25, the address lease limit is 10 days and 12 hours; the domain name is huawei.com; the DNS address is 10.1.1.2; no NetBIOS is configured; the egress router address is 10.1.1.126. For the segment 10.1.1.128/25, the address limit is 5 days; the DNS address is 10.1.1.2; the NetBIOS address is 10.1.1.4; the egress router address is 10.1.1.254.

II. Networking topology

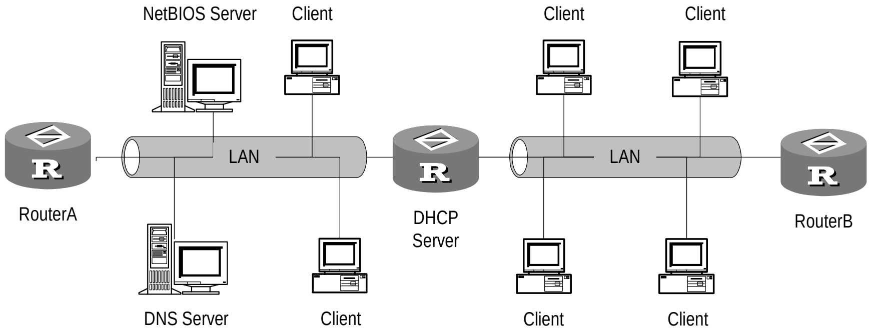


Figure 9-6 DHCP server and client in the same sub-net

III. Configuration procedure

# Enable DHCP

```
[Quidway] dhcp enable
```

# Configure specified interfaces to operate in DHCP server mode and allocate IP addresses from a global address pool.

```
[Quidway] dhcp select global interface ethernet 0/0/0 to ethernet 0/0/1
```

# Forbid auto allocation of IP addresses (including DNS address, NetBIOS address and egress gateway address)

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

# Configure common attributes for DHCP address pool 0 (address pool range, domain name and DNS address).

```
[Quidway] dhcp server ip-pool 0
[Quidway-dhcp-0] network 10.1.1.0 mask 255.255.255.0
 [Quidway-dhcp-0] dns-list 10.1.1.2
[Quidway-dhcp-0] quit
```

# Configure attributes for DHCP address pool 1 (address pool range, egress gateway address and address lease limit)

```
[Quidway] dhcp server ip-pool 1
[Quidway-dhcp-1] network 10.1.1.0 mask 255.255.255.128
[Quidway-dhcp-1] domain-name huawei.com
[Quidway-dhcp-1] gateway-list 10.1.1.126
[Quidway-dhcp-1] expired day 10 hour 12
```

# Configure attributes for DHCP address pool 2 (address pool range, egress gateway address, NetBIOS address and address lease limit).

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

9.9.2 DHCP Relay Configuration Example

I. Network requirements

The segment for DHCP client is 10.110.0.0 and that for DHCP server is 202.38.0.0. A router which supports DHCP relay function is required for forwarding DHCP messages, so that DHCP client can request configuration information (for example IP address) successfully from DHCP server.

DHCP server is configured with an IP address pool whose segment is 10.110.0.0, so the IP addresses can be allocated to the DHCP clients on this segment. DHCP server is also configured with routes to the segment 10.110.0.0.

II. Network diagram

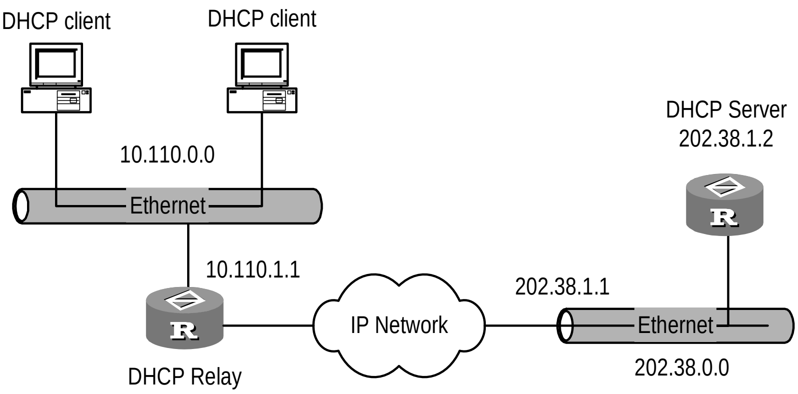


Figure 9-7 DHCP relay configuration

III. Configuration procedure

Configurations on the router:

# Enable DHCP services

```
[Quidway] dhcp enable
```

# Enter an interface where DHCP relay function has been enabled, configure IP address and mask for it, and ensure that the interface and DHCP client are in the same segment.

```
[Quidway] interface ethernet 6/0/0
[Quidway-Ethernet6/0/0] ip address 10.110.1.1 255.255.0.0
```

# Configure IP relay address for the interface to specify the target DHCP server.

```
[Quidway-Ethernet6/0/0] dhcp select relay
[Quidway-Ethernet6/0/0] ip relay address 202.38.1.2
```

Configurations on DHCP server will not be mentioned here.

9.9.3 DHCP Client Configuration Example

Two types of DHCP client configurations are mentioned here: one is that the Ethernet gets dynamic IP address, the other is that the Ethernet sub-interface gets dynamic IP address (supporting VLAN).

I. Ethernet interface as DHCP client

1) Network requirements

The interfaces Ethernet0/0/0 and Ethernet2/0/0 of the router RTA are connected respectively into LAN1 and LAN2, which are respectively configured with DHCP server 1 and DHCP server 2. The segment for LAN1 is 200.254.0.0/16 and that for LAN2 is 172.10.0.0/16. The configuration task is to make the two interfaces get IP addresses through DHCP.

2) Network diagram

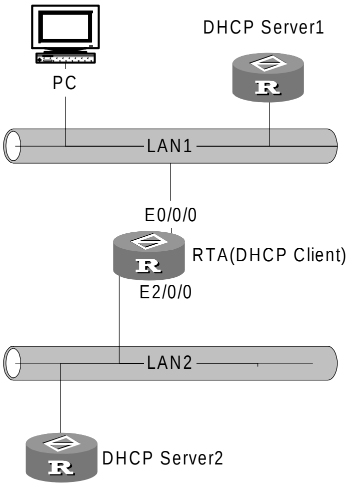


Figure 9-8 Primary interface as DHCP client

3) Configuration procedure

The configuration of both DHCP server and client are mentioned.

- Configure Server1

```
[Quidway] dhcp enable
[Quidway] interface ethernet 0/0/0
[Quidway-Ethernet0/0/0] ip address 200.254.0.1 16
[Quidway] dhcp server ip-pool 1
[Quidway-dhcp1] network 200.254.0.0 mask 255.255.0.0
```

- Configure Server2

```
[Quidway] dhcp enable
[Quidway] interface ethernet 0/0/0
[Quidway-Ethernet0/0/0] ip address 172.10.0.1 16
[Quidway] dhcp server ip-pool 2
[Quidway-dhcp2] network 172.10.0.0 mask 255.255.0.0
```

- Configure the client

# Configure Ethernet0/0/0 to obtain an IP address dynamically though DHCP.

```
[Quidway] interface ethernet 0/0/0
[Quidway-Ethernet0/0/0] ip address dhcp-alloc
```

- Configure Ethernet2/0/0 to get an IP address dynamically through DHCP

```
[Quidway] interface ethernet 2/0/0
[Quidway-Ethernet2/0/0] ip address dhcp-alloc
```

II. Ethernet sub-interface as DHCP client

1) Network requirements

DHCP servers 1 and 2 are respectively in VLAN10 and VLAN20. The configuration task is to create sub-interfaces and configure getting dynamic IP addresses respectively from the two DHCP servers.

2) Networking diagram

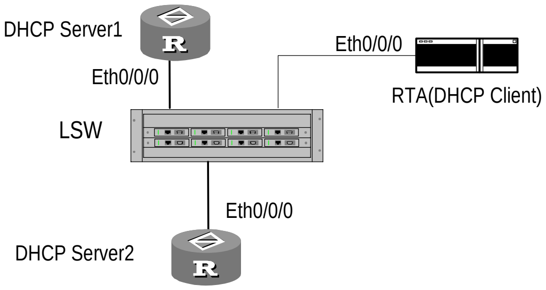


Figure 9-9 Sub-interface as DHCP client

3) Configuration procedures

Configure LAN Switch first (it is not detailed here) and make sure that DHCP servers 1 and 2 can be respectively connected into VLAN10 and VLAN 20. Then configure RTA interface as Trunk interface which enables transparent transmission of messages for VLAN 10 and VLAN 20.

The configurations of DHCP server1 and server2 are similar to those in above example, so the configurations of DHCP client are listed.

# Configure the sub-interface which gets IP address from DHCP server1.

```
[Quidway] interface ethernet 0/0/0.1
[Quidway-Ethernet0/0/0.1] vlan-type dot1q vid 10
```

```
[Quidway-Ethernet0/0/0.1] ip addr dhcp-alloc
```

# Configure the sub-interface which gets IP address from DHCP server2.

```
[Quidway] interface ethernet 0/0/0.2
[Quidway-Ethernet0/0/0.2] vlan-type dot1q vid 20
[Quidway-Ethernet0/0/0.2] ip addr dhcp-alloc
```

9.9.4 DHCP Accounting Configuration Example

I. Network requirements

As shown in Figure 9-10,

- The DHCP server is connected to the DHCP client and the RADIUS server through interface Ethernet1/0/0 and Ethernet1/0/1 respectively.
- The IP address of the RADIUS server is 10.1.2.2/24.
- DHCP accounting is enabled on the DHCP server. The global DHCP address pool is 10.1.1.0 and domain 123 is assigned to the pool for DHCP accounting.

It is required that the RADIUS accounting server could track IP address use of the DHCP client.

II. Network diagram

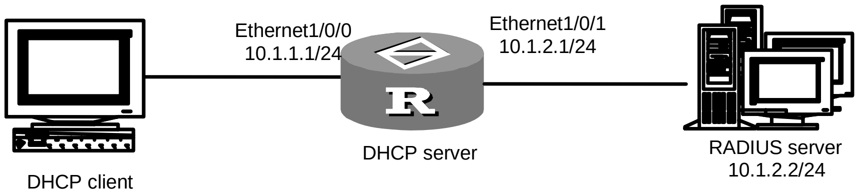


Figure 9-10 Network diagram for DHCP accounting

III. Configuration procedure

# Configure DHCP server network parameters.

```
<Quidway> system-view
[Quidway] interface ethernet 1/0/0
[Quidway-Ethernet1/0/0] ip address 10.1.1.1 255.255.255.0
[Quidway-Ethernet1/0/0] quit
[Quidway] interface ethernet 1/0/1
[Quidway-Ethernet1/0/1] ip address 10.1.2.1 255.255.255.0
[Quidway-Ethernet1/0/1] quit
```

# Enable DHCP server.

```
[Quidway] dhcp enable
[Quidway] dhcp select global interface ethernet 1/0/0 to ethernet 1/0/1
```

# Create a domain, create a RADIUS scheme, and associate them for DHCP accounting.

```
[Quidway] radius scheme 123
[Quidway-radius-123] primary authentication 10.1.2.2
[Quidway-radius-123] quit
[Quidway] domain 123
[Quidway-isp-123] scheme radius-scheme 123
[Quidway-isp-123] quit
```

# Configure an address pool for the DHCP server.

```
[Quidway] dhcp server ip-pool test
[Quidway-dhcp-pool-test] network 10.1.1.0 mask 255.255.255.0
```

# Configure DHCP accounting and assign domain 123 to the pool just created.

```
[Quidway-dhcp-pool-test] accounting domain 123
```

9.9.5 Option 184-Supported DHCP Server Configuration Example

I. Network requirements

Figure 9-11 presents a scenario, where

- 3Com VCX is functioning as the DHCP client, Quidway Router is functioning as the DHCP server.
- Quidway Router supports option 184 when assigning addresses from global address pools. The suboption NCP-IP of option 184 is set to 3.3.3.3, AS-IP to 2.2.2.2, voice VLAN state to enable and ID to 1, Fail-Over IP to 1.1.1.1 and fail-over dial string to 99*.

II. Network diagram

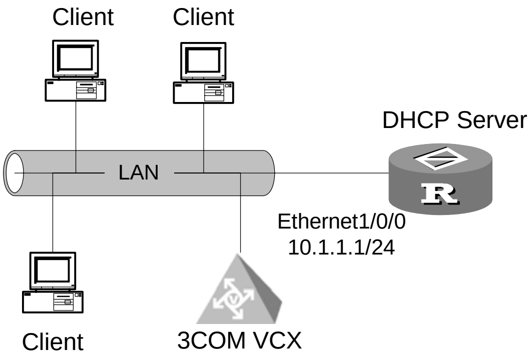


Figure 9-11 Network diagram for option 184 support on the DHCP server

III. Configuration procedure

1) Configure the DHCP client (on 3Com VCX)

Enable DHCP client, and configure it to request all suboptions of option 184 when requesting an address.

2) Configure the DHCP server

```
<Quidway> system-view
[Quidway] dhcp enable
[Quidway] dhcp select global interface ethernet 1/0/0
[Quidway] dhcp server ip-pool 123
[Quidway-dhcp-pool-123] network 10.1.1.1 mask 255.255.255.0
[Quidway-dhcp-pool-123] voice-config as-ip 2.2.2.2
[Quidway-dhcp-pool-123] voice-config ncp-ip 3.3.3.3
[Quidway-dhcp-pool-123] voice-config voice-vlan 1 enable
[Quidway-dhcp-pool-123] voice-config fail-over 1.1.1.1 99*
[Quidway-dhcp-pool-voice] quit
```

9.9.6 Option 28-Supported DHCP Relay Configuration Example

I. Network requirements

As shown in Figure 9-12, two DHCP clients on 10.110.1.0 obtain IP addresses from a DHCP server through a DHCP relay.

Do the following on the DHCP relay:

- Configure option 82 support
- Use the keep strategy to handle DHCP requests with option 82.

II. Network diagram

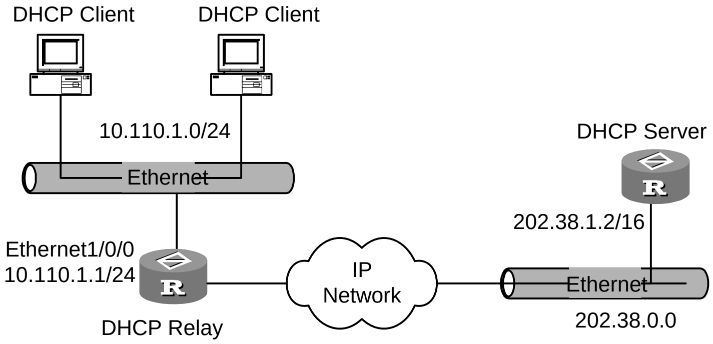


Figure 9-12 Network diagram for option 82 support on DHCP relay

III. Configuration procedure

This example assumes that the DHCP relay and the DHCP server are reachable to each other.

1) Configure the DHCP relay

# Enable DHCP.

```
<Quidway> system-view
[Quidway] dhcp enable
```

# Configure the DHCP relay interface, and assign it an IP address belonging to the same network segment.

```
[Quidway] interface ethernet 1/0/0
[Quidway-Ethernet1/0/0] dhcp select relay
[Quidway-Ethernet1/0/0] ip address 10.110.1.1 255.255.255.0
```

# Specify a DHCP server to the DHCP relay interface.

```
[Quidway-Ethernet1/0/0] ip relay address 202.38.1.2
[Quidway-Ethernet1/0/0] quit
```

# Enable option 82 support on the frame relay and specify the strategy for handling packets with option 82 to keep.

```
[Quidway] dhcp relay information enable
[Quidway] dhcp relay information strategy keep
```

2) Configure the DHCP server

Omitted

9.9.7 DHCP Configuration Example for the Serial Interface Using PPP

I. Network requirements

As shown in Figure 9-13,

- A DHCP relay uses interface Serial 2/0/1 to connect to interface Serial 2/0/1 on a DHCP client and uses interface Serial 2/0/0 to connect to a DHCP relay, both across PPP links.
- The DHCP server uses the address pool with the segment 20.20.0.0/24 for address assignment.

Perform configuration to allow interface Serial 2/0/0 on the DHCP client to obtain IP address from the DHCP server through the DHCP relay.

II. Network diagram

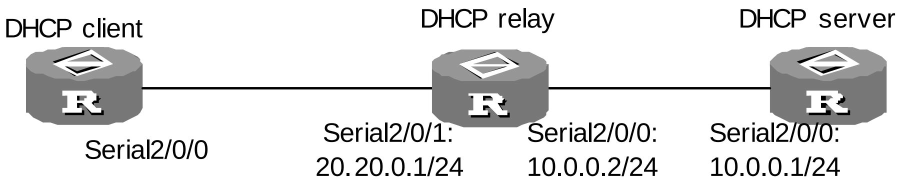


Figure 9-13 Network diagram for the DHCP support on the serial interface using PPP

III. Configuration procedure

1) Configure the DHCP server

```
<Quidway> system-view
[Quidway] dhcp enable
[Quidway] dhcp select global interface serial 2/0/0
```

```
[Quidway] dhcp server ip-pool 1
[Quidway-dhcp-pool-1] network 20.20.0.0 mask 255.255.255.0
[Quidway-dhcp-pool-1] gateway-list 20.20.0.1
[Quidway-dhcp-pool-1] domain-name huawei.com
[Quidway-dhcp-pool-1] quit
[Quidway] interface serial 2/0/0
[Quidway-serial2/0/0] link-protocol ppp
[Quidway-serial2/0/0] ip address 10.0.0.1 255.255.255.0
[Quidway-serial2/0/0] quit
[Quidway] ip route 0.0.0.0 0.0.0.0 10.0.0.2
```

2) Configure the DHCP relay

```
<Quidway> system-view
[Quidway] dhcp enable
[Quidway] interface serial 2/0/0
[Quidway-serial2/0/0] link-protocol ppp
[Quidway-serial2/0/0] ip address 10.0.0.2 255.255.255.0
[Quidway-serial2/0/0] quit
[Quidway] interface serial 2/0/1
[Quidway-serial2/0/1] link-protocol ppp
[Quidway-serial2/0/1] ip address 20.20.0.1 255.255.255.0
[Quidway-serial2/0/1] ip relay address 10.10.0.1
[Quidway-serial2/0/1] dhcp select relay
[Quidway-serial2/0/1] quit
```

3) Configure the DHCP client

```
<Quidway> system-view
[Quidway] dhcp enable
[Quidway] interface serial 2/0/0
[Quidway-serial2/0/0] link-protocol ppp
[Quidway-serial2/0/0] ip address dhcp-alloc
[Quidway-serial2/0/0] quit
```

Chapter 10 IP Performance Configuration

10.1 IP Performance Configuration

10.1.1 Configuring MTU

The maximum transmission unit (MTU) size of the interface decides whether the IP packets on the interface need to be fragmented.

Table 10-1 Configure MTU of the interface

Operation	Command
Configure MTU of the interface	**mtu** *mtu-size*
Restore to the default value of the interface MTU	**undo mtu**

The default value of the interface MTU is 1500 bytes when using Ethernet_II frame format.

10.1.2 Configuring TCP Packet Fragmentation

The parameter of TCP packet fragmentation determines whether the TCP packets are to be fragmented.

Perform these commands in interface view.

Table 10-2 Configure TCP packets fragmentation

Operation	Command
Enable TCP packet fragmentation	**tcp mss** *value*
Disable the TCP packet fragmentation	**undo tcp mss**

By default, TCP packets are not fragmented.

10.1.3 Configuring TCP Attributes

TCP attributes that can be configured include:

- syn timer: When sending the syn packets, TCP starts the syn timer. If response packets are not received before syn timeout, the TCP connection will be terminated. The range of syn timer timeout time is 2 to 600 seconds, and the default is 75 seconds.

- fin timer: When the TCP connection state turns from FIN_WAIT_1 to FIN_WAIT_2, fin timer will be started. If FIN packets are not received before fin timer timeout, the TCP connection will be terminated. The range of fin is 76 to 3600 seconds and the default of fin is 675 seconds.
- The receiving/sending buffer size of connection-oriented Socket: The range is 1 to 32 KB and the default is 8 KB.

Perform the following configuration in the interface view.

Table 10-3 Configure TCP attributes

Operation	Command
Configure syn timer time for TCP connection establishment	**tcp timer syn-timeout** *time-value*
Restore syn timer time for TCP connection establishment to default value	**undo tcp timer syn-timeout**
Configure FIN_WAIT_2 timer time of TCP	**tcp timer fin-timeout** *time-value*
Restore FIN_WAIT_2 timer time of TCP to default value	**undo tcp timer fin-timeout**
Configure Socket receiving/sending buffer size of TCP	**tcp window** *window-size*
Restore Socket receiving/sending buffer size of TCP to default value	**undo tcp window-**

10.1.4 Configuring the Sending of ICMP Redirect Messages

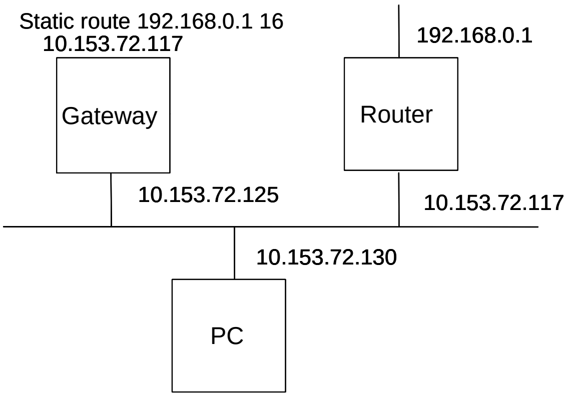


Figure 10-1 Network diagram for configuring the sending of ICMP Redirect messages

As shown in the above figure, when the PC wants to send a packet to the Router, it first sends the packet to the Gateway. With the sending of ICMP Redirect messages disabled, the Gateway forwards the packet directly to the Router. With the function enabled, the Gateway sends back an ICMP Redirect message to redirect the PC to the Router.

Perform the following configuration in system view.

Table 10-4 Configure the sending of ICMP Redirect messages

Operation	Command
Enable the sending of ICMP Redirect messages	**icmp redirect send**
Disable the sending of ICMP Redirect messages	**undo icmp redirect send**

By default, the sending of ICMP Redirect messages is enabled.

10.1.5 Displaying and Debugging IP Performance

After the above configuration, execute the **display** command in any view to display the running of the IP Performance, and to verify the effect of the configuration.

Execute the **reset** command in user views to clear the running statistic information.

Execute the **debugging** command in user view for the debugging of IP Performance.

Table 10-5 Display and debug of IP performance

Operation	Command
Show TCP connection state.	**display tcp status**
Show TCP traffic statistic information.	**display tcp statistics**
Show UDP traffic statistic information.	**display udp statistics**
Show information on all the current socket interfaces in the system.	**display ip socket** [**socktype** *sock_type*] [*task_id socket_id*]
Show information on the IP layer interface table.	**display ip interface** [*interface-type interface-number*]
Show information on the FIB of interface cards.	**display fib**
Output rows that include the string defined by *text* from the cache in regular expressions.	**display fib** | { **begin** | **include** | **exclude** } *text*
Show the filtered FIB information.	**display fib acl** *acl-number*
Show FIB entries by destination address.	**display fib** *dest-addr1* [*dest-mask1*] [**longer**]
Show FIB entries with destination addresses in the range *dest-addr1 dest-mask1* to *dest-addr2 dest-mask2*.	**display fib** *dest-addr1 dest-mask1 dest-addr2 dest-mask2*

Operation	Command
Show in certain format FIB entries that are filtered in by the rules in the specified IP-prefix list.	**display fib ip-prefix** *listname*
Show the total number of FIB entries.	**display fib statistics**
Enable IP packet information debugging	**debugging ip packet** [**acl** *acl-number*]
Disable IP packet information debugging	**undo debugging ip packet**
Enable ICMP packet debugging.	**debugging ip icmp**
Disable ICMP packet debugging.	**undo debugging tcp packet** [*task_id socket_id*]
Enable TCP packet information debugging.	**debugging tcp packet** [*task_id socket_id*]
Disable TCP packet information debugging.	**undo debugging tcp packet** [*task_id socket_id*]
Enable UDP connection information debugging	**debugging udp packet** [*task_id socket_id*]
Disable UDP connection information debugging.	**undo debugging udp packet** [*task_id socket_id*]
Enable TCP event debugging	**debugging tcp event** [*task_id socket_id*]
Disable TCP event debugging.	**undo debugging tcp event** [*task_id socket_id*]
Enable MD5 authentication debugging of TCP connection.	**debugging tcp md5**
Disable MD5 authentication debugging of TCP connection.	**undo debugging tcp md5**
Clear IP statistics.	**reset ip statistics**
Clear TCP traffic statistics.	**reset tcp statistics**
Clear UDP traffic statistics.	**reset udp statistics**

10.2 Configuring Broadcast Forwarding on an Interface

10.2.1 Configuring Broadcast Forwarding on an Interface

Normally routers do not forward layer 2 broadcasts. You may however configure them to do that for special applications, cross-network wake on LAN (WOL) for example, to forward Wakeup frames to a specified network.

Perform the following configuration in interface view.

Table 10-6 Configure broadcast forwarding on the interface

Operation	Command
Configure broadcast forwarding on the current interface	**ip forward-broadcast** [*acl-number*]
Disable broadcast forwarding on the current interface	**undo ip forward-broadcast**

By default, the router does not forward broadcasts.

10.2.2 Configuration Example for Implementing Remote WOL with Routers

I. Network requirements

PC 1 is installed with wakeup software, magic packet.exe for example, in order to wake up all PCs on the remote network segment 192.168.1.0/24.

Configure to ensure that:

- The 192.168.1.0/24 segment is reachable to PC 1.
- All PCs on 192.168.1.0/24 support remote wakeup and the wakeup function must work with power supplies, network adapters, and main boards.
- Enable broadcast forwarding on interface Ethernet 1/0/1 on the router.
- Ensure that only the Wakeup frames from the 192.168.2.1 segment are forwarded to the 192.168.1.0/24 segment.

II. Network diagram

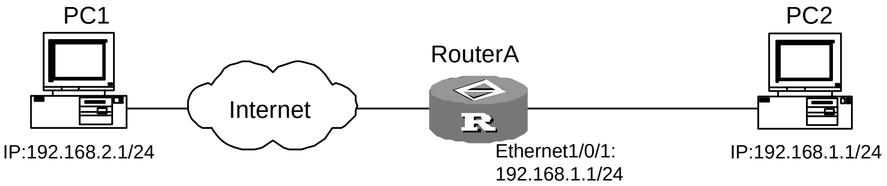


Figure 10-2 Network diagram for implementing remote WOL with routers

III. Configuration procedure

Configure Router A:

```
<Quidway> system-view
[Quidway] interface ethernet 1/0/1
[Quidway-Ethernet1/0/1] ip address 192.168.1.2 24
[Quidway-Ethernet1/0/1] ip forward-broadcast 2100
[Quidway-Ethernet1/0/1] quit
[Quidway] acl number 2100
[Quidway-acl-basic-2100] rule 1 permit source 192.168.2.1 0
[Quidway-acl-basic-2100] rule 2 deny source any
```

10.3 Configuring Fast Forwarding

10.3.1 Introduction to Fast Forwarding

Packet forwarding efficiency is a key feature evaluating router performance. According to regular flow, when a packet arrives, the router will copy it from the interface memory to the main CPU. The CPU specifies the network ID from the IP address, consults with the routing table to get the best path for forwarding the packet, and encapsulates a link layer frame header for the packet. The resulted frame is then copied to the output queue via DMA (Direct Memory Access), and during this process the main system bus is passed twice. This process is repeated for packet forwarding.

In fast forwarding, cache is used to process packets. After the system forwards the first packet in a data flow by searching routing table, corresponding exchange information is generated in the cache, and the system forwards the consequent packets in the flow by directly searching the cache. This simplifies the queuing of IP packets, cuts down the routing time and improves forwarding throughput of IP packets. Since the forwarding table in the cache has been optimized, higher searching speed is obtained.

10.3.2 Unicast Fast Forwarding

I. Features of unicast fast forwarding

The unicast fast forwarding implemented by VRP provides:

- Unicast fast forwarding on all types of high-speed link interfaces (including subinterfaces), such as Ethernet, synchronous PPP, frame relay, and HDLC.
- Unicast fast forwarding in presence of normal firewall.
- Unicast fast forwarding in presence of ASPF firewall.
- Unicast fast forwarding when NAT is configured.
- Unicast fast forwarding when GRE is in use.
- Significantly improved forwarding efficiency.

The performance of unicast fast forwarding sometimes will be affected by some characteristics such as packet queue management and packet header compression. Unicast fast forwarding is not conducted for fragmented packets.

II. Configuring Unicast Fast Forwarding

You can disable fast-forwarding as needed. For example, if load balance is required when forwarding packets, fast-forwarding must be disabled in the forwarding direction of the interface.

Perform the following configuration in interface view.

Table 10-7 Enable/disable unicast fast forwarding on an interface

Operation	Command
Enable unicast fast forwarding in both directions of the interface	**ip fast-forwarding**
Enable unicast fast forwarding on the inbound interface	**ip fast-forwarding inbound**
Enable unicast fast forwarding on the outbound interface	**ip fast-forwarding outbound**
Disable unicast fast forwarding on the interface	**undo ip fast-forwarding** [**inbound** | **outbound**]

By default, unicast fast forwarding is enabled in the input/output directions of the interface.

⚠ **Caution:**

To have an interface participate in load balancing, you must disable fast forwarding on it in the forwarding direction.

If fast-forwarding is configured on an interface, the debugging information of the IP packets on the interface will not be displayed, namely, the **debugging ip packet** command does not work.

III. Displaying and Debugging Unicast Fast Forwarding

Table 10-8 Display and debug unicast fast forwarding

Operation	Command
Display contents in the unicast fast forwarding cache	**display ip fast-forwarding cache** [*ip-address*]
Clear contents in the unicast fast forwarding cache	**reset ip fast-forwarding cache**

When fast-forwarding on the same interface is configured, ICMP redirect packets will not be sent again when IP packets pass the same interface. Otherwise, ICMP reorientation packets needs to be sent while packets are forwarded.

10.3.3 Multicast Fast Forwarding Configuration

I. Features of multicast fast forwarding

The multicast fast forwarding function has the following features:

- Supports high speed link interfaces of various types, including Ethernet, ATM, synchronous PPP, FR, and HDLC.
- Supports environments with packet filtering firewalls.
- Supports environments in which QoS is configured.
- Improves packet forwarding efficiency dramatically.

II. Configuring Multicast Fast Forwarding

Enable multicast fast forwarding as needed.

Perform the following configuration in interface view.

Table 10-9 Enable/disable multicast fast forwarding on an interface

Operation	Command
Enable multicast fast forwarding on an interface	**ip multicast-fast-forwarding**
Disable multicast fast forwarding on an interface	**undo ip multicast-fast-forwarding**

By default, multicast fast forwarding is disabled on an interface.

III. Displaying and Debugging Multicast Fast Forwarding

Table 10-10 Display and debug multicast fast forwarding

Operation	Command
Display information about the multicast fast forwarding table.	**display ip multicast-fast-forwarding cache** [*multicast-group*]
Clear the contents in the multicast fast forwarding cache	**reset ip multicast-fast-forwarding cache**

10.4 IP Performance Configuration Troubleshooting

Fault 1: TCP and UDP cannot work normally.

Troubleshooting: you can enable the corresponding debugging information output to view the debugging information.

- Use the command **debugging udp** to enable the UDP debugging information output to trace the UDP packet. When the router sends or receives UDP packets, the content format of the datagram can be displayed in real time. You can locate the problem from the contents of the datagram.

The following are the UDP packet formats:

```
*0.348541898-SOCKET-8-UDPINI:UDP packet information :
Incoming UDP datagram:
source IP address:   172.16.101.70
source port:   138
destination IP address:   172.16.255.255
destination port:   138
The length of UDP packet:   209
```

- Use the command **debugging tcp packet** to enable the TCP debugging information output to trace the TCP packets. Two TCP packet formats are available for selection. One is to debug and trace the receiving and sending of all the TCP packets of the TCP connection that take this device as one end. The operations are as follows:

```
[Quidway] info-center enable
[Quidway] quit
<Quidway> debugging tcp packet
```

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

```
*0.348623498-SOCKET-8-OUTBAND:TCP packet information :
TCP output packet:
source IP address:   172.16.201.1
source port:   23
destination IP address:   172.16.105.148
destination port:   1031
packet sequence number:   4818317
ACK sequence number:   3644122
The packet flags:  ACK  PUSH
The total length of IP packet:   436
The length of TCP header:   20
```

The other is to debug and trace the packets with SYN, FIN or RST flags being set.

Operations are as follows:

```
[Quidway] info-center enable
[Quidway] quit
<Quidway> debugging tcp event
```

Then the TCP packets received or sent can be checked in real time, and the formats are similar to those mentioned above.

Chapter 11 NAT Configuration

11.1 NAT Overview

As described in RFC1631, Network Address Translation (NAT) is to translate the IP address in IP data packet header into another IP address, which is mainly used to implement private network accessing external network in practice. NAT can reduce the depletion speed of IP address space via using several public IP addresses to represent multiple private IP addresses.

Note:

Private address denotes the address of network or host on intranet, whereas public address denotes the universal unique IP address on Internet.
IP addresses that RFC1918 reserves for private and private use are.
Class A: 10.0.0.0 to 10.255.255.255 (10.0.0.0/8)
Class B: 172.16.0.0 to 172.31.255.255 (172.16.0.0/12)
Class C: 192.168.0.0 to 192.168.255.255 (192.168.0.0/16)
IP addresses in the above three ranges will not be assigned in the Internet, so they can be used in the intranet by a company or enterprise with no need for requesting ISP or register center.

A basic NAT application is shown in the following figure.

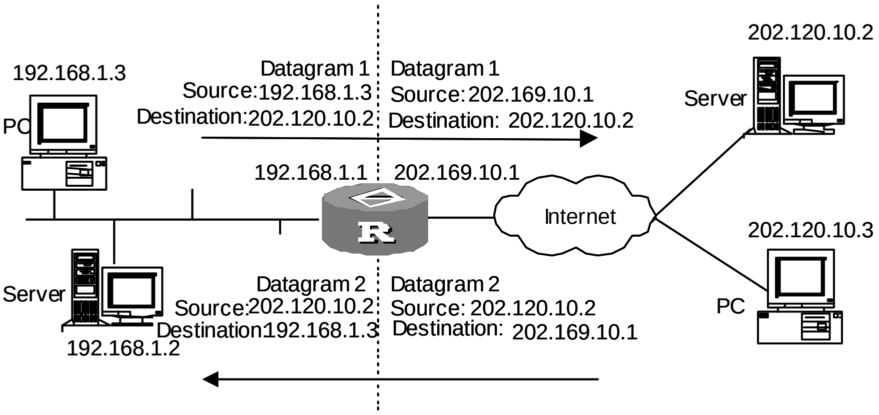


Figure 11-1 Network diagram for basic processes of address translation

NAT server such as the Router is located at the joint between private network and public network. When the internal PC at 192.168.1.3 sends the data packet1 to the external server at 202.120.10.2, the data packet will traverse the NAT server. The NAT server checks the contents in the packet header. If the destination address in the header is an extranet address, the server will translate the source address 192.168.1.3 into a valid public address on the Internet 202.169.10.1, then forward the packet to the external server and record the mapping in the network address translation list. The external server sends the response packet2 (The destination is 202.169.10.1) to the NAT server. After inquiring the network address translation list, the NAT server replaces the destination address in packet2 header with the original private address 192.168.1.3 of the internal PC.

The above mentioned NAT process is transparent for terminals such as the PC and server in the above figure. NAT "hides" the private network of an enterprise because the external server regards 202.169.10.1 as the IP address of the internal PC without the awareness of the existence of 192.168.1.3.

The main benefit NAT offers is the easy access to the outside resources for the intranet hosts while maintaining the privacy of the inner hosts.

- Since it is necessary to translate the IP address translation of data packets, the header of the data packet related to IP address cannot be encrypted. For example, encrypted FTP connection is forbidden to be used. Otherwise, FTP port cannot be correctly translated.
- Network debugging becomes more difficult. For instance, while a certain internal network host attempts to attack other networks, it is hard to point out which computer is malicious, for the host IP address is shielded.
- NAT has little impact on the performance of the network for the 10 Mbps bandwidth links, for the bottleneck is the data transfer circuit. When the baud rate is over 10 Mbps, NAT will cause some certain effects upon the performance of the route.

11.2 Functions Provided by NAT

11.2.1 Many-to-Many Address Translation and Address Translation Control

Based on the above figure, the source address of the intranet will be translated into an appropriate extranet address (the public address of the outbound interface on the NAT server in the above figure) via NAT. In this way, all the hosts in the intranet share one extranet address when they access the external network. In other words, only one host can access the external network at a time when there are many access requirements, which is called "one-to-one address translation".

An extended NAT implements the concurrent access, that is, multiple public IP addresses are assigned to a NAT server. The NAT server assigns a public address IP1 to a requesting host, keeps a record in the address translation list and forwards the data packet, then assigns another public address IP2 to another request host and so on. This is called "many-to-many address translation".

📖 **Note:**

The number of public IP addresses on the NAT server is far less than the number of hosts in the intranet because not all hosts will access the extranet at one time. The public IP address number is determined based on the maximum number of intranet hosts at the rush hour of the network.

In practice, it may be required that only some intranet hosts can access the Internet (external network). In other words, the NAT server will not translate source IP addresses of those unauthorized hosts, which is called address translation control.

Router implements many-to-many address translation and address translation control via address pool and ACL respectively.

- Address pool: A set of public IP addresses for address translation. A client should configure an appropriate address pool according to its valid IP address number, internal host number as well as the actual condition. An address will be selected from the pool as the source address during the translation process.
- ACL-based address translation: Only the data packet matching the ACL rule can be translated, which effectively limits the address translation range and allows some specific hosts to access Internet.

11.2.2 NAPT

There is another way to implement the concurrent access, that is, Network Address Port Translation (NAPT), which allows the map from multiple internal addresses to an identical public address. Therefore, it can be called as “many-to-one address translation” or address multiplex informally.

NAPT maps IP addresses and port numbers of data packets form various internal addresses to an identical public address with different port numbers. In this way, different internal addresses can share an identical public address.

The fundamentals of NAPT are shown in the following figure.

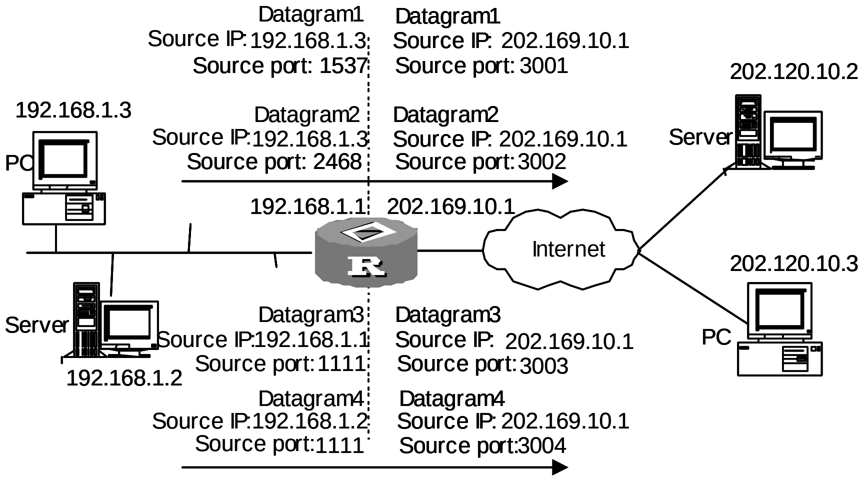


Figure 11-2 NAPT allowing multiple internal hosts to share a public address

As shown in the above figure, four data packets from internal addresses arrive at the NAT server. Among them, packet1 and packet2 come from the same internal address with different source port number, and packet3 and packet4 come from different internal addresses with an identical source port number. After the NAT mapping, all the 4 packets are translated into an identical public address with different source port numbers, so they are still different from each other. As for the response packets, the NAT server can also differentiate these packets based on their destination addresses and port numbers and forward the response packets to the corresponding internal hosts.

11.2.3 Static Net-to-Net NAT

Static net-to-net NAT maps an internal network address range to a public network address range. This approach to NAT only involves the net ID portion of the IP address. The host ID portion remains unchanged after address translation.

Static net-to-net NAT allows an internal host to access an external network through and to be accessed at its associated public address.

Static net-to-net NAT creates direct mapping between internal host addresses and public network addresses, and implements the function similar to NAT server.

However, static net-to-net NAT requires a large IP address space since it holds a one-to-one mapping between internal host addresses and public network addresses. To save IP address resources, you can use it with conventional static or dynamic NAT but should note to avoid address conflicts.

Static net-to-net NAT also supports configuration of NAT multi-instance, which enables an external host to access the host in MPLS VPN.

11.2.4 Bidirectional NAT

In comparison to conventional NAT which translates only the source or destination address, bidirectional NAT translates both addresses. It is suitable for the situation where the addresses of the hosts on your intranet overlap.

As shown in Figure 11-3, the addresses of the internal host PC 1 and the host PC 3 overlap. Normally, if PC 1 or PC 2 sends a packet to PC 3, the packet will be forwarded to PC 1 instead of the intended destination.

To ensure correct forwarding, you may configure bidirectional NAT on Router A on the basis of conventional NAT. By mapping an overlapping address pool to a temporary address pool, you can have the router translate the overlapping address into a unique temporary address.

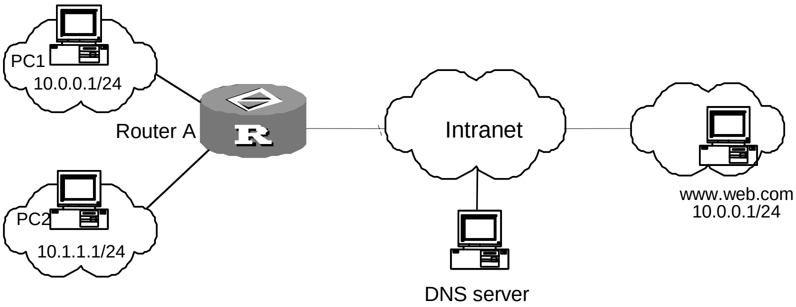


Figure 11-3 Bidirectional NAT implementation

To configure bidirectional NAT on Router A, do the following:

Step 1: Configure conventional NAT, for example, many-to-many address translation.

Configure a NAT address pool with the range of 200.0.0.1 to 200.0.0.100, and apply it to the WAN interface.

Step 2: Map an overlapping address pool to a temporary address pool, for example, 10.0.0.0 to 3.0.0.0, both with a 24-bit subnet mask.

The following are the translation conventions:

- Temporary address = Start address of the temporary address pool + (overlapping address – start address of the overlapping address pool)
- Overlapping address = Start address of the overlapping address pool + (temporary address – start address of the temporary address pool)

When PC 2 uses the domain name of PC 3 to access PC 3, packets are processed as follows:

1) PC 2 sends a DNS request for resolving www.web.com. The DNS server on the private network processes the request and sends a DNS response to Router A. Router A checks the response, and finds out that the resolved address 10.0.0.1 is an overlapping address; then it translates this address to its corresponding temporary address 3.0.0.1. After that, Router A translates the destination

address in the DNS response following the conventional NAT procedures and sends the DNS response to PC 2.

2) PC 2 initiates an access to 3.0.0.1, the temporary address for www.web.com. When Router A receives this request, it first translates the source address following the conventional NAT procedures, and then translates the destination address, which is temporary, to 10.0.0.1, the corresponding overlapping address.
3) Router A sends the request out its outgoing interface, and the request is forwarded across the WAN hop by hop to PC 3.
4) When receiving the response from PC 3, Router A checks it and finds out that the source address 10.0.0.1 is an overlapping address. The router then translates this address to its corresponding temporary address, 3.0.0.1. After translating the destination address following the conventional NAT procedures, Router A sends the response back to PC 2.

11.2.5 Internal Server

NAT can “shield” internal hosts via hiding the architecture of the intranet. However, there are times that you want to permit some hosts on external networks to access some hosts on the intranet, such as a WWW server or a FTP server. You can flexibly add servers on the intranet via NAT, for example, you can use 202.169.10.10 as the external address of the WWW server and 202.110.10.11 as the external address of the FTP server. Even 202.110.10.12:8080 can be used as the external address of the WWW server. Moreover, NAT can provide multiple identical servers such as WWW servers for external clients.

The NAT function on Quidway Series Routers provides some servers on the intranet for some hosts on external networks. When a client on an external network accesses a server on the intranet, the NAT device translates the destination address in the request packet into a private address on the internal server and translates the source address (a private address) in the response packet into a public address.

11.2.6 Easy IP

Easy IP is to use the public IP address of an interface as the source address after the address translation. It also controls the address translation based on ACL.

11.2.7 NAT Support for ALG

Network translation may result in malfunction of many application protocols. These protocols are NAT-sensitive. Some of their packets require special treatment on the IP address and port number in the valid payload, to ensure normal subsequent protocol interaction.

Application level gateway (ALG) of NAT is a common approach to NAT traversal. It substitutes the IP address and port number in payload according to address translation rules. For the involved protocol, this is transparent. So far, VRP’s NAT ALG implementation supports point to point tunneling protocol (PPTP), DNS, FTP, Internet locator service (ILS), MSN, NetBIOS over TCP/IP (NBT), session initiation protocol (SIP), and H.323.

11.2.8 Multi-Instance of MPLS VPN NAT Supported

NAT multi-instance function offers a solution that allow not only the VPN users to access the Internet from inner network, but also the MPLS VPN users to access the Internet through a single gateway, as well as the users from different VPNs to use the same private address. When an MPLS VPN user wants to access the Internet, NAT translates the IP address and the port of the internal host into external IP address and port and records the MPLS VPN information (such as protocol type and route identifier RD) about the user. When the packet is sent back, NAT restores the external IP address and port to the IP address and port of the internal host, and recognizes the MPLS VPN user. No matter what kind of NAT it is, PAT or NO-PAT, multi-instance will be supported.

VRP NAT supports the multi-instance of internal server, and provides the outside network with the access to the hosts within MPLS VPN. For example, the WWW server in VPN1 uses the address of 10.110.1.1 as the inner address, on the other hand, uses the address of 202.110.10.20 as the outer address. Using the outer address (202.110.10.20), the Internet users can get the WWW service provided by MPLS VPN1.

11.2.9 Load Balancing Among Servers

To achieve load balancing, you need to define a NAT server group on the NAT device. A server group is a set of servers that provide the same services. A weight is assigned to each server according to the processing capability. Thus, the NAT gateway will assign an external access to an appropriate server on basis of the current weights and loads of the servers to achieve load balancing.

11.2.10 NAT Limit on Maximum Connections

If a PC in a LAN is infected with virus, it initiates a large amount of connections, which consumes the router resources quickly, causes router inefficiency and in turn impacts the use of other users. To avoid these situations, NAT lays limit on the maximum connection number. It can set upper limit for the number of a connection with certain characteristic to realize NAT's limit on the maximum connections.

The configuration of restricting connections can be very flexible. You can restrict the number of different connection types through configuring policies in the following two aspects:

I. Configuring the characteristic of packets to be restricted

You can specify the packet characteristics flexibly with ACL as required, such as packet source address-based, packet destination address-based and service-based.

II. Configuring how to implement the restriction

You can determine whether to establish connection by specifying the upper threshold and lower threshold. When the connections with certain characteristic reach the upper limit, the connection is disabled. When the connections reduce to be equal or less than the lower limit, the connection is enabled.

11.3 NAT Configuration

NAT configuration includes:

- Configure address pool
- Configure NAT
- Configure Easy IP
- Configure static NAT
- Configure many-to-many NAT
- Configure NAPT
- Create a server group
- Add servers to the server group
- Configure MPLS VPN instance for server group
- Configure an internal server
- Configure NAT ALG
- Configure NAT effective time (optional)
- Configure maximum connections limit (optional)

11.3.1 Configuring Address Pool

The address pool is a collection of some consecutive IP addresses, while internal data packet needs to access external network via NAT, a certain address in the address pool will be chosen as the source address. Perform the following configurations in the system view.

Table 11-1 Configure address pool

Operation	Command
Define an address pool	**nat address-group** *group-number start-addr end-addr*
Delete an address pool	**undo nat address-group** *group-number*

🕮 **Note:**

An address pool is irremovable while this address pool has set up the association with a certain access control list for NAT.
If easy IP is the one and only function supported by the router, the address of the interface will be used plainly as the translated IP address, no NAT pool needed.

11.3.2 Configuring NAT

The NAT is accomplished by associating address pool with ACL. The association creates a relationship between such IP packets, characterized in the ACL, and that addresses, defined in the address pool. When a packet is transferred from inner network to outer network, first, the packet is filtered by the ACL to let it out, then the association between the ACL and address pool is used to find an address, which will later serve actually as the translated address.

The configuration of ACL is discussed in relevant sections.

The configuration varies from kinds to kinds of NAT.

I. Easy IP

The NAT command without the **address-group** parameter functions as the **nat outbound** *acl-number* command, implementing the "easy-ip" feature. When performing address translation, the IP address of the interface is used as the translated address and the ACL can be used to control which addresses can be translated.

Perform the following configuration under the interface view.

Table 11-2 Configure Easy IP

Operation	Command
Add association for access control list and address pool	**nat outbound** *acl-number*
Delete association for access control list and address pool	**undo nat outbound** *acl-number*

II. Using the IP address of a loopback interface for address translation

Perform the following configuration in interface view.

Table 11-3 Use the IP address of a loopback interface for address translation

Operation	Command
Associate an ACL with a Loopback interface	**nat outbound** *acl-number* **interface** *interface-type interface-number*
Remove the association of the ACL to the loopback interface	**undo nat outbound** *acl-number* **interface** *interface-type interface-number*

The IP address of the specified loopback interface is used to substitute for the source addresses of the packets matching the ACL.

III. Configuring static NAT

1) Configure a one-to-one static NAT entry

Perform the following configuration in system view.

Table 11-4 Configure a one-to-one static NAT entry

Operation	Command
Configure a static one-to-one private-to-public NAT entry	**nat static** [**vpn-instance** *vpn-instance-name*] *inside-ip global-ip*
Delete an existing static one-to-one private-to-public NAT entry	**undo nat static** [**vpn-instance** *vpn-instance-name*] *inside-ip global-ip*

2) Configure static net-to-net NAT

In comparison to conventional static NAT, static net-to-net NAT only involves the net ID portion of the IP address. The host ID portion remains unchanged after address translation.

Perform the following configuration in system view.

Table 11-5 Configure a static net-to-net NAT map

Operation	Command
Create a static net-to-net NAT map entry	**nat static inside** [**vpn-instance** *vpn-instance-name*] **ip** *inside-start-address inside-end-address* **global ip** *global-ip* { *mask* **|** *prefix-length* }
Delete a static net-to-net NAT map entry	**undo nat static inside** [**vpn-instance** *vpn-instance-name*] **ip** *inside-start-address inside-end-address* **global ip** *global-ip* { *mask* **|** *prefix-length* }

The static NAT entries configured using the **nat static inside** command must not conflict with those configured using the **nat static** command.

📖 **Note:**

When you use the **nat static inside** command to configure NAT, you must ensure that the translated **global** address does not include the existing IP address of the network devices.

3) Applying static NAT on the interface

Table 11-6 Apply static NAT on the interface

Operation	Command
Apply static NAT on the interface	**nat outbound static**

IV. Configuring many-to-many NAT

The many-to-many NAT is accomplished by associating the ACL with the NAT pool.

Perform the following configuration under the interface view.

Table 11-7 Configure many-to-many NAT

Operation	Command
Associate an ACL with an address pool	**nat outbound** *acl-number* [**address-group** *group-number*]
Remove the association between the ACL and the address pool	**undo nat outbound** *acl-number* [**address-group** *group-number*]

V. Configuring NAPT

While associating the ACL and NAT pool, the selected **no-pat** parameter denotes that only the IP address but the port information is translated, i.e. not using NAPT function; whereas the omit of the **no-pat** parameter denotes using the NAPT function.

By default, the NAPT function is active.

Perform the following configuration in interface view.

Table 11-8 Configure NAPT

Operation	Command
Associate an ACL with an address pool	**nat outbound** *acl-number* **address-group** *group-number* [**no-pat**]
Remove the association between the ACL and the address pool	**undo nat outbound** *acl-number* **address-group** *group-number* [**no-pat**]

VI. Configuring NAT Multi-instance

Easy IP, many-to-many NAT and NAPT whatsoever all support the configuration of NAT multi-instance. And all the works to be done to support **MPLS VPN** is to add **vpn–instance** *vpn-instance-name* option into the **rule** command in ACL view to show clearly which MPLS VPN user needs translation,

11.3.3 Configuring Bidirectional NAT

Perform the following configuration in system view.

Table 11-9 Configure a bidirectional NAT entry

Operation	Command
Configure a bidirectional NAT entry, mapping an overlapping address pool to a temporary address pool	**nat overlapaddress** *number overlappool-startaddress temppool-startaddress* { **pool-length** *pool-length* | **address-mask** *mask* }
Remove a bidirectional NAT entry	**undo nat overlapaddress** *number*

11.3.4 Creating a Server Group

Perform the following configuration in system view:

Table 11-10 Create a server group

Operation	Command
Create an internal server group	**nat server-group** *group-name*
Delete an internal server group	**undo nat server-group** *group-name*

⚠ **Caution:**

You cannot delete any server group that is referenced by using the **nat server** command on an interface.

11.3.5 Adding Servers to the Server Group

Add servers to the server group and assign a proper weight to them according to their processing capability.

Perform the following configuration in server group view:

Table 11-11 Add servers to a server group

Operation	Command
Add a server to a server group	**inside ip** *inside-ip* **port** *port-number* **weight** *weight-value*
Delete a server from a server group	**undo inside ip** *inside-ip*

There are at most ten servers in a server group.

⚠ **Caution:**

- Two servers in a server group must have different IP addresses.
- The port numbers of two servers in a server group must both be zero or must neither be 0.
- Two servers in different server groups may have either the same IP address or the same port number.

11.3.6 Configuring an MPLS VPN Instance for a Server Group

You can specify an MPLS VPN instance for a server group so that multiple server groups can support multiple instances.

Perform the following configuration in server group view:

Table 11-12 Configure an MPLS VPN instance for a server group

Operation	Command
Specify an MPLS VPN instance for a server group	**vpn-instance** *vpn-instance-name*
Delete an MPLS VPN instance of a server group	**undo vpn-instance** *vpn-instance-name*

⚠ **Caution:**

- You cannot specify a non-existent MPLS VPN instance for a server group that is referenced by using the **nat server** command on an interface.
- When you delete an MPLS VPN instance of a server group, you will delete the associated NAT servers from the server group.

11.3.7 Configuring an Internal Server

By configuring internal server, the related external address and port can be mapped into the internal server, thus enabling the function of external network accessing the internal server.

The mapping table for internal server and external network is configured by the **nat server** command.

The information user needs to provide includes external address, external port, internal server address, internal server port and the protocol type of the service.

Quidway series routers support using interface address as the public network address of NAT server. When the public network interface of a router obtains public address through dialing up or DHCP, its NAT server public address can be dynamically updated for a user to configure easily.

If the internal server belongs to a MPLS VPN, it is necessary to specify the *vpn-instance-name.* Otherwise the internal server will be regarded to be in an ordinary VPN rather than a MPLS VPN,

Perform the following configuration in interface view.

Table 11-13 Reference a server group

Operation	Command
Reference a server group	**nat server** [**vpn-instance** *vpn-instance-name*] **protocol** *pro-type* **global** { *global-addr* **| current-interface | interface** *interface-type interface-number* } [*global-port*] **inside** *host-addr* [*host-port*] **nat server** [**vpn-instance** *vpn-instance-name*] **protocol** *pro-type* **global** { *global-addr* **| current-interface | interface** *interface-type interface-number* } [*global-port*1 *global-port2*] **inside** *host-addr1 host-addr2 host-port* **nat server protocol** *pro-type* **global** { *global-addr* **| interface** [**loopback** *interface-number* **|** *loopback-interface-name*] **|** **current-interface** } *global-port* **inside server-group** *group-name*

Operation	Command
Dereference the server group	**undo nat server** [**vpn-instance** *vpn-instance-name*] **protocol** *pro-type* **global** { *global-addr* **| current-interface | interface** *interface-type interface-number* } [*global-port*] **inside** *host-addr* [*host-port*] **undo nat server** [**vpn-instance** *vpn-instance-name*] **protocol** *pro-type* **global** { *global-addr* **| current-interface | interface** *interface-type interface-number* } [*global-port*1 *global-port2*] **inside** *host-addr1 host-addr2 host-port* **undo nat server protocol** *pro-type* **global** { *global-addr* **|** **interface** [**loopback** *interface-number* **|** *loopback-interface-name*] **| current-interface** } *global-port* **inside server-group** *group-name*

Note:

- While either one of the *global-port* and *inside-port* being defined as "any", the other one must either be defined as "any" or not be defined.
- To ensure the normal operation of NAT while configuring **nat server** for tftp, You are required to configure the **nat outbound** command for tftp server in internal network.

11.3.8 Configuring NAT ALG

Perform the following configuration in system view.

Table 11-14 Configure NAT ALG

Operation	Command
Configure NAT ALG	**nat alg** { **dns | ftp | h323 | ils | msn | nbt | pptp | sip** }
Disable NAT ALG	**undo nat alg** { **dns | ftp | h323 | ils | msn | nbt | pptp | sip** }

By default, NAT ALG is enabled.

11.3.9 Configuring NAT Entries for Domain Names

Given an internal network that has no DNS server, you may configure NAT entries for domain names to allow internal hosts to identify and access internal servers (such as FTP and WWW) by domain name.

Perform the following configuration in system view.

Table 11-15 Configure a NAT entry for a domain name

Operation	Command
Map a domain name to a triplet of external IP address, port number, and protocol type	**nat dns-map** *domain-name global-addr global-port* { **tcp** | **udp** }
Delete the NAT entry for a domain name	**undo nat dns-map** *domain-name*

You may configure up to 16 NAT entries for domain names.

11.3.10 Configuring Address Translation Lifetimes

Since the Hash table used by NAT will not exist forever, the user can configure the lifetime of the Hash table for protocols such as TCP, UDP and ICMP respectively. If the Hash table is not used in the set time, the connection as well as the table it uses will be outdated.

For example, the user with the IP address 10.110.10.10 sets up an external TCP connection using port 2000, and NAT assigned corresponding address and port for it, but in a defined time, this TCP connection is not in use, the system will delete this connection.

Perform the following configuration in the system view.

Table 11-16 Configure address translation lifetime values

Operation	Command
Configure address translation lifetime values	**nat aging-time** { **default** | { **dns** | **ftp-ctrl** | **ftp-data** | **icmp** | **pptp** | **tcp** | **tcp-fin** | **tcp-syn** | **udp** } *seconds* }

If the **nat aging-time default** command is configured, the default address translation lifetime values of the system apply.

Following are the default address translation lifetime values for different protocols:

DNS: 60 seconds

FTP control link: 7200 seconds

FTP data link: 240 seconds

PPTP: 86400 seconds

TCP: 86400 seconds

TCP FIN (or RST)/SYN connection: 60 seconds

UDP: 300 seconds

ICMP: 60 seconds

11.3.11 Configuring Maximum Connections Limit

Table 11-17 Configure maximum connections limit

Operation	Command	Description
Enter system view	**system-view**	—
Create an ACL and enter its view	**acl number** *acl-number*	Required
Define ACL rules	**rule** [*rule-id*] { **permit** | **deny** | **comment** *text* } **source** [*sour-addr sour-wildcard* | **any**] [**time-range** *time-name*] [**logging**] [**fragment**] [**vpn-instance** *vpn-instance-name*]	Required
Exit ACL view	**quit**	—
Enable connection limit function	**connection-limit enable**	Required Disabled by default.
Set the action taken when no connection limit policy is available	**connection-limit default** { **permit** | **deny** }	Optional. By default, it is **deny**.
Set default value for connection limit threshold	**connection-limit default amount** { **upper-limit** *upper-limit* | **lower-limit** *lower-limit* }*	Optional. By default, set the upper limit to 50, and the lower limit to 20.
Create connection limit policy and enter its view	**connection-limit policy** *policy-number*	Required
Define rules for connection limit policy	**limit** *limit-id* **acl** *acl-number* [{ **per-source** | **per-destination** | **per-service** }* **amount** *upper-limit lower-limit*]	Required
Exit the connection limit policy view	**quit**	—
Specify the connection limit policy bound with NAT	**nat connection-limit-policy** *policy-number*	Required

11.3.12 Configuring Match Rule for Packets

You can use the following commands to change the match rule for packets in system view.

Table 11-18 Configure a match rule for packets

Operation	Command	Description
Enter system view	**system-view**	—
Configure the 3-tuple match rule for packets	**undo nat match factor-all**	Required
Configure the 5-tuple match rule for packets	**nat match factor-all**	Required

By default, the 5-tuple match rule is adopted for packets.

Note:

The 3-tuple match rule means that packet match is based on the protocol type, destination IP address, and destination port, and this rule applies only to UDP packets.

11.4 Displaying and Debugging NAT

After the above configuration, execute the **display** command in any view to display the running of the NAT configuration, and to verify the effect of the configuration.

Execute the **reset** command in user views to clear the running.

Execute the **debugging** command in user view for the debugging of NAT.

Table 11-19 Display and debug NAT

Operation	Command
Check NAT status	**display nat** { **address-group** | **aging-time** | **all** | **outbound** | **server** | **statistics** | **session** [**vpn-instance** *vpn-instance-name*] [**slot** *slot-number*] [**destination** *ip-addr*] [**source global** *global-addr* | **source inside** *inside-addr*] }
Display connection limit information	**display connection-limit statistics** [**source** *source-addr* { *source-wildcard* | *source-mask-len* }] [**destination** *destination-addr* { *destination-wildcard* | *destination-mask-len* }] [**destination-port** { { **eq** | **neq** | **gt** | **lt** } *destination-port* | **range** *destination-port1* *destination-port2* }] [**vpn-instance** *vpn-name*]
Display connection limit policy	**display connection-limit policy** { *policy-number* | **all** }

Operation	Command
Display NAT-related connection limit information	**display nat connection-limit** [**source** *source-addr* { *source-wildcard* **|** *source-mask-len* }] [**destination** *destination-addr* { *destination-wildcard* **|** *destination-mask-len* }] [**destination-port** { { **eq | neq | gt | lt** } *destination-port* **| range** *destination-port1 destination-port2* }] [**vpn-instance** *vpn-name*]
Display one or all server groups	**display nat server-group** [*group-name*]
Enable the debugging of NAT	**debugging nat** { **alg | event | packet** [**interface** { *interface-type interface-number*] }
Disable the debugging of NAT	**undo debugging nat** { **alg | event | packet** [**interface** *interface-type interface-number*] }
Enable connection limit debugging	**debugging connection-limit**
Disable connection limit debugging	**undo debugging connection-limit**
Clear NAT mapping table	**reset nat session**

11.5 NAT Configuration Example

11.5.1 Typical NAT Configuration

I. Network requirements

An enterprise is connected to WAN by the address translation function of router. It is required that the enterprise can access the Internet via serial 3/0/0 of the router, and provide www, ftp and smtp services to the outside, as well as two WWW servers. The internal network address of the enterprise is 10.110.0.0/16.

The internal ftp server address is 10.110.10.1. The internal www server1 address is 10.110.10.2. The internal www server 2 address is 10.110.10.3. The internal smtp server address is 10.110.10.4. It is expected to provide uniform server IP address to the outside. Internal network segment 10.110.10.0/24 may access Internet, but PC on other segments cannot access Internet. External PC may access internal server. The enterprise has six legal IP addresses from 202.38.160.100 to 202.38.160.105.

Choose 202.38.160.100 to be the external IP address of the enterprise, and www server2 uses 8080 port to the outside.

II. Network diagram

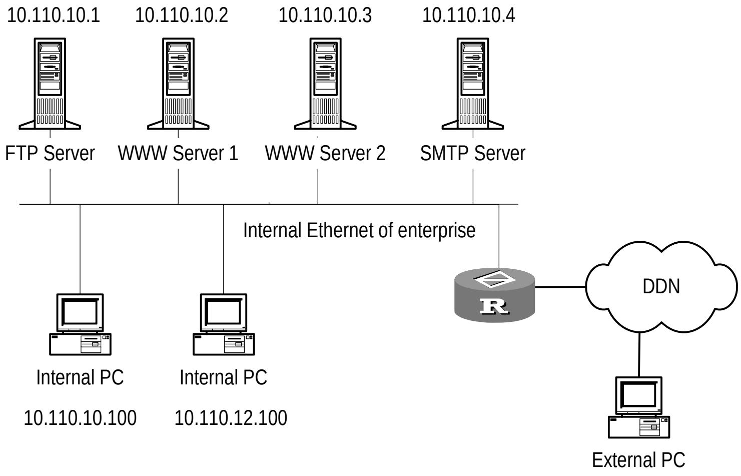


Figure 11-4 Network diagram for NAT configuration

III. Configuration procedure

# Configure address pool and access control list.

```
[Quidway] nat address-group 1 202.38.160.100 202.38.160.105
[Quidway] acl number 2001
[Quidway-acl-basic-2001] rule permit source 10.110.10.0 0.0.0.255
[Quidway-acl-basic-2001] rule deny source 10.110.0.0 0.0.255.255
[Quidway-acl-basic-2001] quit
```

# Allow address translation of segment at 10.110.10.0/24

```
[Quidway] interface serial 3/0/0
[Quidway-Serial3/0/0] nat outbound 2001 address-group 1
```

# Set internal ftp server

```
[Quidway-Serial3/0/0] nat server protocol tcp global 202.38.160.100 inside
10.110.10.1 ftp
```

# Set internal www server 1

```
[Quidway-Serial3/0/0] nat server protocol tcp global 202.38.160.100 inside
10.110.10.2 www
```

# Set internal www server 2

```
[Quidway-Serial3/0/0] nat server protocol tcp global 202.38.160.100 8080
inside 10.110.10.3 www
```

# Set internal smtp server

```
[Quidway-Serial3/0/0] nat server protocol tcp global 202.38.160.100 inside
10.110.10.4 smtp
```

11.5.2 Configuration Example of NAT Using IP Address of Loopback Interface

I. Network requirements

As shown in Figure 11-5, the intranet accesses the Internet through the serial interface 3/0/0 on the Quidway router; the internal network segment 10.110.10.0/24 can access the Internet, but other network segments cannot; the internet network segment uses the Loopback interface address 202.38.160.106 as the converted address. The intranet provides WWW, FTP and SMTP services to the outside, and the three servers use the same public address 202.38.160.100.

II. Network diagram

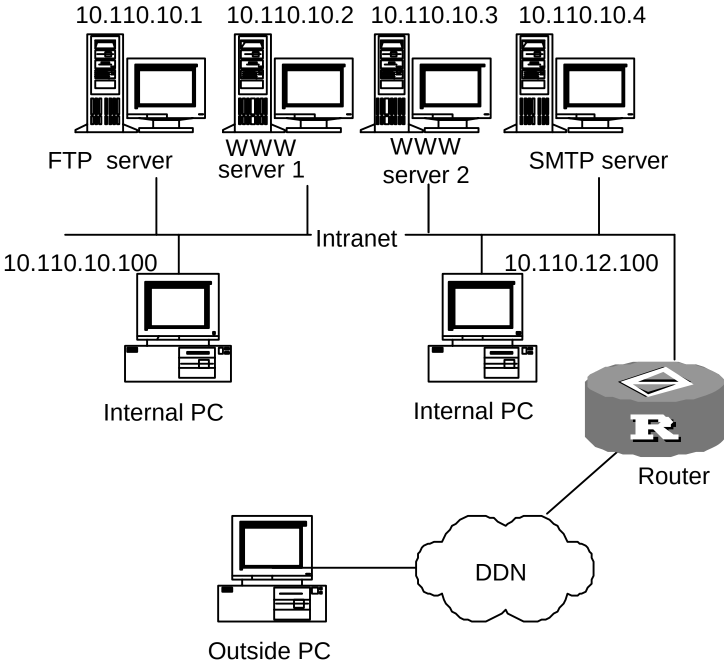


Figure 11-5 Configuration network diagram

III. Configuration procedure

# Configure an ACL.

```
[Quidway] acl number 2001
[Quidway-acl-basic-2001] rule permit source 10.110.10.0 0.0.0.255
[Quidway-acl-basic-2001] rule deny source 10.110.0.0 0.0.255.255
[Quidway-acl-basic-2001] quit
```

# Configure the loopback interface.

```
[Quidway] interface loopback 0
[Quidway-LoopBack0] ip address 202.38.160.106
[Quidway-LoopBack0] quit
```

# Configure the internal FTP server.

```
[Quidway] interface serial3/0/0
[Quidway-Serial3/0/0] nat server protocol tcp global 202.38.160.100 inside
10.110.10.1 ftp
```

# Configure the internal WWW server 1.

```
[Quidway-Serial3/0/0] nat server protocol tcp global 202.38.160.100 inside
10.110.10.2 www
```

# Configure the internal WWW server 2.

```
[Quidway-Serial3/0/0] nat server protocol tcp global 202.38.160.100 8080
inside 10.110.10.3 www
```

# Configure the internal SMTP server.

```
[Quidway-Serial3/0/0] nat server protocol tcp global 202.38.160.100 inside
10.110.10.4 smtp
```

# Associate the ACL with the loopback interface.

```
[Quidway-Serial3/0/0] nat outbound 2001 interface loopback 0
```

11.5.3 Static Net-to-Net NAT Configuration Example

I. Network requirements

As shown in the following diagram, two private networks, Network A and Network B, are connected to the Internet through Router A and Router B respectively. The addresses of both networks are 10.1.1.0/24.

On Network A,

- Router A provides access to the Internet through the WAN interface with IP address 201.1.1.1/24.
- The IP address of PC 1 is 10.1.1.2 and its public IP address on Router A is 211.2.1.2.

On Network B,

- Router B provides access to the Internet through the WAN interface with IP address 201.2.2.2/24.
- The IP address of PC 2 is 10.1.1.2, the same as that of PC 1 on Network A. The public IP address of PC 2 on Router B is 211.2.2.2.

To enable the two private networks to access the Internet and to enable PC 1 and PC 2 to access each other with their respective public addresses, do the following on Router A and Router B:

- On Router A create a static net-to-net NAT entry, translating network address 10.1.1.0/24 to 211.2.1.0/24; and configure dynamic routing, ensuring the route to 211.2.2.0/24 is reachable.

- Likewise, on Router B create a static net-to-net NAT entry, translating network address 10.1.1.0/24 to 211.2.2.0/24; and configure dynamic routing, ensuring the route to 211.2.1.0/24 is reachable.

II. Network diagram

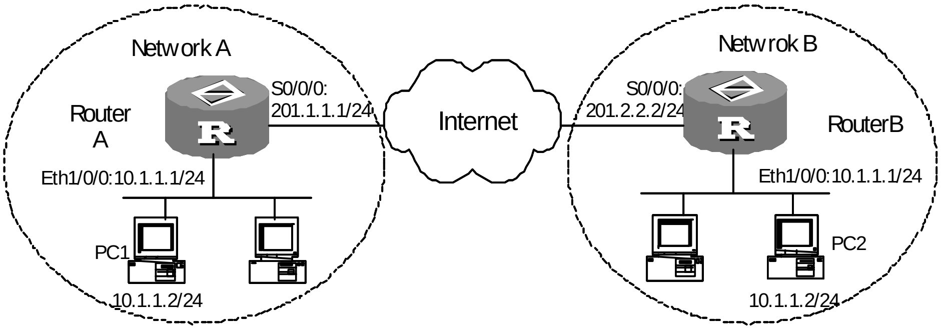


Figure 11-6 Network diagram for static net-to-net NAT

III. Configuration procedure

1) Configure Router A

# Create a static net-to-net NAT entry.

```
[Quidway]  nat  static  inside  ip  10.1.1.1  10.1.1.254  global  211.2.1.0
255.255.255.0
```

# Enable static net-to-net NAT on interface Serial0/0/0.

```
[Quidway] interface serial 0/0/0
[Quidway-Serial0/0/0] ip address 201.1.1.1 255.255.255.0
[Quidway-Serial0/0/0] nat outbound static
[Quidway-Serial0/0/0] quit
```

# Configure interface Ethernet1/0/0.

```
[Quidway] interface ethernet 1/0/0
[Quidway-Ethernet1/0/0] ip address 10.1.1.1 255.255.255.0
```

# Configure dynamic routing, ensuring the 211.2.2.0 network segment is reachable.

Omitted

2) Configure Router B

# Create a static net-to-net NAT entry.

```
[Quidway]  nat  static  inside  ip  10.1.1.1  10.1.1.255  global  211.2.2.0
255.255.255.0
```

# Enable static net-to-net NAT on interface Serial0/0/0.

```
[Quidway] interface serial 0/0/0
[Quidway-Serial0/0/0] ip address 201.2.2.2 255.255.255.0
```

```
[Quidway-Serial0/0/0] nat outbound static
[Quidway-Serial0/0/0] quit
```

# Configure interface Ethernet1/0/0.

```
[Quidway] interface ethernet 1/0/0
[Quidway-Ethernet1/0/0] ip address 10.1.1.1 255.255.255.0
```

# Configure dynamic routing, ensuring the 211.2.1.0 network segment is reachable.

Omitted

11.5.4 Bidirectional NAT Configuration Example

I. Network requirements

Figure 11-7 presents a scenario where:

- Two segments of an intranet, 10.0.0.0/24 and 10.1.1.0/24, are connected to Router A. They are merged into one network segment 10.0.0.0/24.
- A DNS server is located on network 192.168.0.0/24.
- On segment 10.0.0.0/24, PC 1 is assigned the IP address 10.0.0.1, the same as that of PC 3.

Configure Router A, the DNS server, and Router B to allow PC 1 and PC 2 to access PC 3 using domain name www.web.com or IP address 3.0.0.1/24.

II. Network diagram

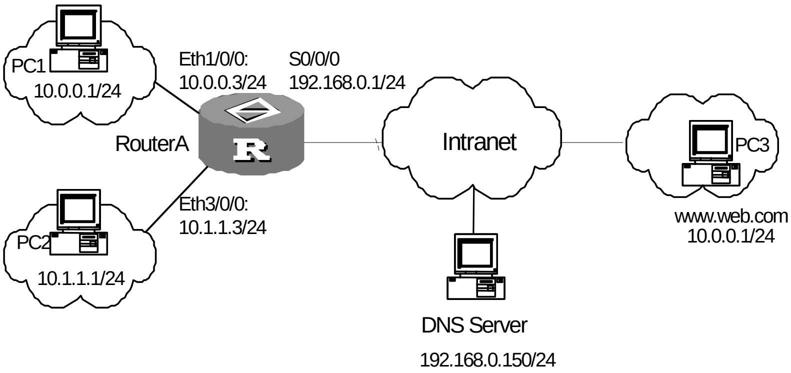


Figure 11-7 Network diagram for bidirectional NAT

III. Configuration procedure

Configure Router A

# Configure a NAT address pool.

```
[Quidway] nat address-group 1 2.0.0.1 2.0.0.200
```

# Create a bidirectional NAT entry.

```
[Quidway] nat overlapaddress 3 10.0.0.0 3.0.0.0 address-mask 24
```

# Configure an ACL.

```
[Quidway] acl number 2000
[Quidway-acl-basic-2000] rule 0 permit source 10.0.0.0 0.0.0.255
[Quidway-acl-basic-2000] rule 1 permit source 10.1.1.0 0.0.0.255
[Quidway-acl-basic-2000] quit
```

# On the WAN interface bind the address pool with the ACL.

```
[Quidway] interface serial 0/0/0
[Quidway-Serial0/0/0] ip address 192.168.0.1 255.255.255.0
[Quidway-Serial0/0/0] nat outbound 2000 address-group 1
```

# Assign IP addresses to LAN interfaces.

```
[Quidway-Serial0/0/0] interface ethernet 1/0/0
[Quidway-Ethernet1/0/0] ip address 10.0.0.3 255.255.255.0
[Quidway-Ethernet1/0/0] interface ethernet 3/0/0
[Quidway-Ethernet3/0/0] ip address 10.1.1.3 255.255.255.0
[Quidway-Ethernet3/0/0] quit
```

# Configure a static route.

```
[Quidway] ip route-static 3.0.0.0 255.255.255.0 serial 0/0/0
[Quidway] ip route-static 192.168.1.0 255.255.255.0 serial 0/0/0
The IP address of the DNS server is 192.168.0.150/24.
```

11.5.5 Internal Servers Combined with IPSec VPN

I. Network requirements

The headquarters of a company is connected to the public network through Router 1 and to the branches through IPSec VPNs established over the public network.

All traffic between the headquarters and its branches is protected using IPSec, where manually-established SAs, the security protocol of ESP, the encryption algorithm of DES, and the authentication algorithm of SHA1-HMAC-96 are adopted.

At the headquarters, the WWW and FTP servers are located on the 10.110.10.0 segment. Router 1 provides access to these two internal servers, allowing the internal users to access using private addresses and the external users to access using public addresses.

The PCs of the headquarters and branches are located on 10.110.20.0/24 and 10.110.30.0/24 respectively. They use the address translation service provided by Router 1, accessing the Internet with the public address of interface S1/0/0.

II. Network diagram

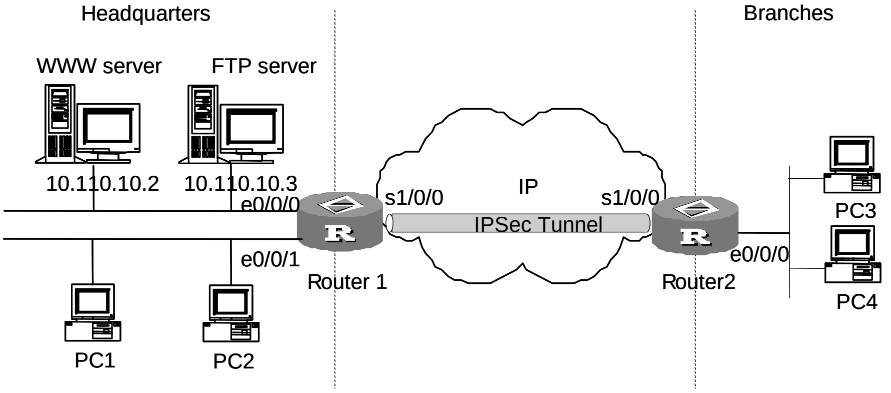


Figure 11-8 Internal servers combined with IPSec VPN

III. Configuration procedure

1) Configure Router 1

# Assign an IP address to interface Ethernet 0/0/0.

```
[Quidway] interface ethernet 0/0/0
[Quidway-ethernet 0/0/0] ip address 10.110.10.1 255.255.255.0
[Quidway-ethernet 0/0/0] interface ethernet 0/0/1
[Quidway-ethernet 0/0/1] ip address 10.110.20.1 255.255.255.0
```

# Configure an ACL to control address translation for PCs.

```
[Quidway] acl number 2001
[Quidway-acl-basic-2001] rule permit ip source 10.110.20.0 0.0.0.255
[Quidway-acl-basic-2001] rule permit ip source 10.110.30.0 0.0.0.255
[Quidway-acl-basic-2001] rule deny ip source any destination any
```

# Configure an ACL to control access to internal servers.

```
[Quidway-acl-basic-2001] acl number 2002
[Quidway-acl-basic-2002]  rule  permit  ip  source  10.110.10.0  0.0.0.255
[Quidway-acl-basic-2002]  rule  deny  ip  source  10.110.0.0  0.0.255.255
destination 10.110.30.0 0.0.0.255
[Quidway-acl-basic-2002] rule deny ip source any destination any
```

# Configure an ACL, implementing IPSec.

```
[Quidway-acl-basic-2002] acl number 2003
[Quidway-acl-basic-2003]  rule  permit  ip  source  10.110.0.0  0.0.255.255
destination 10.110.30.0 0.0.0.255
[Quidway-acl-adv-2003] rule deny ip source any destination any
[Quidway-acl-adv-2003] quit
```

# Configure Easy IP.

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

```
[Quidway-Serial1/0/0] ip address 202.38.160.1 255.255.255.0
[Quidway-Serial1/0/0] nat outbound 2001
```

# Configure the internal FTP and WWW servers.

```
[Quidway-Serial1/0/0] nat server 2002 protocol tcp global 202.38.160.1 inside
10.110.10.3 ftp
[Quidway-Serial1/0/0] nat server 2002 protocol tcp global 202.38.160.1 inside
10.110.10.2 www
[Quidway-Serial1/0/0] quit
```

# Configure IPSec.

```
[Quidway] ipsec proposal tran1
[Quidway-ipsec-proposal-tran1] encapsulation-mode tunnel
[Quidway-ipsec-proposal-tran1] transform esp
[Quidway-ipsec-proposal-tran1] esp encryption-algorithm des
[Quidway-ipsec-proposal-tran1] esp authentication-algorithm sha1
[Quidway-ipsec-proposal-tran1] quit
[Quidway] ipsec policy map1 10 manual
[Quidway-ipsec-policy-manual-map1-10] security acl 2003
[Quidway-ipsec-policy-manual-map1-10] proposal tran1
[Quidway-ipsec-policy-manual-map1-10] tunnel remote 202.38.162.1
[Quidway-ipsec-policy-manual-map1-10] tunnel local 202.38.160.1
[Quidway-ipsec-policy-manual-map1-10] sa spi outbound esp 12345
[Quidway-ipsec-policy-manual-map1-10] sa spi inbound esp 54321
[Quidway-ipsec-policy-manual-map1-10] sa string-key outbound esp abcdefg
[Quidway-ipsec-policy-manual-map1-10] sa string-key inbound esp gfedcba
[Quidway-ipsec-policy-manual-map1-10] quit
```

# Apply the IPSec policy group to interface serial 1/0/0.

```
[Quidway] interface serial 1/0/0
[Quidway-Serial1/0/0] ipsec policy map1
[Quidway-Serial1/0/0] quit
```

# Configure a static route to Router 2.

```
[Quidway] ip route-static 10.110.30.0 255.255.255.0 202.38.162.1
```

2) Configure Router 2

# Assign an IP address to interface Ethernet 0/0/0.

```
[Quidway] interface ethernet 0/0/0
[Quidway-ethernet 0/0/0] ip address 10.110.30.1 255.255.255.0
[Quidway-ethernet 0/0/0] quit
```

# Configure an ACL, implementing IPSec.

```
[Quidway] acl number 2003
```

```
[Quidway-acl-basic-2003]  rule  permit  ip  source  10.110.30.0  0.0.0.255
destination 10.110.0.0 0.0.255.255
[Quidway-acl-adv-2003] rule deny ip source any destination any
[Quidway-acl-adv-2003] quit
```

# Configure IPSec.

```
[Quidway] ipsec proposal tran1
[Quidway-ipsec-proposal-tran1] encapsulation-mode tunnel
[Quidway-ipsec-proposal-tran1] transform esp
[Quidway-ipsec-proposal-tran1] esp encryption-algorithm des
[Quidway-ipsec-proposal-tran1] esp authentication-algorithm sha1
[Quidway-ipsec-proposal-tran1] quit
[Quidway] ipsec policy use1 10 manual
[Quidway-ipsec-policyl-manual-use1-10] security acl 2003
[Quidway-ipsec-policyl-manual-use1-10] proposal tran1
[Quidway-ipsec-policyl-manual-use1-10] tunnel remote 202.38.160.1
[Quidway-ipsec-policyl-manual-use1-10] tunnel local 202.38.162.1
[Quidway-ipsec-policyl-manual-use1-10] sa spi outbound esp 54321
[Quidway-ipsec-policyl-manual-use1-10] sa spi inbound esp 12345
[Quidway-ipsec-policyl-manual-use1-10] sa string-key outbound esp gfedcba
[Quidway-ipsec-policyl-manual-use1-10] sa string-key inbound esp abcdefg
[Quidway-ipsec-policyl-manual-use1-10] quit
```

# Assign an IP address to interface serial 1/0/0 and apply the IPSec policy group on the interface.

```
[Quidway] interface serial 1/0/0
[Quidway-Serial1/0/0] ip address 202.38.162.1 255.0.0.0
[Quidway-Serial1/0/0] ipsec policy use1
[Quidway-Serial1/0/0] quit
```

# Configure a static route to Router 1.

```
[Quidway] ip route-static 10.110.0.0 255.255.0.0 202.38.160.1
```

11.5.6 Domain Name-Related NAT Configuration Example

I. Network requirements

Figure 11-9 presents a scenario where:

- On intranet 10.0.0.0/8 deployed an FTP server and a WWW server.
- The domain name is ftp.zc.com for the FTP server and www.zc.com for the WWW server. The two names can be correctly resolved by external DNS servers.
- The router uses interface Serial0/0/0 to provide access to the external network. The IP address of the serial interface is 1.1.1.1/8.

Configure NAT entries for domain names to allow internal hosts to identify and access the internal servers correctly by domain name.

II. Network diagram

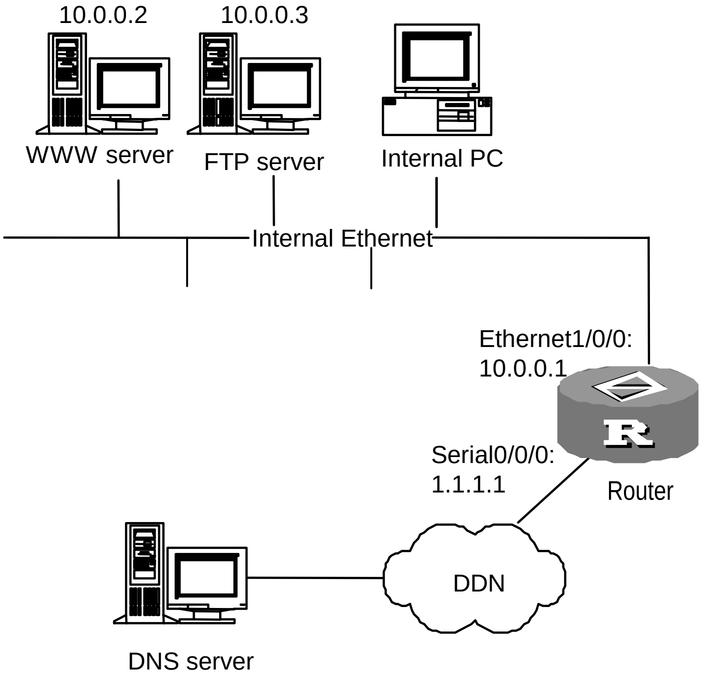


Figure 11-9 Network diagram for domain name-related NAT

III. Configuration procedure

# Configure internal FTP and WWW servers on interface Serial0/0/0.

```
[Quidway] interface serial 0/0/0
[Quidway-Serial0/0/0] ip address 1.1.1.1 255.0.0.0
[Quidway-Serial0/0/0] nat outbound 2000
[Quidway-Serial0/0/0] nat server protocol tcp global 1.1.1.1 www inside
10.0.0.2 www
[Quidway-Serial0/0/0] nat server protocol tcp global 1.1.1.1 ftp inside
10.0.0.3 ftp
[Quidway-Serial0/0/0] quit
```

# Configure an ACL, permitting the 10.0.0.0/8 segment to access the Internet.

```
[Quidway] acl number 2000
[Quidway-acl-basic-2000] rule 0 permit source 10.0.0.0 0.0.0.255
[Quidway-acl-basic-2000] rule 1 deny
```

# Configure interface Ethernet1/0/0.

```
[Quidway] interface ethernet 1/0/0
[Quidway-Ethernet1/0/0] ip address 10.0.0.1 255.0.0.0
```

After you complete the above configuration tasks, the outside hosts can access the two internal servers by domain name. To allow the internal hosts to access the internal servers by domain name, do the following in addition:

# Map the domain names each to a triplet of external address, port number, and protocol type.

```
[Quidway] nat dns-map www.zc.com 1.1.1.1 80 tcp
[Quidway] nat dns-map ftp.zc.com 1.1.1.1 21 tcp
```

11.5.7 Configuration Example for NAT Limit on Maximum Connections

I. Network requirements

As shown in Figure 11-10, the interface Ethernet0/0/0 of Router is connected to the LAN 192.168.1.0/24 and the interface Serial1/0/1 is connected to the Internet. On Router, NAT is configured to enable the PCs in the LAN to access the Internet.

To limit the connections initiated by the host in the LAN, the router is configured with the feature of NAT limit on maximum connections, in order to limit the number of connections initiated towards a single source address. The upper limit is 10 and the lower limit is 1.

II. Network diagram

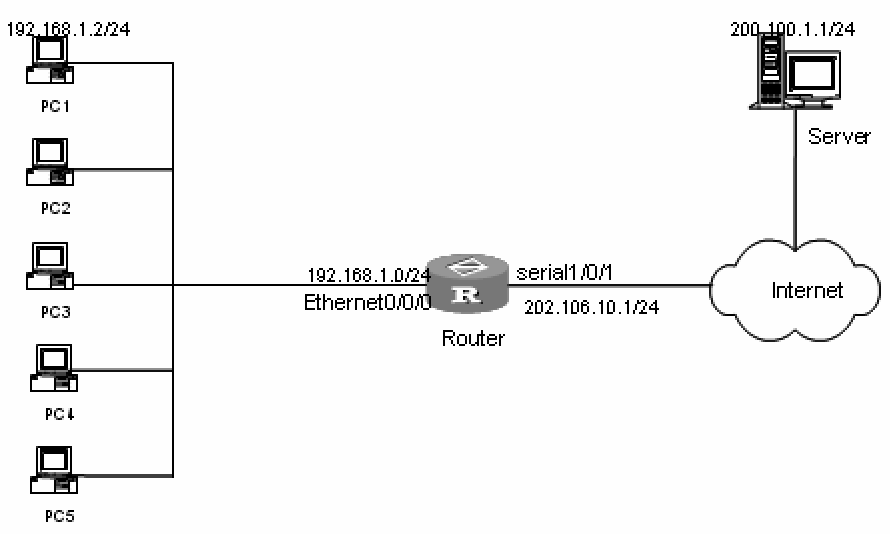


Figure 11-10 Network diagram for NAT limit on maximum connections

III. Configuration procedure

# Configure NAT on Router.

Omitted.

# Create ACL and configure ACL rules to match the data transmitted from the IP address 192.168.1.2/24.

```
<Quidway> system-view
[Quidway] acl number 2000
[Quidway-acl-basic-2000] rule 0 permit source 192.168.1.2 0
[Quidway-acl-basic-2000] quit
```

# Create connection limit policy and relevant rules to limit the connections initiated by the single source address.

```
[Quidway] connection-limit enable
[Quidway] connection-limit policy 0
[Quidway-connection-limit-policy-0] limit 0 acl 2000 per-source amount 10 1
[Quidway-connection-limit-policy-0] quit
```

# NAT references the connection limit policy 0.

```
[Quidway] nat connection-limit-policy 0
```

11.5.8 Configuration Example for Load Balancing among NAT Servers

I. Network requirements

The internal network of a server provider is the subnet 10.0.0.0/24 and provides WWW services.

There are three WWW servers with the same processing capability in the internal network.

The IP address of the interface Ethernet 0/0/0 connecting external networks is 200.0.0.2/24.

It is required that external accesses should be evenly distributed to the three WWW servers.

II. Network diagram

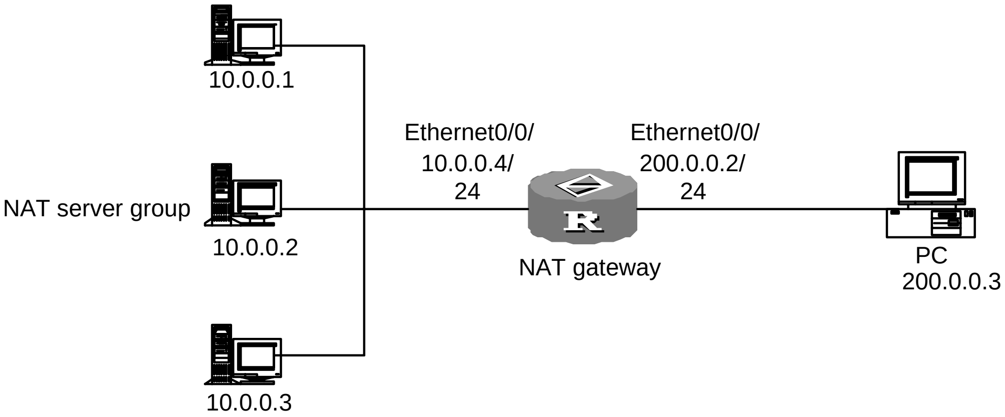


Figure 11-11 Network diagram for load balancing among NAT servers

III. Configuration procedure

# Create a NAT server group named www on the NAT device.

```
<Quidway> system-view
[Quidway] nat server-group www
```

# Add internal to the NAT server group (www_group).

```
[Quidway-nat-server-group-www] inside ip 10.0.0.1 port 80 weight 1
[Quidway-nat-server-group-www] inside ip 10.0.0.2 port 80 weight 1
[Quidway-nat-server-group-www] inside ip 10.0.0.3 port 80 weight 1
[Quidway-nat-server-group-www] quit
```

# Reference the NAT server group (www_group) on the interface ethernet 0/0/0.

```
[Quidway] interface ethernet 0/0/0
[Quidway-Ethernet0/0/0] nat server protocol tcp global 200.0.0.2 www inside
server-group www
```

11.6 Troubleshooting NAT Configuration

Fault 1: address translation abnormal

Troubleshooting: enable the debug for NAT, and refer to **debugging nat** in the **debugging** command for specific operation. According to the Debugging information displayed on the router, initially locate the failure, and then use other commands for further check. Observe the source address after translation carefully, and make sure that it is the expected address. Otherwise, it is possible the configuration of address pool is wrong. Meanwhile, make sure that there is route in the accessed network to return to the address segment defined in the address pool. Take into consideration the influence onto the NAT by the ACL of firewall and address conversion itself, and also route configuration.

Fault 2: internal server abnormal

Troubleshooting: if an external host can not access the internal server normally, check the configuration on the internal server host, or the internal server configuration on the router. It is possible that the internal server IP address is wrong, or that the firewall has inhibited the external host to access the internal network. Use the command **display acl** for further check. Refer to the firewall configuration.

Chapter 12 IP Unicast Policy Routing Configuration

12.1 IP Unicast Policy Routing Overview

IP policy routing is a mechanism in which packets are transmitted and forwarded by strategy without going through the routing table. It is a more flexible routing mechanism, compared with routing according to the destination address of data packet.

When a router is forwarding a packet, it is filtered via a **route-policy** first, deciding which packets to be forwarded and the next hop.

Policy routing is configured by the user. It is composed of a group of **if-match** clauses and a group of **apply** clauses. When some packets fully satisfy the **if-match** clauses of strategy, the **apply** clauses in the strategy are executed in a certain sequence, to complete the packet forwarding.

Route-policies are used for policy routing. One route-policy may contain multiple nodes, each consisting of multiple if-match and apply clauses.

The if-match clauses of a route-policy node define the match rules whereas its apply clauses define the actions performed on the packets filtered in by the node.

For a route-policy node, the relationship between its if-match clauses is AND for packet filtering, meaning a packet is permitted by the node only when it matches all if-match clauses.

At present, two **if-match** clauses i.e. **if-match packet-length** and **if-match acl** are provided.

The **apply** clause defines the operation of the policy. At present, there are seven **apply** clauses: **apply ip-precedence**, **apply ip-dscp**, **apply output-interface**, **apply ip-address next-hop**, **apply default output-interface**, **apply ip-address default next-hop** and **apply ip-df**. When all the if-match clauses are satisfied, the operation defined by the apply clauses are as follows:

- Configuring the DSCP value: **apply ip-dscp**. Once configured, this clause will be executed.
- Configuring the priority: **apply ip-precedence**. The precedence is just below that of the **apply ip-dscp** clause.
- Configuring the outbound interface and next hop: **apply output-interface** and **apply ip-address next-hop**, where the **apply output-interface** clause has a higher priority than the **apply ip-address next-hop** clause. When both of them

are configured and valid, the system executes only the **apply output-interface** clause.

- Configuring the default outbound interface and next hop: **apply default output-interface** and **apply ip-address default next-hop**. The **apply default output-interface** clause has a higher priority than the **apply ip-address default next-hop** clause. When both of them are configured and valid, the system executes only the **apply default output-interface** clause. Note that these two clauses are executed only when no outbound interface and next hop are configured for policy routing or the configured outbound interface and next hop are invalid, and no corresponding route is found in the routing table.

There are two kinds of policy routings: interface policy routing and local policy routing. The former is configured in interface view and performs strategic routing for packets coming through this interface, while the latter is configured in global view and performs policy routing for packets generated by this router. Generally, for the request about forwarding and security, in most cases, interface policy route will be used.

The policy routing can be used for security and load sharing.

12.2 IP Unicast Policy Routing Configuration

IP unicast policy routing configuration includes:

1) Configure a route-policy

- Establish a Route-policy
- Define match clause of policy routing
- Define apply clause of policy routing

2) Enable policy routing

- Enable/disable local policy routing
- Enable/disable policy routing on the interface

12.2.1 Configuring a Route-Policy

I. Creating a route-policy

Each route-policy comprises multiple policy nodes, each assigned a sequence number. The smaller the sequence number, the higher the priority. The policy with the highest priority is executed first.

A route-policy is made up of if-match and apply statements and can be used for route redistribution or policy routing.

Perform the following task in system view.

Table 12-1 Establish a route-policy

Operation	Command
Establish a route-policy or a policy node	**route-policy** *policy-name* { **permit** | **deny** } **node** *sequence-number*
Delete a route-policy or a policy node	**undo route-policy** *policy-name* [**permit** | **deny** | **node** *sequence-number*]

permit means applying policy routing for the packets meeting the conditions, and **deny** means not applying policy routing for the packets meeting the conditions.

By default, no route-policy and the related node configuration is defined.

II. Defining if-match clauses for the route-policy

The if-match clauses are used for matching packets on which policy routing is to be performed. IP unicast policy routing provides two if-match clauses, **if-match packet-length** clause and **if-match acl** clause. When both of them are configured, their relationship is AND.

Perform the following task in route-policy view.

Table 12-2 Define if-match clause of policy routing

Operation	Command
Specify an IP packet length if-match clause	**if-match packet-length** *min-len max-len*
Specify an ACL matching if-match clause	**if-match acl** *acl-number*

By default, no if-match clause is defined.

III. Defining the apply clauses of the route-policy

IP unicast policy routing provides seven types of apply clauses: **apply ip-precedence**, **apply ip-dscp, apply output-interface**, **apply ip-address next-hop**, **apply default output-interface**, **apply ip-address default next-hop** and **apply ip-df**. One route-policy node may have multiple apply clauses. These clauses are executed in the order in which they are configured until a valid apply clause is executed.

Perform the following task in route-policy view.

Table 12-3 Define apply clause of policy routing

Operation	Command
Set packet precedence	**apply ip-precedence** *precedence*

Operation	Command
Set packet DSCP value	**apply ip-dscp** { *value* | **af11** | **af12** | **af13** | **af21** | **af22** | **af23** | **af31** | **af32** | **af33** | **af41** | **af42** | **af43** | **be** | **cs1** | **cs2** | **cs3** | **cs4** | **cs5** | **cs6** | **cs7** | **ef** }
Set packet transmitting interface	**apply output-interface** { *interface-type interface-number* | *interface-name* } [**detect-group** *group-number*] [{ *interface-type interface-number* | *interface-name* } [**detect-group** *group-number*]
Set packet next-hop	**apply ip-address next-hop** [**detect-group** *group-number*] [*ip-address* [**detect-group** *group-number*]]
Set packet default transmitting interface	**apply default output-interface** { *interface-type interface-number* | *interface-name* } [**detect-group** *group-number*] [{ *interface-type interface-number* | *interface-name* } [**detect-group** *group-number*]]
Set packet default next-hop	**apply ip-address default next-hop** *ip-address* [**detect-group** *group-number*] [*ip-address* [**detect-group** *group-number*]]
Set the DF bit in packets	**apply ip-df** *df-value*

The user can specify multiple next hops or set several outbound interfaces. In this case, the forwarding of packets will be shared among multiple parameters, namely, each packet is sent on each next hop or outbound interface in turn. This is only applicable to multiple parameters configured of one kind. If the outbound interfaces and next hops are both configured, only the outbound interface is set to perform the load sharing.

By default, no apply clause is defined.

Note:

When you configure the apply clause of the policy routing, for a point to point interface (Serial interface encapsulated with PPP protocol, for example) you can configure the packet sending interface and the next hop as well; for a broadcast or NBMA interface (Ethernet and ATM interface, for example) you must set the address of the next hop of the packet.

12.2.2 Enabling Policy Routing

I. Enabling or Disabling Local Policy Routing

Enable or disable local policy routing in the system view. Only one local policy can be enabled.

Table 12-4 Enable/disable local policy routing

Operation	Command
Enable local policy routing	**ip local policy route-policy** *policy-name*
Disable local policy routing	**undo ip local policy route-policy** *policy-name*

By default, local policy routing is disabled.

II. Enabling or Disabling Policy Routing on the Interface

Enable or disable policy routing on a specified interface. At most one policy can be referenced on each interface.

Perform the following configuration in interface view.

Table 12-5 Enable/disable policy routing on the interface

Operation	Command
Enable policy routing on the interface	**ip policy route-policy** *policy-name*
Disable policy routing on the interface	**undo ip policy route-policy** *policy-name*

By default, policy routing is disabled on the interface.

12.3 Displaying and Debugging IP Unicast Policy Routing

After the above configuration, execute the **display** command in any view to display the running of the IP Unicast Policy Routing configuration, and to verify the effect of the configuration.

Execute the **debugging** command in user view for the debugging of IP Unicast Policy Routing.

Table 12-6 Display and debug IP unicast policy routing

Operation	Command
Show local policy routing and interface policy routing	**display ip policy**
Show the setting of the local policy routing	**display ip policy setup local**
Show the setting of the interface policy routing	**display ip policy setup interface** *interface-type interface-number*
Show the packet statistics of the local policy routing	**display ip policy statistic local**
Show the packet statistics of the interface policy routing	**display ip policy statistic interface** *interface-type interface-number*

Operation	Command
Display configuration information of a routing policy	**display route-policy** [*policy-name*]
enable the debugging of the policy routing	**debugging ip policy**

12.4 Typical Configuration of IP Unicast Policy Routing

12.4.1 Configuring Policy Routing Based on Source Address

I. Configuration requirements

Enable a policy routing named aaa, which controls all TCP packets received from Ethernet3/0/0 to be sent via the interface of serial1/0/0, whereas other packets to be forwarded based on routing table.

Node 5 denotes that Ethernet packets matched with **acl 3101** will be sent to serial1/0/0.

Node 10 denotes that any packets matched with **acl 3102** will not be processed by policy routing.

The packets from Ethernet 3/0/0 will try to match the if-match clauses of nodes 5 and 10 in turn. If nodes in **permit** mode are matched, execute corresponding apply clauses. If nodes in **deny** mode are matched, exit from policy routing.

II. Network diagram

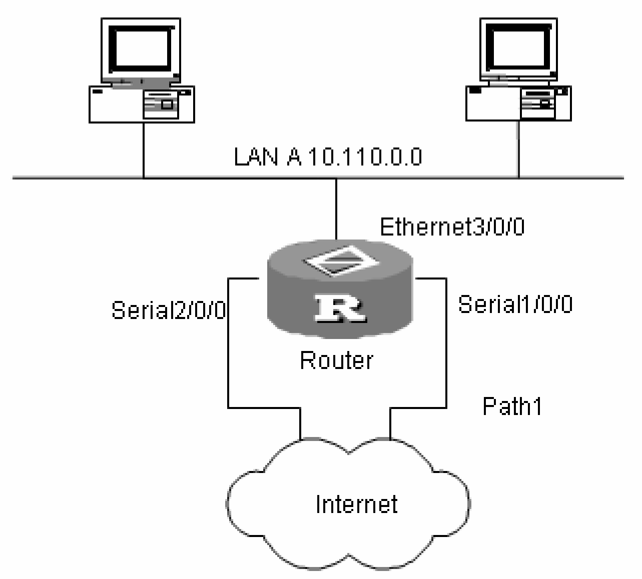


Figure 12-1 Network diagram for configuring policy routing based on source address

III. Configure procedure

# Set the default filtering method of firewall to deny.

```
[Quidway] firewall default deny
```

# Define access control list:

```
[Quidway] acl number 3101
[Quidway-acl-adv-3101] rule permit tcp
[Quidway-acl-adv-3101] quit
[Quidway] acl number 3102
[Quidway-acl-adv-3102] rule permit ip
[Quidway-acl-adv-3102] quit
```

# Define acl 5 node to make any TCP packet matching ACL 3101 be sent to serial interface serial 1/0/0.

```
[Quidway] route-policy aaa permit node 5
[Quidway-route-policy] if-match acl 3101
[Quidway-route-policy] apply output-interface serial 1/0/0
[Quidway-route-policy] quit
```

# Define acl 10 node not to apply the policy routing to the packet matching ACL 3102.

```
[Quidway] route-policy aaa deny node 10
[Quidway-route-policy] if-match acl 3102
[Quidway-route-policy] quit
```

# Apply policy aaa on the Ethernet interface

```
[Quidway] interface ethernet 3/0/0
[Quidway-Ethernet3/0/0] ip policy route-policy aaa
```

12.4.2 Configuring Policy Routing Based on Packet Size

I. Configuration requirement

Router A sends the packets of 64 to 100 bytes long through serial 2/0/0, packets of 101 to 1000 bytes long through serial 2/0/1 and those of other size should be routed normally.

Apply IP unicast policy routing lab1 on E1/2/0 of Router A. This strategy will set packet of 64 to 100 bytes long to 150.1.1.2 as the IP address of next hop and set packet of 101 to 1000 bytes long to 151.1.1.2 as the IP address of next hop. All packets of other size should be routed in the method based on the destination address

II. Network diagram

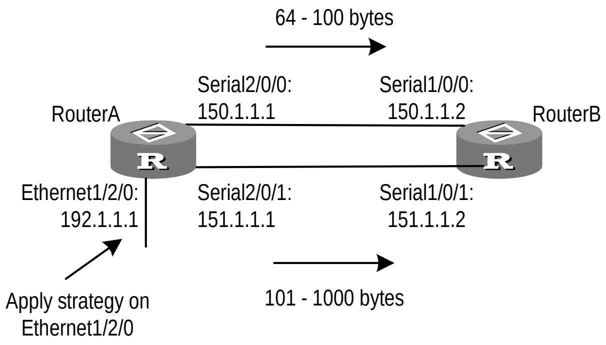


Figure 12-2 Network diagram for configuring policy routing based on packet size

III. Configure procedure

# Configure Router A:

```
[Quidway] interface ethernet 1/2/0
[Quidway-Ethernet 1/2/0] ip address 192.1.1.1 255.255.255.0
[Quidway-Ethernet 1/2/0] ip policy route-policy lab1
[Quidway] interface serial 2/0/0
[Quidway-Serial2/0/0] ip address 150.1.1.1 255.255.255.0
[Quidway] interface serial 2/0/1
[Quidway-Serial2/0/1] ip address 151.1.1.1 255.255.255.0
[Quidway] rip
[Quidway-rip] network 192.1.1.0
[Quidway-rip] network 150.1.0.0
[Quidway-rip] network 151.1.0.0
[Quidway] route-policy lab1 permit node 10
[Quidway-route-policy] if-match packet-length 64 100
[Quidway-route-policy] apply ip-address next-hop 150.1.1.2
[Quidway] route-policy lab1 permit node 20
[Quidway-route-policy] if-match packet-length 101 1000
[Quidway-route-policy] apply ip-address next-hop 151.1.1.2
```

# Configure Router B:

```
[Quidway] interface serial 1/0/0
[Quidway-Serial1/0/0] ip address 150.1.1.2 255.255.255.0
[Quidway] interface serial 1/0/1
[Quidway-Serial1/0/1] ip address 151.1.1.2 255.255.255.0
[Quidway] rip
[Quidway-rip] network 150.1.0.0
[Quidway-rip] network 151.1.0.0
```

Use the **debugging ip policy** command to monitor policy routing on Router A. Note: the packets of 64 bytes long match the entry item whose id number is 10 as shown in the route policy lab1, therefore they are forwarded to 150.1.1.2.

```
<Quidway> debugging ip policy
*0.483448-POLICY-8-POLICY-ROUTING:IP Policy routing success : next-hop :
150.1.1.2
```

On Router A, change the packet size to 101 bytes and monitor policy routing with the **debugging ip policy** command. Note: the packets of 101 bytes match the entry item whose serial number is 20 as shown in the route policy lab1. They are forwarded to 151.1.1.2.

```
<Quidway> debugging ip policy
*0.483448-POLICY-8-POLICY-ROUTING:IP Policy routing success : next-hop :
151.1.1.2
```

On Router A, change the packet size to 1001 bytes, and then use the **debugging ip policy** command to monitor policy routing. Note that this packet does not match any entry item in lab1, so it is forwarded in regular mode. The policy routing debugging does not output information of the forwarding packets.

Chapter 13 IP Multicast Policy Routing Configuration

13.1 Introduction to IP Multicast Policy Routing

13.1.1 Overview of IP Multicast Policy Routing

IP multicast policy routing is subsidiary and enhancement to the function that multicast forwards packets according to the routing table. It forwards multicast packets according to the policy the user specifies.

IP multicast policy routing is implemented by configuring the route-policy. The route-policy is an extension of unicast policy routing, described by a group of **if-match** and **apply** statements the user defines. The **if-match** clause defines the match rule, i.e., the filter conditions to be met to pass the current route-policy. It specifies when a multicast packet meets the match conditions the user defines, the multicast packet is not forwarded according to the usual process, but forwarded according to the action the user sets (described by the **apply** statement).

13.1.2 Concepts Related to IP Multicast Policy Routing

- route-policy

IP multicast policy routing is implemented through route-policies. Multiple route-policies can be configured on a router.

- Policy node

A policy node is a complete policy, which sets the conditions packets should match with the **if-match** command and sets the forwarding actions that should be executed to packets meeting the match conditions with the **apply** command. Each node contains at most one ACL used for defining the match conditions of packets, one ACL used for specifying the outgoing interface and one ACL used for specifying the next hop.

Multiple nodes with different conditions and actions can be configured in a route-policy. Different policy-nodes in each route-policy can be identified through an integer sequence-number.

- Match rule

Match conditions of multicast packets are described by the **if-match** clause and are set by configuring the standard or extended ACL (ranging from 2000 to 3999).

- Forwarding actions of multicast packets

Forwarding actions of multicast packets are described by the APPLY clause including setting the outgoing interface and the next hop IP address. The output interface list is specified through an interface-based ACL (ranging from 1000 to 1999). The next hop IP address list is specified through a standard ACL (ranging from 2000 to 2999).

13.1.3 Packet Forwarding Process after the IP Multicast Policy Routing is Applied

For a multicast packet, if IP multicast policy routing is configured on the incoming interface and the packet meets the match conditions of IP multicast policy routing, the packet will be forwarded according to the actions set by the policy routing. Otherwise, the packet will be forwarded according to the usual forwarding process.

13.2 Configuring IP Multicast Policy Routing

IP Multicast Policy Routing Configuration includes:

- Define a route-policy
- Define the if-match clause for IP multicast routing policy
- Define the apply clause of the route-policy
- Enable IP multicast policy routing on an interface

13.2.1 Defining a Route-Policy

Multiple policy-nodes with different conditions and actions can be configured in a route-policy. Each policy-node has its own **if-match** clauses and **apply** clauses. Their match order is specified by *sequence-number*.

Perform the following configurations in system view.

Table 13-1 Define a route-policy

Operation	Command
Define a policy-node of the route-policy	**route-policy** *policy-name* { **permit** | **deny** } **node** *sequence-number*
Remove a policy-node of the route-policy	**undo route-policy** *policy-name* [**permit** | **deny**]

When IP multicast policy routing is configured on an interface of a router, all multicast data packets that enter the router from this interface will be filtered. The filtering method is that all policy-nodes of the route-policy specified by the policy routing are processed in order of the *sequence-number* from small to large.

Note that the relationship among all parts of different *sequence-numbers* is “or”, that is, the packet pass by every node of different *sequence-number* in sequence. If packet can match if-match clause of one node, the packet will be forwarded by the apply clause of the node and not reach all the following nodes.

13.2.2 Defining the if-match Clause of the Route-Policy

An **if-match** clause defines the match rule, which is the filtering condition that should be met by the packets to pass the current route-policy.

Perform the following configurations in route-policy view.

Table 13-2 Define match conditions

Operation	Command
Set conditions that multicast packets should meet	**if-match acl** *acl-number*
Remove the match conditions set	**undo if-match acl**

If a packet meets the if-match conditions specified in a policy-node, actions specified by the node will be performed. If a packet does not meet the if-match conditions specified in a policy-node, the next node will be detected. If a packet does not meet the conditions of all route-nodes, the packet will return to the normal forwarding flow.

The following points should be noted:

- For a node of a route-policy, the relationship among all **if-match** clauses in the same node is “and” during matching.
- Multicast policy routing only considers the **if-match acl** configuration in a policy-node. Any other **if-match** clause does not concern forwarding of multicast policy routing.
- If no **if-match** clause is specified, all routing information will pass the filtering of the node.

13.2.3 Defining Apply Clauses for a Route-Policy

The **apply** clauses specify actions, that is, some configuration commands executed after the filter conditions specified by the **if-match** clauses have been met.

Perform the following configurations in route-policy view.

Table 13-3 Define **apply** clauses

Operation	Command
Configure an outgoing interface list in a policy-node	**apply output-interface acl** *acl-number*
Remove the outgoing interface list configured	**undo apply output-interface** [**acl** *acl-number*]
Configure the next hop IP address list in a policy-node	**apply ip-address next-hop** { **acl** *acl-number* | *ip-address* [*ip-address*] }

Operation	Command
Remove the next hop address list configured	**undo apply ip-address next-hop** [**acl** *acl-number* | *ip-address* [*ip-address*]]

Use the ACL to specify the output interface list and the next hop IP address list for IP multicast policy routing. The basic ACL (ranging from 2000 to 2999) is specified for the next hop IP address. The interface-based ACL (ranging from 1000 to 1999) is specified for the output interface list.

13.2.4 Enabling IP Multicast Policy Routing on an Interface

Perform the following configurations in interface view.

Table 13-4 Enable IP multicast policy routing on an interface

Operation	Command
Enable an IP multicast policy routing on an interface	**ip multicast-policy route-policy** *policy-name*
Remove an IP multicast policy routing on an interface	**undo ip multicast-policy route-policy** *policy-name*

When IP multicast policy routing is configured on an interface of a router, all multicast packets (excluding multicast protocol packets such as packets generated by multicast routing protocols) entering the router on the interface will be filtered.

The filter method is as follows: All policy nodes of the route-policy specified by the policy routing are filtered in order of sequence number from small to large. If a packet meets the if-match conditions specified in a policy-node, actions specified by the node will be executed. If a packet does not meet the if-match conditions specified in a policy-node, the next node will be detected. If a packet does not meet the conditions of any policy nodes, the packet will return to the normal forwarding process.

13.3 Displaying and Debugging IP Multicast Policy Routing

After the above configuration, execute **display** command in any view to display the running of IP Multicast Policy Routing configuration, and to verify the effect of the configuration.

Execute the **debugging** command in user view for the debugging of IP Multicast Policy Routing.

Table 13-5 Display and debug IP multicast policy routing

Operation	Command
Display the multicast policy routing information	**display ip multicast-policy** [**setup interface** *interface-type interface-num* **|** **statistic interface** *interface-type interface-num*]
Enable the IP multicast policy routing debugging	**debugging ip multicast-policy** [*acl-number*]
Disable the IP multicast policy routing debugging	**undo debugging ip multicast-policy**

Chapter 14 QLLC Configuration

14.1 QLLC Configuration

14.1.1 Introduction to QLLC

Qualified logical link control (QLLC) is a protocol for transmitting SDLC over an X25 networks by encapsulating . Therefore, QLLC is “SDLC over X25” which encapsulating the SDLC frames in X.25 frames for transmission.

QLLC enables an SNA device to communicate with a remote SNA device through across an X25 network. SNA is an architecture proposed by IBM and corresponds to the TCP/IP system of ISO. The link layer of SNA defines some link layer protocols , such as LLC2, SDLC and QLLC.

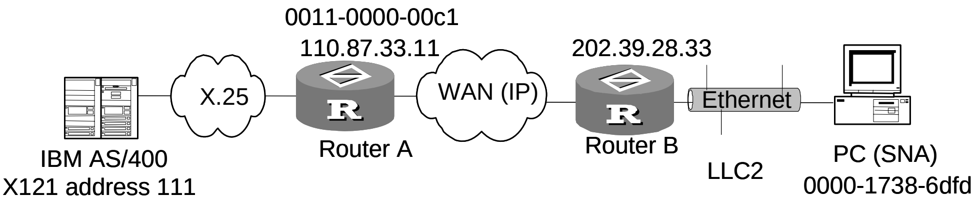


Figure 14-1 Network diagram for QLLC

As shown in Figure 14-1, QLLC is functioning at the link layer to exchange SNA negotiation packets between UNIX and IBM hosts. After SNA negotiation is completed, the packets exchanged between the UNIX host and Router A are X.25 packets.

14.1.2 Configuring QLLC

Configuring QLLC is to configure QLLC switching map on the router, with each map entry comprising remote X.121 address, virtual MAC address of the local interface, and MAC address of the remote SNA device.

When the router receives an SNA negotiation request from the peer, it looks up the switching map based on virtual MAC address for a match. If a match is found, the router initiates an X.25 call based on the matched X.121 address. If the call succeeds, SNA negotiation is started.

When the router receives a call from the X.25 network, it looks up the switching map based on X.121 address of the call for a match. If a match is found, the router establishes an X.25 virtual circuit and starts SNA negotiation using the matched remote MAC address.

Virtual MAC address discussed here is the address where the router is functioning as a virtual SNA device. It is the address that the router uses in SNA negotiation.

🕮 **Note:**

Each synchronous interface can have only one QLLC link, meaning you can configure only one switching map entry for a physical interface.

Normally, QLLC adopts client/server model where the SNA device is acting as the client to originate negotiation and the X.25 host is acting as the server. Therefore, on the router that provides QLLC switching, you need not to configure the X.121 to remote MAC address map but the X.121 to virtual MAC address map.

You must configure the X.121 to remote MAC address map however to handle the situation where the server is allowed to initiate X.25 call requests.

Perform the following configuration in synchronous interface view.

Table 14-1 Create a QLLC switching map entry

Operation	Command
Create a QLLC switching map entry	**X25 qllc-switch** *x.121-address* **virtual-mac** *mac-address* [**partner-mac** *mac-address*]
Delete a QLLC switching map entry	**X25 qllc-switch** *x.121-address*

By default, no switching map entry exists.

14.1.3 Displaying and Debugging QLLC

Perform the following configuration in user view.

Table 14-2 Enable QLLC debugging

Operation	Command
Enable QLLC debugging	**debugging qllc** { **packet** | **event** | **all** }

14.1.4 QLLC Configuration Example

I. Network requirements

As shown in the following network diagram, Router A is connected to the LAN to which a UNIX host (SNA device) is attached and Router B is connected to the X.25 network to which an IBM server (SNA device) is attached. The two routers are connected through an IP network. On Router A, DLSw is enabled, and on Router B, DLSw and QLLC are enabled.

It is required that the UNIX host could communicate with the remote server across an IP network and an X.25 network.

II. Network diagram

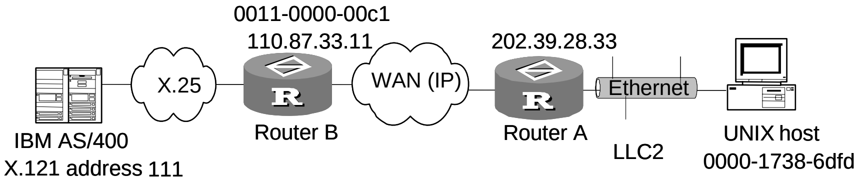


Figure 14-2 Network diagram for QLLC

III. Configuration procedure

Note:

This scenario assumes that the two routers have reachable routes between them.

1) Configure Router A

```
[Quidway] dlsw local 202.39.28.33
[Quidway] dlsw remote 110.87.33.11
[Quidway] dlsw bridge-set 1
[Quidway] interface ethernet 0/0/0
[Quidway-Ethernet0/0/0] bridge-set 1
```

2) Configure Router B

```
[Quidway] dlsw local 110.87.33.11
[Quidway] dlsw remote 202.39.28.33
[Quidway] interface serial 0/0/0
[Quidway-Serial1/0/0] link-protocol x25 dce ietf
[Quidway-Serial1/0/0] x25 x121-address 222
[Quidway-Serial1/0/0]  x25  qllc-switch  111  virtual-mac  0011-0000-00c1
partner-mac 0000-1738-6dfd
```

Chapter 15 SOT Configuration

15.1 SOT Overview

SDLC over TCP/IP (SOT) is a tunneling technology which integrates SNA into TCP/IP, to implement SDLC protocol transmission over a wide area network (WAN). SOT encapsulates SDLC frames in TCP/IP, for transmission with TCP/IP. SOT is a data link layer solution of SNA multi-protocol router.

SOT applies to connect a front end processor or IBM host to a remote communication controller.

SOT can operate in one of the following three modes:

Simple SOT mode: where the router sends all received packets intact to the remote end without address checking, just as the IBM devices at its two ends would when directly connected. This mode is only applicable to point-to-point communication, as shown in Figure 15-1.

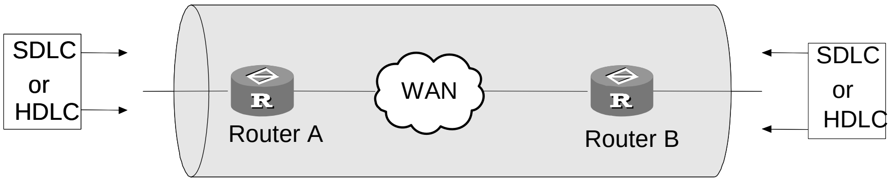


Figure 15-1 Simple SOT mode

SDLC pass-through mode: where the router sends all received SDLC frames (including the control frames) intact to the destination. SDLC sessions are maintained by the IBM devices at both ends. In this mode however, the router checks the destination SDLC address in each received SDLC frame and looks up the address maps configured using the **sot send address** command for the associated IP address. If a match is found, the router then encapsulates the SDLC frame in a TCP packet and sends it to the router with the obtained IP address. The SDLC pass-through mode is applicable to point to multipoint communication, as shown in Figure 15-2.

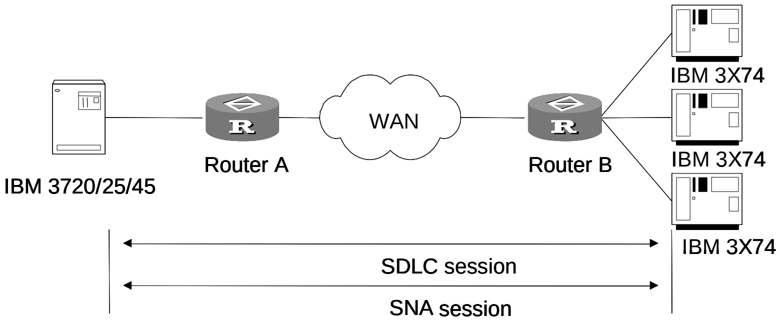


Figure 15-2 SDLC pass-through mode

SOT local acknowledgment mode: where the router must participate in SDLC session, processing all SDLC control frames, including receive end not ready frame, receive end ready frame, reject frame, and so on, as shown in Figure 15-3.

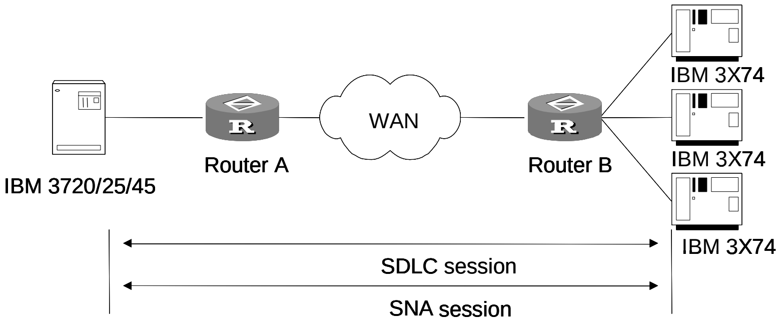


Figure 15-3 SOT local acknowledgment mode

The SDLC pass-through mode and SOT local acknowledgment mode are called SDLC modes; however, their configurations are different.

15.2 SOT Configuration

SOT configuration tasks include:

I. Global configuration

- Configuring the local SOT entity
- Configuring SOT protocol groups
- Specifying the maximum number of keepalive checks (optional, configured only when the role of the router is primary in SOT local acknowledgment mode)
- Configuring the keepalive timer (optional, only for the SOT local acknowledgment mode)

II. Interface configuration

1) Simple mode

- Configuring SOT encapsulation
- Assigning the interface to a SOT protocol group
- Configuring an address for the router to forward all SDLC frames

2) SDLC mode

SDLC pass-through mode (broadcast mode included):

- Configuring SOT encapsulation
- Assigning the interface to a SOT protocol group
- Configuring the SDLC addresses of the terminal
- Setting the SDLC role of the router (required in broadcasting mode only)
- Configuring SOT routing

SOT local acknowledgment mode:

- Configuring SOT encapsulation
- Assigning interfaces to SOT protocol groups
- Configuring the SDLC addresses of terminals
- Configuring the SDLC role of the router in pass-through (broadcast) mode or SOT local acknowledgment mode
- Configuring SOT routing

15.2.1 Assigning an IP Address to the Local SOT Entity

Use the **sot peer** command on the local and remote routers respectively to specify the two endpoints of the SOT tunnel for SDLC frame transmission with TCP/IP.

Perform the following configuration in system view.

Table 15-1 Assign an IP address to the local SOT entity

Operation	Command
Assign an IP address to a local SOT entity	**sot peer** *ip-address*
Remove the local SOT entity	**undo sot peer**

The IP address provided in this command must belong to an interface that is always up, a loopback interface for example. Or, the tunnel cannot be established and the system prompts that the IP address is not a local address.

15.2.2 Configuring SOT Protocol Groups

The SOT protocol groups fall into two modes: simple and SDLC.

Perform the following configuration in system view.

I. Configuring a simple protocol group

Table 15-2 Configure a simple protocol group

Operation	Command
Configure a simple protocol group	**sot group-set** *group-number* **simple**
Remove a specified protocol group	**undo sot group-set** *group-number*

II. Configuring an SDLC protocol group

Table 15-3 Configure an SDLC protocol group

Operation	Command
Configure an SDLC protocol group	**sot group-set** *group-number* **sdlc**
Remove a specified protocol group	**undo sot group-set** *group-number*

15.2.3 Configuring SOT Encapsulation

Perform the following configuration in synchronous serial interface view.

Table 15-4 Configure SOT encapsulation

Operation	Command
Encapsulate the synchronous serial interface with SOT.	**link-protocol sot**

15.2.4 Adding Serial Interfaces to SOT Protocol Groups

You can assign a serial interface to only one SOT protocol group. If this group is operating in simple SOT mode, the interface will operate in simple SOT mode providing only point-to-point data transmission. If this group is operating in SDLC mode, the interface operates in pass-through mode or local acknowledgement mode providing point to multipoint data transmission.

Only after configuring the **sot gather** command can you configure other interface-level commands except for the **link-protocol sot** command. Depending on the type of the configured protocol group, configure protocol group parameters appropriately.

📖 **Note:**

The configuration of the **sot gather** *group-number* command will replace the original one, if there is any.

When the type of the SOT protocol group changes, from simple to SDLC for example, the SOT configuration on the interface is removed.

Perform the following configuration in synchronous serial interface view.

Table 15-5 Assign the serial interface to a SOT protocol group

Operation	Command
Assign the interface to an existing SOT protocol group	**sot gather** *group-number*
Remove the SOT protocol group to which the interface is assigned	**undo sot gather** *group-number*

15.2.5 Specifying the Maximum Number of Keepalive Checks

You can specify the primary end to check connectivity after the TCP connection between the SOT entities fails. If all checks are failed, the primary peer terminates the SOT connection. If the number of keepalive checks is not configured, the system disconnects the SOT connection upon the expiration of the timer configured using the **sot timer keepalive** command.

Perform the following configuration in system view.

Table 15-6 Specify the maximum number of keepalive checks

Operation	Command
Specify the maximum number of keepalive checks	**sot counter keepalive** *count*
Disable connectivity check before terminating the connection	**undo sot counter keepalive** *count*

The command is valid for the primary peer in the SOT local acknowledgment mode. You may use it in conjunction with the **sot timer keepalive** command.

By default, SOT connection is disconnected without keepalive check.

15.2.6 Configuring the Keepalive Timer

You can specify the primary end to check connectivity after the TCP connection between the SOT entities fails. If the number of keepalive checks is not configured, the system disconnects the SOT connection upon the expiration of the timer configured using the **sot timer keepalive** command.

Perform the following configuration in system view.

Table 15-7 Configure the keepalive timer

Operation	Command
Configure the keepalive timer	**sot timer keepalive** [*seconds*]
Restore the default of the keepalive timer	**undo sot timer keepalive** [*seconds*]

The keepalive timer defaults to 30 seconds.

Use this command in SOT local acknowledgement mode and in conjunction with the **sot counter keepalive** command.

15.2.7 Configuring the Parameters about a Protocol Group on the Interface

Perform the following configuration in synchronous serial interface view.

I. Configuring the SDLC address of a connected terminal

Use the **sot sdlc controller** command in SDLC pass-through mode (non-broadcast mode) or SOT local acknowledgement mode.

You can configure the SDLC addresses of multiple terminals on an interface. Before you can send SDLC frames to a terminal using the **sot send address** command, you must configure its SDLC address using the **sot sdlc controller** command.

Before deleting the SDLC address of a connected terminal using the **undo sot sdlc controller** command, you must use the **undo sot send address** command to remove the corresponding SDLC frame routing entry, if one has been configured.

Table 15-8 Configure the SDLC address of a terminal

Operation	Command
Configure the SDLC address of a connected terminal	**sot sdlc controller** *sdlc-address*
Remove the SDLC address of a connected terminal	**undo sot sdlc controller** *sdlc-address*

The SDLC address of the terminal cannot be 0 or FF; they are reserved for other purpose or broadcast.

In the pass-through (broadcast) mode, use the **sot sdlc broadcast** command to configure the broadcast SDLC address FF for the connected terminals.

Table 15-9 Configure the broadcast address FF for the connected terminals

Operation	Command
Configure the broadcast address FF for the connected SDLC terminals	**sot sdlc broadcast**
Disable SDLC broadcast	**undo sot sdlc broadcast**

II. Setting the SDLC role of the router

This command is applicable to the SOT local acknowledgement mode and the SDLC pass-through (broadcast) mode.

In SOT local acknowledgement mode, you must assign a role to the router, depending on the position of the router in the sequence of primary (IBM host), secondary (router), primary (router), and secondary (terminal). If the router is connected to an IBM host, its role is SDLC secondary node; if the router is connected to a terminal, its role is SDLC primary node. In this mode, the SDLC address of a terminal must be unique within its protocol group.

In broadcast mode, you must set the role of the router to secondary, regardless of whether it is connected to an IBM host or to a terminal. Other SOT modes however, do not involve the role of secondary node.

In other mode, you do not need to assign a role to the router.

Table 15-10 Set the SDLC role of the router

Operation	Command
Set the SDLC role of the router to primary	**sot sdlc-status primary**
Set the SDLC role of the router to secondary	**sot sdlc-status secondary**
Delete the SDLC role setting	**undo sot sdlc-status**

III. Configuring SOT routing

1) Simple mode

When operating in simple mode, you can configure the router to forward all SDLC frames to the specified address.

In simple mode, the SDLC address of the connected terminal defaults to 01. You do not need to configure it.

Table 15-11 Configure the interface to send all SDLC frames to the specified address

Operation	Command
Configure the interface to send all received SDLC frames to the specified address	**sot send all tcp** *ip-address*
Disable the interface to forward SDLC frames	**undo sot send all tcp** *ip-address*

2) SDLC mode

Table 15-12 Configure the route for sending SDLC frames to a specified terminal

Operation	Command
Configure the route for sending SDLC frames to a specified terminal	**sot send address** *sdlc-address* **tcp** *ip-address* [**local**] [**send-queue**]
Remove the specified route entry	**undo sot send address** *sdlc-address* **tcp** *ip-address* [**local**] [**send-queue**]

- SOT non-local acknowledgement mode

In SOT non-local acknowledgement (or pass-through) mode, the router checks the destination SDLC address in each received SDLC frame and looks up the address maps configured using the **sot send address** command for the associated IP address. If a match is found, the router then encapsulates the SDLC frame in a TCP packet and sends it to the router with the obtained IP address. If broadcast is desired, you can set the *sdlc-address* argument to the broadcast address 0xFF.

- SOT local acknowledgement mode

In SOT local acknowledgement mode, the router checks the contents of each received SDLC frame in addition to the destination terminal SDLC address. The router removes the contents that are not intended for the destination, and looks up the SOT routing table for a match corresponding to the SDLC address of the destination terminal. If a match is found, the router encapsulates the SDLC frame in a TCP packet and sends it across the IP network.

This mode does not support broadcast.

15.3 Displaying and Debugging SOT

Execute the **display** command in any view.

Table 15-13 Display information about SOT

Operation	Command
Display the current SOT connection state	**display sot**
Display the state of the current serial interface	**display interface serial** *number*
Display the TCP connection state	**display tcp status**

15.4 SOT Configuration Example

15.4.1 Simple-Mode SOT Configuration Example

I. Network requirements

As shown in Figure 15-4, an IBM host is connected to the Serial0/0/0 interface on Router A; a terminal is connected to the Serial0/0/0 interface on Router B. The two routers are connected using their Serial1/0/0 interfaces through a WAN.

Configure simple-mode SOT on Router A and Router B to enable the IBM host to communicate with the terminal.

II. Network diagram

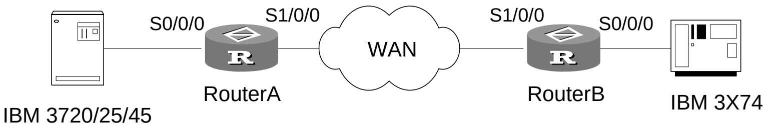


Figure 15-4 Network diagram for simple-mode SOT configuration

III. Configuration procedure

1) Configure Router A

```
[Quidway] interface loopback 0
[Quidway-LoopBack0] ip address 1.0.0.1 24
[Quidway-LoopBack0] quit
[Quidway] sot peer 1.0.0.1
[Quidway] sot group-set 8 simple
[Quidway] interface serial 0/0/0
[Quidway-Serial0/0/0] link-protocol sot
[Quidway-Serial0/0/0] sot gather 8
[Quidway-Serial0/0/0] sot send all tcp 1.0.0.2
[Quidway-Serial0/0/0] interface serial 1/0/0
[Quidway-Serial1/0/0] ip address 100.1.1.1 16
[Quidway-Serial1/0/0] quit
[Quidway] ip route-static 200.2.1.1 serial 1/0/0
```

```
[Quidway] ip route-static 1.0.0.2 serial 1/0/0
```

2) Configure Router B

```
[Quidway] interface loopback 0
[Quidway-LoopBack0] ip address 1.0.0.2 24
[Quidway-LoopBack0] quit
[Quidway] sot peer 1.0.0.2
[Quidway] sot group-set 8 simple
[Quidway] interface serial 0/0/0
[Quidway-Serial0/0/0] link-protocol sot
[Quidway-Serial0/0/0] sot gather 8
[Quidway-Serial0/0/0] sot send all tcp 1.0.0.1
[Quidway-Serial0/0/0] interface serial 1/0/0
[Quidway-Serial1/0/0] ip address 200.2.1.1 16
[Quidway-Serial1/0/0] quit
[Quidway] ip route-static 100.1.1.1 serial 1/0/0
[Quidway] ip route-static 1.0.0.1 serial 1/0/0
```

15.4.2 Pass-Through Mode SOT Configuration Example

I. Network requirements

As shown in Figure 15-5, an IBM host is connected to the Serial0/0/0 interface on Router A; terminal C1 and C2 are connected to the Serial0/0/0 and Serial 0/0/1 interfaces on Router B respectively. The two routers are connected using their Serial1/0/0 interfaces through a WAN.

Configure pass-through SOT on Router A and Router B to enable the IBM host to communicate with terminal C1 and C2.

II. Network diagram

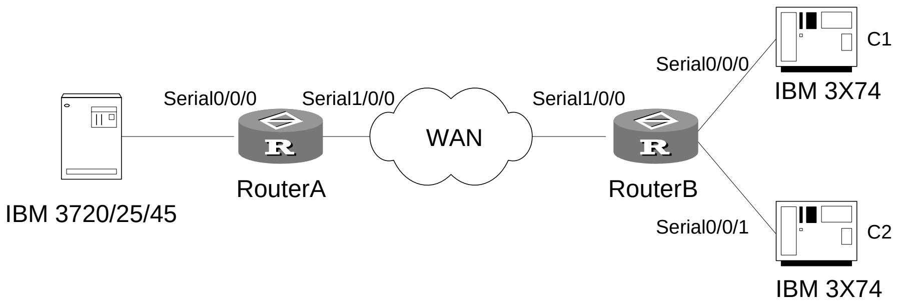


Figure 15-5 Network diagram for pass-through SOT

III. Configuration procedure

1) Configure Router A

```
[Quidway] interface loopback 0
```

```
[Quidway-LoopBack0] ip address 1.0.0.1 24
[Quidway-LoopBack0] quit
[Quidway] sot peer 1.0.0.1
[Quidway] sot group-set 1 sdlc
[Quidway] interface serial 0/0/0
[Quidway-Serial0/0/0] link-protocol sot
[Quidway-Serial0/0/0] sot gather 1
[Quidway-Serial0/0/0] sot sdlc controller c1
[Quidway-Serial0/0/0] sot send address c1 tcp 1.0.0.2
[Quidway-Serial0/0/0] sot sdlc controller c2
[Quidway-Serial0/0/0] sot send address c2 tcp 1.0.0.2
[Quidway-Serial0/0/0] interface serial 1/0/0
[Quidway-Serial1/0/0] ip address 100.1.1.1 16
[Quidway-Serial1/0/0] quit
[Quidway] ip route-static 200.2.1.1 serial 1/0/0
[Quidway] ip route-static 1.0.0.2 serial 1/0/0
```

2) Configure Router B

```
[Quidway] interface loopback 0
[Quidway-LoopBack0] ip address 1.0.0.2 24
[Quidway-LoopBack0] quit
[Quidway] sot peer 1.0.0.2
[Quidway] sot group-set 1 sdlc
[Quidway] interface serial 0/0/0
[Quidway-Serial0/0/0] link-protocol sot
[Quidway-Serial0/0/0] sot gather 1
[Quidway-Serial0/0/0] sot sdlc controller c1
[Quidway-Serial0/0/0] sot send address c1 tcp 1.0.0.1
[Quidway-Serial0/0/0] interface serial 0/0/1
[Quidway-Serial0/0/1] link-protocol sot
[Quidway-Serial0/0/1] sot gather 1
[Quidway-Serial0/0/1] sot sdlc controller c2
[Quidway-Serial0/0/1] sot send address c2 tcp 1.0.0.1
[Quidway-Serial0/0/1] interface serial 1/0/0
[Quidway-Serial1/0/0] ip address 200.2.1.1 16
[Quidway-Serial1/0/0] quit
[Quidway] ip route-static 100.1.1.1 serial 1/0/0
[Quidway] ip route-static 1.0.0.1 serial 1/0/0
```

15.4.3 Pass-Through SOT (Broadcast) Configuration Example

I. Network requirements

As shown in Figure 15-6, an IBM host is connected to the Serial0/0/0 interface of Router A; terminal C1 and C2 are connected to the Serial0/0/0 and Serial 0/0/1 interfaces on Router B respectively. The two routers are connected using their Serial1/0/0 interfaces through a WAN.

Configure pass-through SOT (broadcast) on Router A and Router B, and broadcast data to terminal C1 and C2.

II. Network diagram

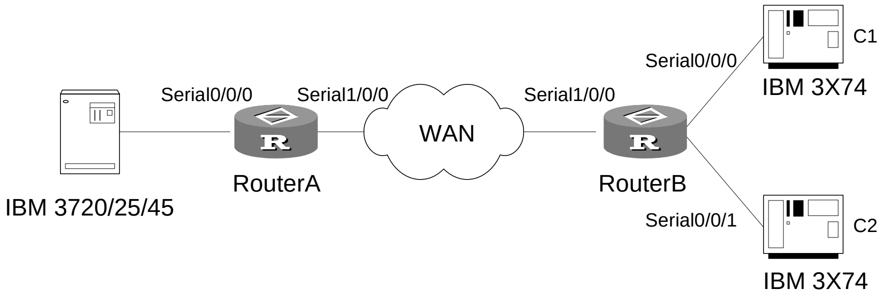


Figure 15-6 Network diagram for pass-through SOT (broadcast)

III. Configuration procedure

1) Configure Router A

```
[Quidway] interface loopback 0
[Quidway-LoopBack0] ip address 1.0.0.1 24
[Quidway-LoopBack0] quit
[Quidway] sot peer 1.0.0.1
[Quidway] sot group-set 1 sdlc
[Quidway] interface serial 0/0/0
[Quidway-Serial0/0/0] link-protocol sot
[Quidway-Serial0/0/0] sot gather 1
[Quidway-Serial0/0/0] sot sdlc-status secondary
[Quidway-Serial0/0/0] sot sdlc broadcast
[Quidway-Serial0/0/0] sot send address ff tcp 1.0.0.2
[Quidway-Serial0/0/0] interface serial 1/0/0
[Quidway-Serial1/0/0] ip address 100.1.1.1 16
[Quidway-Serial1/0/0] quit
[Quidway] ip route-static 200.2.1.1 serial 1/0/0
[Quidway] ip route-static 1.0.0.2 serial 1/0/0
```

2) Configure Router B

```
[Quidway] interface loopback 0
```

```
[Quidway-LoopBack0] ip address 1.0.0.2 24
[Quidway-LoopBack0] quit
[Quidway] sot peer 1.0.0.2
[Quidway] sot group-set 1 sdlc
[Quidway] interface serial 0/0/0
[Quidway-Serial0/0/0] link-protocol sot
[Quidway-Serial0/0/0] sot gather 1
[Quidway-Serial0/0/0] sot sdlc-status secondary
[Quidway-Serial0/0/0] sot sdlc broadcast
[Quidway-Serial0/0/0] sot send address ff tcp 1.0.0.1
[Quidway-Serial0/0/0] interface serial 0/0/1
[Quidway-Serial0/0/1] link-protocol sot
[Quidway-Serial0/0/1] sot gather 1
[Quidway-Serial0/0/1] sot sdlc-status secondary
[Quidway-Serial0/0/1] sot sdlc broadcast
[Quidway-Serial0/0/1] sot send address ff tcp 1.0.0.1
[Quidway-Serial0/0/1] interface serial 1/0/0
[Quidway-Serial1/0/0] ip address 200.2.1.1 16
[Quidway-Serial1/0/0] quit
[Quidway] ip route-static 100.1.1.1 serial 1/0/0
[Quidway] ip route-static 1.0.0.1 serial 1/0/0
```

15.4.4 SOT Local Acknowledgement Mode Configuration Example

I. Network requirements

As shown in Figure 15-7, an IBM host is connected to the Serial0/0/0 interface on Router A; terminal C1 and C2 are connected to the Serial0/0/0 and Serial 0/0/1 interfaces on Router B respectively. The two routers are connected using their Serial1/0/0 interfaces through a WAN.

Configure SOT local acknowledgement mode on Router A and Router B to enable the IBM host to communicate with terminal C1 and C2.

II. Network diagram

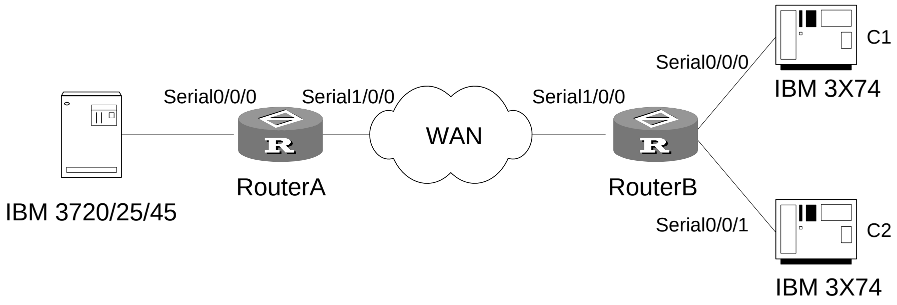


Figure 15-7 Network diagram for SOT local acknowledgement mode configuration

III. Configuration procedure

1) Configure Router A

```
[Quidway] interface loopback 0
[Quidway-LoopBack0] ip address 1.0.0.1 24
[Quidway-LoopBack0] quit
[Quidway] sot peer 1.0.0.1
[Quidway] sot group-set 1 sdlc
[Quidway] interface serial 0/0/0
[Quidway-Serial0/0/0] link-protocol sot
[Quidway-Serial0/0/0] sot gather 1
[Quidway-Serial0/0/0] sot sdlc-status secondary
[Quidway-Serial0/0/0] sot sdlc controller c1
[Quidway-Serial0/0/0] sot send address c1 tcp 1.0.0.2 local
[Quidway-Serial0/0/0] sot sdlc controller c2
[Quidway-Serial0/0/0] sot send address c2 tcp 1.0.0.2 local
[Quidway-Serial0/0/1] interface serial 1/0/0
[Quidway-Serial1/0/0] ip address 100.1.1.1 16
[Quidway-Serial1/0/0] quit
[Quidway] ip route-static 200.2.1.1 serial 1/0/0
[Quidway] ip route-static 1.0.0.2 serial 1/0/0
```

2) Configure Router B

```
[Quidway] interface loopback 0
[Quidway-LoopBack0] ip address 1.0.0.2 24
[Quidway-LoopBack0] quit
[Quidway] sot peer 1.0.0.2
[Quidway] sot group-set 1 sdlc
[Quidway] interface serial 0/0/0
[Quidway-Serial0/0/0] link-protocol sot
[Quidway-Serial0/0/0] sot gather 1
[Quidway-Serial0/0/0] sot sdlc-status primary
[Quidway-Serial0/0/0] sot sdlc controller c1
[Quidway-Serial0/0/0] sot send address c1 tcp 1.0.0.1 local
[Quidway-Serial0/0/0] interface serial 0/0/1
[Quidway-Serial0/0/1] link-protocol sot
[Quidway-Serial0/0/1] sot gather 1
[Quidway-Serial0/0/1] sot sdlc-status primary
[Quidway-Serial0/0/1] sot sdlc controller c2
[Quidway-Serial0/0/1] sot send address c2 tcp 1.0.0.1 local
[Quidway-Serial0/0/1] interface serial 1/0/0
[Quidway-Serial1/0/0] ip address 200.2.1.1 16
[Quidway-Serial1/0/0] quit
[Quidway] ip route-static 100.1.1.1 serial 1/0/0
```

```
[Quidway] ip route-static 1.0.0.1 serial 1/0/0
```

Chapter 16 Web Cache Redirection Configuration

16.1 Introduction to Web Cache Redirection

The Web cache redirection is a technology that lightens the pressure on the link to the WAN and speeds up the Internet access.

As shown in Figure 16-1, the PC is in the LAN connected to the router and the Web cache server stores information of frequently accessed websites. With Web cache redirection enabled on the router, HTTP requests from the PC will be redirected to the Web cache server. If what the PC desires is available on the Web cache server, the server will directly send it to the PC; otherwise, the PC needs to access the Internet to obtain it.

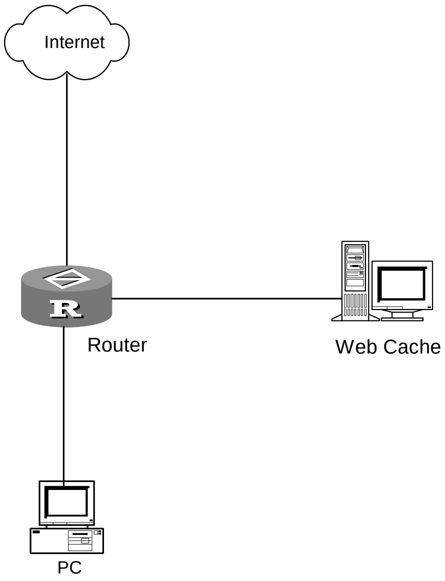


Figure 16-1 Web cache redirection

16.2 Configuring Web Cache Redirection

16.2.1 Specifying the Web Cache Server

Perform the following configuration in system view.

Table 16-1 Specify the Web cache server

Operation	Command
Specify the IP address of the Web cache server and the TCP port number for HTTP packets	**webcache redirect address** *ip-address* [**port** *tcp-port-number*]

Operation	Command
Delete the configured Web cache server	**undo webcache redirect**

16.2.2 Enabling Web Cache Redirection

Perform the following configuration in interface view.

Table 16-2 Enable Web cache redirection

Operation	Command
Enable Web cache redirection	**webcache redirect enable**
Disable Web cache redirection	**undo webcache redirect enable**

Note:

- If the Web cache server is unreachable, Web cache redirection will fail to function.
- If you configure both the IP address of the Web cache server and the TCP port number for HTTP packets correctly but do not enable Web cache redirection on the inbound interface, the Web cache function will not work. In this case, HTTP packets will be sent out of the normal outbound interface.

16.3 Web Cache Redirection Configuration Example

I. Network requirements

As shown in Figure 16-2, two PCs are connected to the router via the interfaces Ethernet1/0/1 and Ethernet1/0/2 respectively, and the Web cache server is connected to the router via the interface Ethernet1/0/3. The IP address of the Web cache server is 10.15.20.2/24. It is required that the HTTP traffic of the two PCs should be redirected after the Web cache redirection is enabled.

II. Network diagram

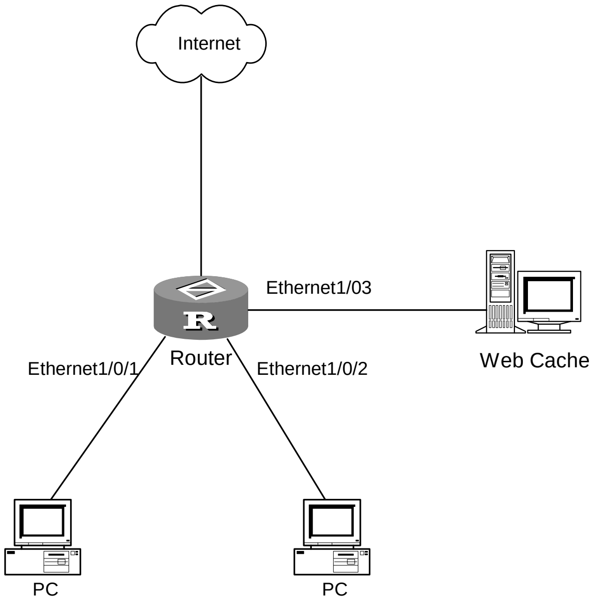


Figure 16-2 Network diagram for Web cache redirection

III. Configuration procedure

# Configure the IP address of the Web cache server and the TCP port number for HTTP packets on the router.

```
<Quidway> system-view
[Quidway] webcache redirect address 10.15.20.2 port 8080
```

# Enable Web cache redirection in interface view.

```
[Quidway] interface ethernet 1/0/1
[Quidway-Ethernet1/0/1] webcache redirect enable
[Quidway-Ethernet1/0/1] quit
[Quidway] interface ethernet 1/0/2
[Quidway-Ethernet1/0/2] webcache redirect enable
```

Chapter 17 MIP Configuration

Note:

This feature is only available on AR 46 Series Routers.

17.1 Introduction to MIP

The fast network expansion along with technology innovation leads to growing demands for a more flexible access to the Internet, especially for the ubiquitous access and connectivity in rapid mobile data communication.

On traditional TCP/IP networks, once a mobile node of a subnet moves to another subnet, it cannot use its fixed IP address on its home network to communicate any more. Mobile IP (MIP) is introduced to solve this problem.

With MIP, which is independent of network media, a mobile node can always maintain the same IP address and a live TCP connection regardless of movement between heterogeneous networks.

In addition, using the MIP technology can break the regional limitation of wireless LAN (WLAN) and overcome the problems caused by using dynamic host configuration protocol (DHCP) across network segments, such as interrupted communications.

17.1.1 Basic Concepts of MIP

I. Terms

- Home network: A network, possibly virtual, having a network prefix matching that of the home address of a mobile node. Note that standard IP routing mechanisms will deliver datagrams destined for the home address of a mobile node to the home network.
- Home agent (HA): A host or router on the home network of a mobile node that tunnels datagrams for delivery to the mobile node when it is away from home, and maintains current location information for the mobile node.
- Home address: An IP address that is assigned from the home network segment to a mobile node. It remains unchanged regardless of where the node is attached to the Internet.
- Foreign network: Any network other than the home network of the mobile node.
- Foreign agent (FA): A router on a mobile node's visited network which forwards datagrams from the home agent to the mobile node.

- Care-of address: The termination point of a tunnel toward a mobile node, for datagrams forwarded to the mobile node while it is away from home. MIP can use two different types of care-of address: a "foreign agent care-of address" is an address of a foreign agent with which the mobile node is registered, and a "co-located care-of address" is an externally obtained (through manual configuration or DHCP) local address which the mobile node has associated with one of its own network interfaces.
- Mobile node (MN): A host or router that keeps its IP address unchanged and continues its ongoing communication when changing its attachment point from one network or subnetwork to another.
- Mobile router (MR): A router with the functions of a mobile node.
- Correspondent node (CN): A peer with which a mobile node is communicating. A CN may be either mobile or stationary.
- Mobility agent (MA): Either a home agent or a foreign agent.
- Mobility binding: The association of a home address with a care-of address, along with the remaining lifetime of that association.
- Visitor list: The list of mobile nodes visiting a foreign agent.

II. Security association

When a mobile node registers, it can use the SPI and secret (a share key, or appropriate public/private key pair) defined in the security association for authentication, encryption, and decryption (through MD5 encryption/decryption algorithm). This helps secure the communications.

Six types of security associations are available:

- HA-MN security association
- HA-FA security association
- FA-MN security association
- FA-HA security association
- MR-HA security association
- MR-FA security association

III. Binding table

A binding table is on an HA. It maintains the association of home addresses with care-of addresses. An HA updates its binding table entries based on registration events of its mobile nodes.

IV. Pending table

A pending table is on an FA. It maintains information about mobile nodes registering with the FA, such as the home address, MAC address, and HA address. Once a mobile node is registered, information about it is deleted from the pending table and added to the visitor table. If a mobile node fails the registration, information about it is simply deleted from the pending table.

V. Visitor table

A visitor table is on an FA. It maintains information about mobile nodes visiting the local network such as the home address, MAC address, and HA address. An FA updates its visitor table entries based on registration events of the mobile nodes.

VI. Simultaneous binding

When an MR supports simultaneous binding, if the HA also supports simultaneous binding, the HA retains its prior mobility binding information (including information about the care-of address), that is, the HA retains information about multiple care-of addresses of the MR. Otherwise, the HA replaces the prior mobility binding information with the new binding information specified in the registration request.

Multiple simultaneous mobility bindings are likely to be useful when an MN using at least one wireless network interface moves within a wireless transmission range with more than one foreign agent. When the HA allows simultaneous bindings, it tunnels a separate copy of each arriving packet to each care-of address of the MR, and the MR will receive multiple copies of packets destined for it.

17.1.2 Fundamentals of MIP

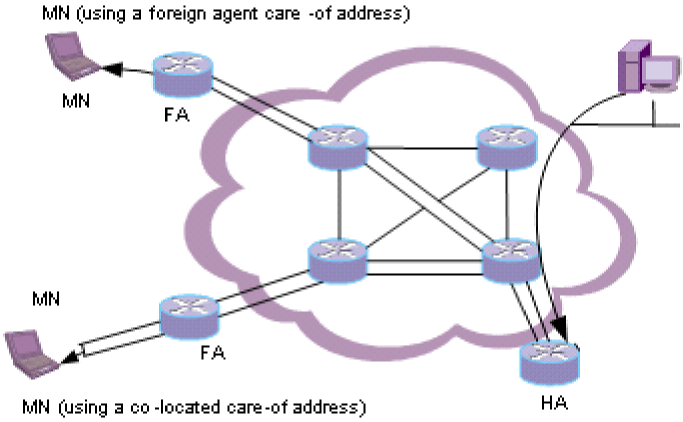

MN (using a foreign agent care -of address)
MN
FA
MN
FA
MN (using a co -located care-of address)
HA

Figure 17-1 Fundamentals of MIP

1) Mobility agents advertise their presence through agent advertisements on their respective local networks. Upon receipt of agent advertisements, an MN determines whether it is on its home network or a foreign network. When the MN detects that it is located on its home network, it operates in conventional TCP/IP mode and does not need mobility services.
2) When an MN detects that it has moved to a foreign network, it starts MIP, obtains a care-of address on the foreign network, and registers its care-of address with its HA, so as to receive IP packets destined for it. The care-of address can be either the address of the FA (a foreign agent care-of address), or an address dynamically obtained through DHCP (a co-located care-of address).

3) Upon receiving the care-of address of an MN, the HA builds a tunnel to the care-of address, and intercepts and forwards IP packets destined for the MN to the care-of address through the tunnel. Three tunneling technologies are available: IP in IP encapsulation, minimal IP encapsulation, and generic routing encapsulation (GRE).

- IP in IP encapsulation encapsulates the original IPv4 packet into the payload part of another IPv4 packet and takes the addresses of the two tunnel ends (that is, the HA address and the care-of address) as the source address and destination address respectively. The source address and destination address in the header of the inner IP packet (the original IPv4 packet) identifies the IP addresses of the sender and receiver of the original packet.
- Minimal IP encapsulation, an optional tunneling mode, eliminates the redundant part of the outer IP header and the inner IP header of an IP in IP encapsulated packet to reduce tunneling overhead. This assumes that the original IP packets are not fragments, for minimal IP encapsulation inserts between the new IP packet header and the original payload a minimum forwarding header, which does not accommodate information about fragmentation.
- GRE encapsulation supports IP as well as other network layer protocols. It supports encapsulating the packet of a protocol into the packet of another protocol.

MIP in this manual supports two tunneling technologies: IP-in-IP encapsulation and GRE.

4) The tunneled packets are detunneled at the care-of address to restore the original IP packets. If the MN is using a foreign agent care-of address, the FA performs detunneling and forwards the resulted original IP packets to the MN. If the MN is using a co-located care-of address, it detunnels the tunneled packets and continues to resolve the IP packet. This way, the MN can receive IP packets destined for it while it is away from its home network.
5) When located on a foreign network, an MN can send IP packets to its CN through a router on the foreign network of an FA. In addition, an MN can also use the reverse tunneling technology to send IP packets through the tunnel to the HA (when adopting a co-located care-of address), or sending the packets to the FA (when adopting a foreign agent care-of address). In the latter case, the FA then encapsulates and forwards the packets to the HA, which decapsulates and forwards the packets to the CN through conventional routing.
6) When moving from one foreign network to another, an MN only needs to register its updated care-of address with its HA.
7) After returning to its home network, an MN deregisters its care-of address with its HA. Thus, it can communicate in conventional TCP/IP mode again.

17.1.3 Functions Implemented by the MIP Module

The MIP module implements these functions: agent discovery, registration, routing, virtual network, and mobile router.

I. Agent discovery

FAs and HAs advertise their availability on their respective local networks through agent advertisements of the ICMP router discovery protocol (IRDP). An MN detecting these messages can determine whether it is on the local network or a foreign network and which HAs or FAs are present on the current network:

- If it receives agent advertisements from an HA, it concludes that it is still on its home network and does not enable the Mobile IP function.
- If it detects that it has moved to a new foreign network, it renews its registration with its HA after obtaining its care-of address, notifying the HA of its new location.
- If it detects that it has returned to its home network, it deregisters with its HA.

By default, an FA or HA does not periodically send agent advertisements; they send agent advertisements only after receiving agent solicitations from MNs. By setting IRDP-relevant attributes, you can specify an FA or HA to advertise its availability periodically by agent advertisements.

II. Registration

1) When an MN detects that it moves from a network to another, the connected FA is rebooting, or the current registration is expiring, it sends a registration request to the FA (when it is using a foreign agent care-of address) or to the HA (when it is using a co-located care-of address). If it sends its registration request to the HA, skip to step 3.
2) Upon receiving a registration request, the FA performs a series of validity check. Failure of any item causes the FA to send to the MN a registration reply that denies the request. The Code field of the registration reply is used to indicate the reason. If the registration request is valid, the FA relays the message to the HA of the MN and builds a pending entry.
3) Upon receiving a registration request, the HA performs a series of validity check similar to that of an FA. If the request is invalid, the HA sends to the MN or FA a registration replay, indicating the failure reason by the Code field. If the request is valid, the HA updates its binding table and adds to its routing table a route for the home address of the MN (taking virtual interface Mobile0 as the next hop), and responds with a registration reply, informing the MN or FA of the successful registration. If the MN is using a co-located care-of address, skip to step 5.
4) When receiving a registration reply, an FA also performs a series of validity check. If the reply is invalid, the FA sends a registration reply including a proper Code filed to the MN. If the reply is valid, the FA updates its visitor table, deletes the corresponding entry from its pending table, and relays the reply to the MN.

5) When receiving a registration reply, an MN performs a series of validity check alike. If the reply is valid, the MN checks the Code field to determine whether the request is granted or denied. If the request is denied, the MN takes measures to correct the mistakes and tries to register again. If the request is granted, the MN adapts its routing table to the current link and begins to communicate or continues its original communications.

6) After an MN is registered, the HA tunnels packets to the care-of address of the MN or detunnels packets from the MN (when using reverse tunneling). When the MN is using a foreign agent care-of address, the FA detunnels the packets tunneled to the MN, or tunnels packets from the MN to the HA (when using reverse tunneling). When the MN is using a co-located care-of address, the MN itself detunnels the packets tunneled to it, or tunnels packets to the HA (when using reverse tunneling).

In addition, an HA sends gratuitous ARP and proxy ARP messages. When an MN sends an ARP request, the HA relays the ARP request through proxy ARP to the CN on a foreign network and sends the obtained MAC address to the MN. When an MN away from home gets registered with the HA, the HA sends gratuitous ARP packets for the MN to update ARP entries.

III. Routing of packets

When an HA receives a packet destined for an MN, it looks up its routing table to locate the corresponding entry. If the next hop is interface Mobile0, the HA tunnels the packet to the care-of address of the MN.

When the MN is using a foreign agent care-of address, the FA is the endpoint of the tunnel, detunneling and forwarding the tunneled packets to the MN. When the MN is using a co-located care-of address, the MN is the endpoint of the tunnel that detunnels the received packets.

When an MN obtaining an FA care-of address uses reverse tunneling to communicate with its CN, the FA tunnels packets from the MN to the HA. When an MN obtaining a co-located care-of address uses reverse tunneling to communicate with its CN, the MN itself tunnels packets to the HA. The HA, as the endpoint of the reverse tunnel, detunnels the tunneled packets and routes them to the CN through conventional IP routing.

IV. Virtual network

If a home network is a virtual network, it has no physical realization external to the home agent itself and has no physical network link for sending Agent Advertisement messages. In this case, mobile nodes of the home network are always regarded as being away from home. Virtual network allows a local router to support an MN that is always located on a foreign network.

V. Mobile router

An MR is a router with the functions of an MN. It can move along with its attached static network between MAs. Therefore, the static network is also a mobile network.

A mobile router can also provide the functions of an FA for MNs. For example, the LAN of a moving ship is a mobile network, which accesses the Internet through an MR.

17.2 General MIP Policy Configuration

General MIP policy configuration refers primarily to enabling the MIP function, which is required before HA or FA configuration.

17.2.1 Configuring General MIP Policy

Table 17-1 Configure general MIP policy

Operation	Command	Description
Enter system view	**system-view**	—
Enable MIP	**mobile-ip**	Required
Set the PMTU update policy	**mobile-ip tunnel path-mtu-discovery** [**age-timer** {*seconds* | **infinite**}]	Optional By default, PMTU discovery is not performed.
Enable the MIP SNMP trap function	**snmp-agent trap enable mobile-ip**	Optional By default, MIP SNMP trap is disabled.
Display global MIP information	**display mobile-ip globals**	Available in any view
Display all MIP statistics	**display mobile-ip statistics**	

17.2.2 General MIP Policy Configuration Example

I. Network requirements

Enable MIP on two AR46 routers, one as the HA and the other as the FA. Use two laptops, one with MIP software as the MN, the other as the CN. In communication, the MN can move from its home network to the foreign network.

II. Network diagram

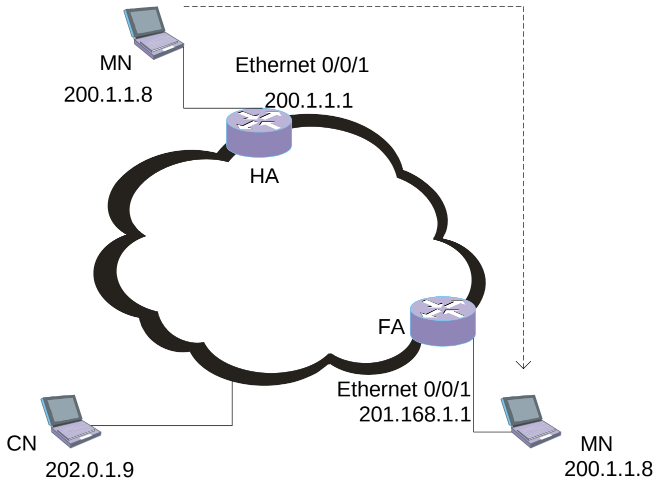


Figure 17-2 General MIP policy configuration

III. Configuration procedure

1) Configure general MIP policy on the HA

# Enable MIP on the HA.

```
<Quidway> system-view
[Quidway] mobile-ip
```

# Set the PMTU update policy on the HA. (Optional)

```
[Quidway] mobile-ip tunnel path-mtu-discovery
```

# Enable SNMP trap on the HA. (Optional)

```
[Quidway] snmp-agent trap enable mobile-ip
```

2) Configure general MIP policy on the FA

# Enable MIP on the FA.

```
<Quidway> system-view
[Quidway] mobile-ip
```

# Set the PMTU update policy on the FA. (Optional)

```
[Quidway] mobile-ip tunnel path-mtu-discovery
```

# Enable SNMP trap on the FA. (Optional)

```
[Quidway] snmp-agent trap enable mobile-ip
```

17.3 HA Configuration

17.3.1 Configuration Prerequisites

For a device to provide HA service, you must perform HA configurations on it. You can perform HA configurations only on a device with MIP enabled and MR disabled.

17.3.2 Configuring HA

Table 17-2 Configure HA

Operation	Command	Description
Enter system view	**system-view**	—
Enable the MIP function	**mobile-ip**	Required
Enable the HA function	**mobile-ip home-agent** [**care-of-acl** *number*] [**ha-virtual-net** *ip-address*] [**lifetime** *seconds*] [**replay** *seconds*] [**reverse-tunnel** {**off** | **mandatory** }] [**roam-acl** *number*]	Required
Configure the MN policy	Refer to section 17.5 "MN Configuration"	Required
Configure MIP security associations	Refer to section 17.7 "MIP Security Policy Configuration"	Required
Define a virtual network	**mobile-ip virtual-network** *ip-address* { *mask* | *mask-length* } [**ha-address** *ip-address*]	Optional If virtual network is supported when HA is enabled, you must define the virtual network.
Display information about the MIP binding table	**display mobile-ip binding** [*ip-address* | **brief**]	Available in any view
Remove a binding entry from the binding table	**reset mobile-ip binding** [*ip-address* | **interface ethernet** *interface-number*]	Available in user view

17.3.3 HA Configuration Example

I. Network requirements

The network requirements are the same as those described in section 17.2.2 I. "Network requirements". In addition, configure to allow the MN with the IP address of 200.1.1.8 to roam to FA 201.168.1.1.

II. Configuration procedure

# Add ACL 2000 as the roam-acl to specify the MN, and ACL 2001 as the care-of-acl to specify the FA.

```
<Quidway> system-view
[Quidway] acl number 2000
[Quidway-acl-basic-2000] rule permit source 200.1.1.8 0.0.0.0
[Quidway-acl-basic-2000] quit
[Quidway] acl number 2001
[Quidway-acl-basic-2001] rule permit source 201.168.1.1 0.0.0.0
[Quidway-acl-basic-2001] quit
```

# Enable the HA function.

```
[Quidway] mobile-ip home-agent care-of-acl 2001 roam-acl 2000
```

17.4 FA Configuration

17.4.1 Configuration Prerequisites

For a device to provide FA service, you must perform FA configurations on it. You can perform FA configurations only on a device with MIP enabled.

17.4.2 Configuring FA

Table 17-3 Configure FA

Operation	Command	Description
Enter system view	**system-view**	—
Enable the MIP function	**mobile-ip**	Required
Enable the FA function	**mobile-ip foreign-agent** { **care-of ethernet** *interface-number* | **pending** *seconds* }	Required
Enter Ethernet interface view	**interface ethernet** *interface-number*	—
Enable FA service on the interface	**mobile-ip foreign-agent service** [**home-acl** *acl*] [**registration-required**] [**restrict** *number*] [**reverse-tunnel** [**mandatory**]]	Required
Enable MIP prefix-length extension	**mobile-ip prefix-length**	Optional By default, this function is not enabled.
Configure the registration lifetime	**mobile-ip registration-lifetime** *seconds*	Optional By default, the registration lifetime is 3,600 seconds.

Operation	Command	Description
Configure MIP security associations	Refer to section 17.7 "MIP Security Policy Configuration"	Optional
Display information about MIP visitors	**display mobile-ip visitor** [**pending**] [*ip-address* | **brief**]	Available in any view
Display MIP information of interfaces	**display mobile-ip interface** [**ethernet** *interface-number*]	
Remove information in the visitor table and/or the pending table on the FA	**reset mobile-ip visitor** [**pending**] [*ip-address* | **interface ethernet** *interface-number*]	Available in user view

17.4.3 FA Configuration Example

I. Network requirements

The network requirements are the same as those described in section 17.2.2 I. "Network requirements".

II. Configuration procedure

# Enable the FA function and configure the care-of interface.

```
<Quidway> system-view
[Quidway] mobile-ip foreign-agent care-of ethernet 0/0/1
```

# Enable FA service on interface Ethernet 0/0/1.

```
[Quidway] interface ethernet 0/0/1
[Quidway-Ethernet0/0/1] mobile-ip foreign-agent service
```

# Enable prefix-length extension on interface Ethernet 0/0/1. (Optional)

```
[Quidway-Ethernet0/0/1] mobile-ip prefix-length
```

# Set registration lifetime on interface Ethernet 0/0/1. (Optional)

```
[Quidway-Ethernet0/0/1] mobile-ip registration-lifetime 38000
```

17.5 MN Configuration

17.5.1 Configuration Prerequisites

For a device to provide HA service for MNs, you must perform MN configurations on it. You can perform MN configurations only on a device with HA enabled.

In addition, you must perform some MR configurations when an MN is an MR, so that the HA supports the MR and the connected mobile network.

17.5.2 Configuring MN

Table 17-4 Configure MN

Operation	Command	Description
Enter system view	**system-view**	—
Enable the MIP function	**mobile-ip**	Required
Configure MN attributes	**mobile-ip node** *low-addr* [*up-addr*] { **interface ethernet** *name* | **virtual-network** *ip-address mask*} [**lifetime** *lifetime*]	Required
If an MN is an MR, configure the number of the MR on the HA and enter HA-MR view	**mobile-ip home-agent mobile-router** *number*	Optional Required when an MN is an MR and the HA is required to support the mobile network connected by the MR.
Configure the IP address of the MR	**ip address** *ip-address*	Optional Required when an MN is an MR and the HA is required to support the mobile network connected by the MR.
Configure a mobile network for the MR	**mobile-network** *ip-address* {*mask* | *mask-length* }	Optional Required when an MN is an MR and the HA is required to support the mobile network connected by the MR.
Display information about MNs	**display mobile-ip node** [*ip-address* | **interface ethernet** *interface-number* | **virtual-network** *ip-address* | **brief**]	Available in any view
Clear statistics about MNs	**reset mobile-ip node-statistics** [*ip-address*]	Available in user view

17.5.3 MN Configuration Example

I. Network requirements

The network requirements are the same as those described in section 17.2.2 I. "Network requirements".

II. Configuration procedure

# Configure MN attributes on the HA, letting MNs with IP addresses in the range of 200.1.1.2 through 200.1.2.10 belong to interface Ethernet 0/0/1.

```
<Quidway> system-view
[Quidway] mobile-ip node 200.1.1.2 200.1.2.10 interface ethernet 0/0/1
```

# Suppose MN 200.1.1.9 is an MR with mobile network 201.1.3.0, configure as follows.

```
[Quidway] mobile-ip home-agent mobile-router 1
[Quidway-HA-MobileRouter] ip address 200.1.1.9
[Quidway-HA-MobileRouter] mobile-network 201.1.3.0 255.255.255.0
```

17.6 MR Configuration

17.6.1 Configuration Prerequisites

For a device to provide MR service, you must perform MR configurations on it. You can perform MR configurations only on a device with MIP enabled and HA disabled.

17.6.2 Configuring MR

Table 17-5 Configure MR

Operation	Command…	Description
Enter system view	**system-view**	—
Enable the MIP function	**mobile-ip**	Required
Enable the MR function and enter MR view	**mobile-ip mobile-router**	Required
Configure the home address of the MR	**ip address** *ip-address* { *mask* | *mask-length* }	Required
Configure the HA of the MR	**home-agent ip-address** *ip-address*	Required
Enter the corresponding interface view	**interface** *interface-type interface-number*	—
Configure the roaming function for the interface	**mobile-ip mobile-router roam** [**priority** *value*]	Required
Exit to system view	**quit**	—

Operation	Command…	Description
Configure the mobile network for the MR to support	**mobile-network** { *interface-type interface-number* | *ip-address* { *mask* | *mask-length* } }	Optional If the HA also supports MR and you have configured the mobile network on the MR, the HA adds a route to the mobile network in its routing table, enabling the mobile network of the MR to communicate.
Configure MR registration lifetime	**register lifetime** *value*	Optional By default, the MR registration lifetime is 36,000 seconds.
Configure MR registration retransmission parameters	**register retransmit** { **initial** *initial-time* | **maximum** *max-time* | **retry** *number* }	Optional By default, the initial registration retransmission interval is one second, the maximum registration retransmission interval is 128 seconds, and the maximum number of registration retransmission attempts is five.
Configure the reverse tunneling function	**reverse-tunnel enable**	Optional By default, reverse tunneling is not enabled.
Configure the simultaneous binding function	**simultaneous-bindings enable**	Optional By default, simultaneous binding is not enabled.
Configure the packet encapsulation mode	**encapsulation gre**	Optional By default, the packet encapsulation mode is IP in IP.
Enter the corresponding interface view	**interface** *interface-type interface-number*	—

Operation	Command…	Description
Configure agent solicitation parameters	**mobile-ip mobile-router solicit** { **interval** *value* | **retransmit** { **initial** *value* | **maximum** *value* | **retry** *value* } }	Optional By default, the agent solicitation transmission interval is 600 seconds, the initial agent solicitation retransmission interval is 1,000 ms, the maximum agent solicitation retransmission interval is 4,000 ms, and the maximum number of agent solicitation retransmission attempts is five.
Specify an MR to use only a co-located care-of address to register and configure the default gateway for the MR to use when registering	**mobile-ip mobile-router ccoa only** **mobile-ip mobile-router ccoa gateway** *ip-address*	Optional By default, an interface is neither specified to use only a co-located care-of address to register, nor configured with a default gateway address.
Display information about an MR	**display mobile-ip mobile-router**	Available in any view

17.6.3 MR Configuration Example

I. Network requirements

Enable MIP on three AR46 routers, setting them as HA, FA and MR respectively. The MR can communicate with its CN when it is on a foreign network.

II. Network diagram

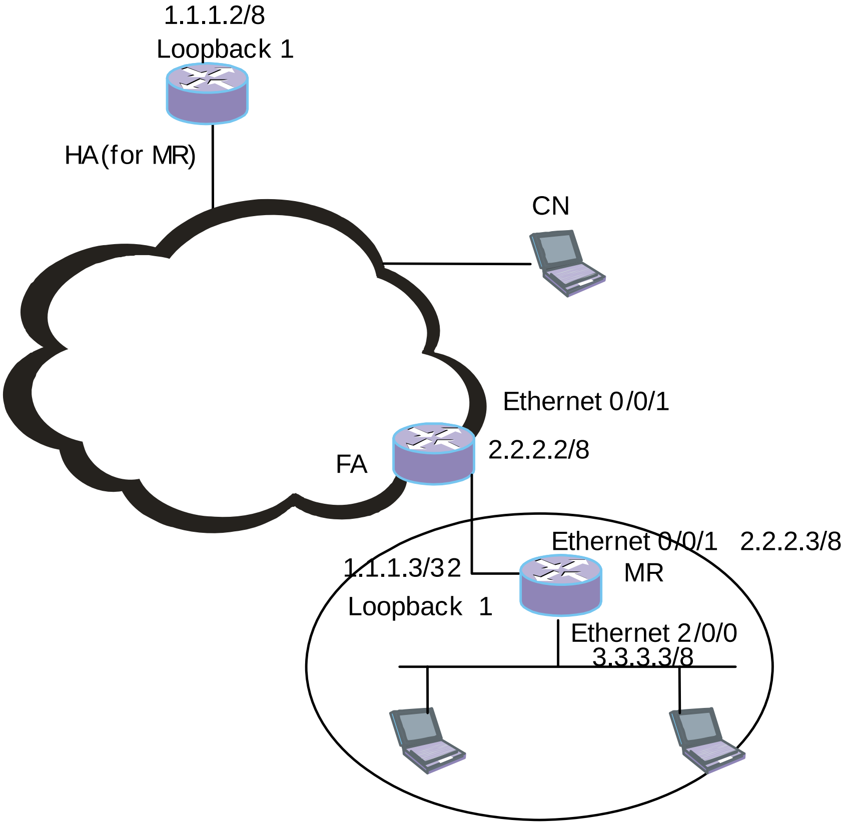


Figure 17-3 MR configuration

III. Configuration procedure

# Enable MIP .

```
[Quidway] mobile-ip
```

# Enable MR function.

```
[Quidway] mobile-ip mobile-router
```

# Configure MR home address.

```
[Quidway-MobileRouter] ip address 1.1.1.3 255.0.0.0
```

# Configure HA.

```
[Quidway-MobileRouter] home-agent ip-address 1.1.1.2
```

v# Configure the mobile network.

```
[Quidway-MobileRouter] mobile-network ethernet 2/0/0
```

Or

```
[Quidway-MobileRouter] mobile-network 3.3.3.3 255.0.0.0
```

# Configure an IP address on interface loopback1, which is the home address of the MR.

```
[Quidway] interface LoopBack1
[Quidway-LoopBack1] ip address 1.1.1.3 255.255.255.255
```

# Configure the roaming function on interface Ethernet2/0/0.

```
[Quidway] interface ethernet2/0/0
[Quidway-Ethernet2/0/0] ip address 3.3.3.3 255.0.0.0
[Quidway-Ethernet2/0/0] mobile-ip mobile-router roam
```

17.7 MIP Security Policy Configuration

17.7.1 Configuration Prerequisites

You can configure mobility security associations between mobile hosts, HAs, and FAs to enhance security in MN registration.

- For a device providing HA service, you must configure MN-HA security associations and can optionally configure FA-HA security associations.
- For a device providing FA service, you can optionally configure MN-FA security associations and HA-FA security associations.
- You can perform MIP security policy configurations only on a device with MIP enabled.
- For a device providing MR service, you must configure the MR-HA security associations and can optionally configure MR-FA security associations.

17.7.2 Configuring MIP Security Policies

Table 17-6 Configure MIP security policies

Operation	Command	Description
Enter system view	**system-view**	—
Enable the MIP function	**mobile-ip**	Required
Configure MIP security associations	**mobile-ip secure** { **home-agent** { **host** | **foreign-agent** } | **foreign-agent** { **visitor** | **home-agent** } | **mobile-router** { **home-agent** | **foreign-agent** } } *low-addr* [*up-addr*] **spi** *spi* **key** *string*	Required MN-HA security associations are required for a device providing HA service, and MR-HA security associations are required for a device providing MR service. Other types of security associations are optional.
Display MN security violation information logged by the mobility agent	**display mobile-ip violation** [*ip-address*]	Available in any view

Operation	Command	Description
Display information about MIP security associations	**display mobile-ip secure** { **home-agent** { **host** | **foreign-agent** } | **foreign-agent** { **visitor** | **home-agent** } | **mobile-router** { **home-agent** | **foreign-agent** } } [*ip-address*]	

Note:

Before configuring the security association between HA and MR, you must specify the MR address on the HA. For related configuration, refer to section 17.5 "MN Configuration".

17.7.3 MIP Security Policy Configuration Example

I. Network requirements

The network requirements are the same as those described in section 17.6.3 "MR Configuration Example".

II. Configuration procedure

# Configure an HA-MN security association on the HA.

```
<Quidway> system-view
[Quidway] mobile-ip secure home-agent host 1.1.1.3 spi 123 key abc
```

# Configure an MR-HA security association on the MR.

```
<Quidway> system-view
[Quidway] mobile-ip secure mobile-router home-agent 1.1.1.2 spi 123 key abc
```

# Configure an HA-FA security association on the HA. (Optional)

```
<Quidway> system-view
[Quidway] mobile-ip secure home-agent foreign-agent 2.2.2.2 spi 123 key abc
```

# Configure an FA-MN security association on the FA. (Optional)

```
<Quidway> system-view
[Quidway] mobile-ip secure foreign-agent visitor 1.1.1.3 spi 123 key abc
```

# Configure an FA-HA security association on the FA. (Optional)

```
<Quidway> system-view
[Quidway] mobile-ip secure foreign-agent home-agent 1.1.1.2 spi 123 key abc
```

# Configure an MR-FA security association on the MR.

```
<Quidway> system-view
[Quidway] mobile-ip secure mobile-router foreign-agent  2.2.2.2 spi 123 key
abc
```

17.8 IRDP Configuration

17.8.1 Configuration Prerequisites

An FA or HA does not periodically send agent advertisements; it sends agent advertisements only when receiving agent solicitations from MNs. With IRDP (ICMP Router Discovery Protocol) enabled and the relevant attributes configured, however, an FA or HA periodically sends agent advertisements on the attached network through IRDP to advertise its presence.

You can enable IRDP and configure the relevant attributes only on a device with MIP enabled.

17.8.2 Configuring IRDP

Table 17-7 Configure IRDP

Operation	Command	Description
Enter system view	**system-view**	—
Enable the MIP function	**mobile-ip**	Required
Enable IRDP and configure the relevant parameters	**mobile-ip irdp** [**lifetime** *seconds*] [**max-interval** *seconds*] [**min-interval** *seconds*] [**multicast**]	Required
Display IRDP configuration information	**display mobile-ip irdp**	Available in any view

17.9 Displaying and Maintaining MIP

After completing the above configurations, you can execute the **display** commands in any view to display operation of MIP and verify your configuration.

You can also execute the **reset** command in user view to clear MIP statistics.

Table 17-8 Display and maintain MIP

Operation	Command	Description
Display global MIP information	**display mobile-ip globals**	Available in any view
Display all MIP statistics	**display mobile-ip statistics**	
Display information about MIP visitors	**display mobile-ip visitor** [**pending**] [*address* | **brief**]	
Display MIP information of an or all interfaces	**display mobile-ip interface** [**ethernet** *interface-number*]	
Display MN security violation information logged by the mobility agent	**display mobile-ip violation** [*address*]	
Display information about MIP security associations	**display mobile-ip secure** { **home-agent** { **host | foreign-agent** } | **foreign-agent** { **visitor | home-agent** } | **mobile-router** { **home-agent | foreign-agent** } } [*address*]	
Display IRDP configuration information	**display mobile-ip irdp**	
Display information about an MR	**display mobile-ip mobile-router** [**agent | registration | statistics**]	
Clear all MIP statistics	**reset mobile-ip statistics**	In user view
Clear MR information	**reset mobile-ip mobile-router** { **agent** [*agent-address*] | **registration** [*reg-address*] | **statistics** }	In user view

17.10 MIP Configuration Example

17.10.1 MIP Configuration with a Usual Home Network

I. Network requirements

Set two AR46 routers on the networks. Enable MIP on both routers, HA on one and FA on the other. Use a laptop as an MN, and allow it to move from its home network to another network. Use another laptop as the CN of the MN.

II. Network diagram

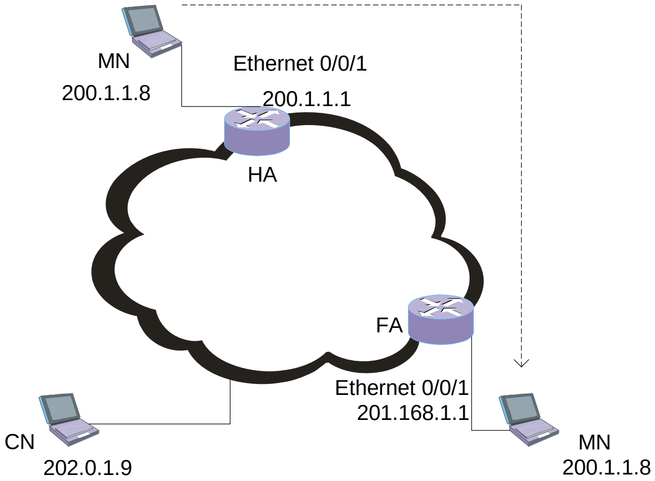


Figure 17-4 MIP configuration with a usual home network

III. Configuration procedure

1) Configure the HA

- Configure the general MIP policy

# Enable MIP.

```
<Quidway> system-view
[Quidway] mobile-ip
```

# Set the PMTU update policy. (Optional)

```
[Quidway] mobile-ip tunnel path-mtu-discovery
```

# Enable SNMP trap. (Optional)

```
[Quidway] snmp-agent trap enable mobile-ip
```

- Configure the HA policy

# Enable the HA function.

```
[Quidway] mobile-ip home-agent
```

- Configure the MN policy

# Configure MN attributes.

```
[Quidway] mobile-ip node 200.1.1.2  200.1.1.10 interface ethernet 0/0/1
```

- Configure the MIP security policy

# Configure an HA-MN security association.

```
[Quidway] mobile-ip secure home-agent host 200.1.1.2  200.1.1.10 spi 123 key
abc
```

# Configure an HA-FA security association. (Optional)

```
[Quidway] mobile-ip secure home-agent foreign-agent 201.168.1.1 spi 123 key
abc
```

2) Configure the FA

- Configure the general MIP policy

# Enable MIP.

```
<Quidway> system-view
[Quidway] mobile-ip
```

# Set the PMTU update policy. (Optional)

```
[Quidway] mobile-ip tunnel path-mtu-discovery
```

# Enable SNMP trap. (Optional)

```
[Quidway] snmp-agent trap enable mobile-ip
```

- Configure the MIP security policy (Optional)

# Configure an FA-MN security association.

```
[Quidway] mobile-ip secure foreign-agent visitor 200.1.1.2  200.1.1.10 spi
123 key abc
```

# Configure an FA-HA security association.

```
[Quidway] mobile-ip secure foreign-agent home-agent 200.1.1.1 spi 123 key abc
```

# Enable the FA function, setting the care-of interface.

```
[Quidway] mobile-ip foreign-agent care-of ethernet 0/0/1
```

# Enable the FA function on interface Ethernet 0/0/1.

```
[Quidway] interface ethernet 0/0/1
[Quidway-Ethernet0/0/1] mobile-ip foreign-agent service
```

# Enable prefix-length extension on interface Ethernet 0/0/1. (Optional)

```
[Quidway-Ethernet0/0/1] mobile-ip prefix-length
```

# Set registration lifetime on interface Ethernet 0/0/1. (Optional)

```
[Quidway-Ethernet0/0/1] mobile-ip registration-lifetime 38000
```

- Configure the MIP route advertisement policy (Optional)

# Enable IRDP on interface Ethernet 0/0/1.

```
[Quidway-Ethernet0/0/1] mobile-ip irdp
```

17.10.2 MIP Configuration with a Virtual Home Network

I. Network requirements

Enable MIP on three AR46 routers, setting one as HA, and the other two as FAs. A laptop functions as an MN. Its home network is a virtual network, and it is always roaming. Another laptop works as the CN of the MN. An MN of a virtual home network is always roaming.

II. Network diagram

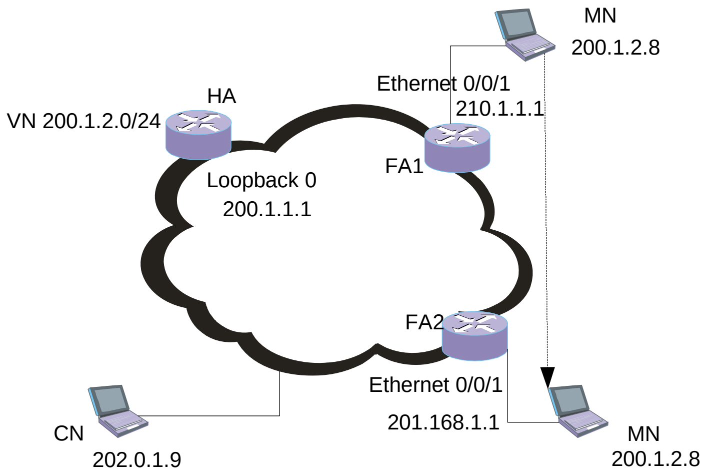


Figure 17-5 MIP configuration with a virtual home network

III. Configuration procedure

1) Configure the HA

- Configure the general MIP policy

# Enable MIP.

```
<Quidway> system-view
[Quidway] mobile-ip
```

# Set the PMTU update policy. (Optional)

```
[Quidway] mobile-ip tunnel path-mtu-discovery
```

- Configure the HA policy

# Enable the HA function, setting the HA address of the virtual network.

```
[Quidway] mobile-ip home-agent ha-virtual-net 200.1.2.1
```

# Define a logical interface and configure its IP address.

```
[Quidway] interface loopback 0
[Quidway-loopback0] ip address 200.1.2.1 255.255.255.0
```

# Define a virtual network, setting its HA address to the loopback address configured previously.

```
[Quidway-loopback0] quit
[Quidway] mobile-ip virtual-network 200.1.2.0 24 ha-address 200.1.2.1
```

- Configure the MN policy

# Configure MN attributes.

```
[Quidway] mobile-ip node 200.1.2.2  200.1.2.10 virtual-network 200.1.2.0 24
```

- Configure the MIP security policy

# Configure an HA-MN security association.

```
[Quidway] mobile-ip secure home-agent host 200.1.2.2  200.1.2.10 spi 123 key
abc
```

# Configure an HA-FA security association for FA1. (Optional)

```
[Quidway] mobile-ip secure home-agent foreign-agent 210.1.1.1 spi 123 key abc
```

# Configure an HA-FA security association for FA2. (Optional)

```
[Quidway] mobile-ip secure home-agent foreign-agent 201.168.1.1 spi 123 key
abc
```

2) Configure FA1

- Configure the general MIP policy

# Enable MIP.

```
<Quidway> system-view
[Quidway] mobile-ip
```

# Set the PMTU update policy. (Optional)

```
[Quidway]mobile-ip tunnel path-mtu-discovery
```

- Configure the MIP security policy (Optional)

# Configure an FA1-Visitor security association.

```
[Quidway] mobile-ip secure foreign-agent visitor 200.1.2.2  200.1.2.10 spi
123 key abc
```

# Configure an FA1-HA security association.

```
[Quidway] mobile-ip secure foreign-agent home-agent 200.1.1.1 spi 123 key abc
```

- Configure the FA policy

# Enable the FA function and configure the care-of address.

```
[Quidway] mobile-ip foreign-agent care-of ethernet 0/0/1
```

# Enable FA service on interface Ethernet 0/0/1.

```
[Quidway-Ethernet0/0/1] mobile-ip foreign-agent service
```

# Enable prefix-length extension on interface Ethernet 0/0/1. (Optional)

```
[Quidway-Ethernet0/0/1] mobile-ip prefix-length
```

# Set registration lifetime on interface Ethernet 0/0/1. (Optional)

```
[Quidway-Ethernet0/0/1] mobile-ip registration-lifetime 38000
```

- Configure the MIP route advertisement policy (Optional)

# Enable IRDP on interface Ethernet 0/0/1.

```
[Quidway-Ethernet0/0/1] mobile-ip irdp
```

3) Configure FA2

- Configure the general MIP policy

# Enable MIP.

```
<Quidway> system-view
[Quidway] mobile-ip
```

# Set the PMTU update policy. (Optional)

```
[Quidway]mobile-ip tunnel path-mtu-discovery
```

- Configure the MIP security policy (Optional)

# Configure an FA2-Visitor security association.

```
[Quidway] mobile-ip secure foreign-agent visitor 200.1.1.2  200.1.2.10 spi
123 key abc
```

# Configure an FA2-HA security association.

```
[Quidway] mobile-ip secure foreign-agent home-agent 200.1.1.1 spi 123 key abc
```

- Configure the FA policy

# Enable the FA function and configure the care-of address.

```
[Quidway] mobile-ip foreign-agent care-of ethernet 0/0/1
```

# Enable FA service on interface Ethernet 0/0/1.

```
[Quidway] interface ethernet0/0/1
[Quidway-Ethernet0/0/1] mobile-ip foreign-agent service
```

# Enable prefix-length extension on interface Ethernet 0/0/1. (Optional)

```
[Quidway-Ethernet0/0/1] mobile-ip prefix-length
```

# Set registration lifetime on interface Ethernet 0/0/1. (Optional)

```
[Quidway-Ethernet0/0/1] mobile-ip registration-lifetime 38000
```

- Configure the MIP route advertisement policy (Optional)

# Enable IRDP on interface Ethernet 0/0/1.

```
[Quidway-Ethernet0/0/1] mobile-ip irdp
```

17.10.3 MIP Configuration with an MR Using a Foreign Agent Care-Of Address

I. Network requirements

Enable MIP on four AR46 routers, setting them as HA, FA1, FA2 and MR respectively. The MR can roam across networks connected to FA1 and FA2 and use its fixed IP address 1.1.1.3 and a foreign agent care-of address to communicate with a CN.

II. Network diagram

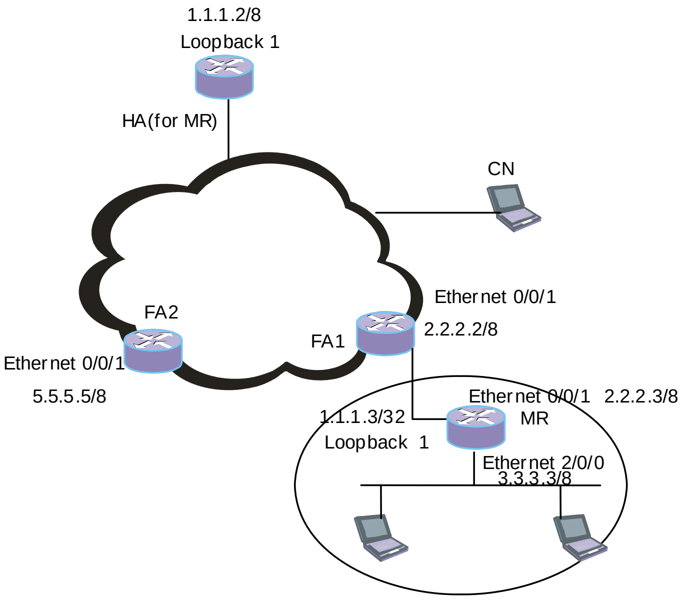


Figure 17-6 MIP configuration with an MR using a foreign agent care-of address

III. Configuration procedure

1) Configure the HA

- Configure the general MIP policy

# Enable MIP.

```
<Quidway> system-view
[Quidway] mobile-ip
```

# Set the PMTU update policy. (Optional)

```
[Quidway] mobile-ip tunnel path-mtu-discovery
```

- Configure the HA policy

# Enable the HA function.

```
[Quidway] mobile-ip home-agent
```

# Configure the virtual network.

```
[Quidway] mobile-ip virtual-network 1.0.0.0 255.0.0.0
```

# Define a logical interface and configure the IP address.

```
[Quidway] interface loopback 0
[Quidway-loopback0] ip address 1.1.1.2 255.255.255.255
```

# Define a virtual network, setting its HA address to the loopback address configured previously.

```
[Quidway-loopback0] quit
[Quidway] mobile-ip virtual-network 1.0.0.0 8 ha-address 1.1.1.2
```

- Configure the MN policy

# Configure MN attributes.

```
[Quidway] mobile-ip node 1.1.1.3 virtual-network 1.0.0.0 255.0.0.0
```

- Configure the MR and the corresponding mobile network.

```
[Quidway] mobile-ip home-agent mobile-router 1
[Quidway-HA-MobileRouter1] ip address 1.1.1.3
[Quidway-HA-MobileRouter1] mobile-network 3.0.0.0 255.0.0.0
[Quidway-HA-MobileRouter1] quit
```

- Configure the MIP security policy

# Configure an HA-MN security association.

```
[Quidway] mobile-ip secure home-agent host 1.1.1.3 spi 123 key abc
```

# Configure an HA-FA1 security association for FA1. (Optional)

```
[Quidway] mobile-ip secure home-agent foreign-agent 2.2.2.2 spi 123 key abc
```

# Configure an HA-FA2 security association for FA2. (Optional)

```
[Quidway] mobile-ip secure home-agent foreign-agent 5.5.5.5 spi 123 key abc
```

2) Configure FA1

- Configure the general MIP policy

# Enable MIP.

```
<Quidway> system-view
[Quidway] mobile-ip
```

# Set the PMTU update policy. (Optional)

```
[Quidway]mobile-ip tunnel path-mtu-discovery
```

- Configure the MIP security policy (Optional)

# Configure an FA1-Visitor security association.

```
[Quidway] mobile-ip secure foreign-agent visitor 1.1.1.3 spi 123 key abc
```

# Configure an FA1-HA security association.

```
[Quidway] mobile-ip secure foreign-agent home-agent 1.1.1.2 spi 123 key abc
```

- Configure the FA policy

# Enable the FA function and configure the care-of address.

```
[Quidway] mobile-ip foreign-agent care-of ethernet 0/0/1
```

# Enable FA service on interface Ethernet 0/0/1.

```
[Quidway] interface Ethernet0/0/1
[Quidway-Ethernet0/0/1] mobile-ip foreign-agent service
```

# Enable prefix-length extension on interface Ethernet 0/0/1. (Optional)

```
[Quidway-Ethernet0/0/1] mobile-ip prefix-length
```

# Set registration lifetime on interface Ethernet 0/0/1. (Optional)

```
[Quidway-Ethernet0/0/1] mobile-ip registration-lifetime 1600
```

- Configure the MIP route advertisement policy (Optional)

# Enable IRDP on interface Ethernet 0/0/1.

```
[Quidway-Ethernet0/0/1] mobile-ip irdp
```

3) Configure FA2

- Configure the general MIP policy

# Enable MIP.

```
<Quidway> system-view
[Quidway] mobile-ip
```

# Set the PMTU update policy. (Optional)

```
[Quidway] mobile-ip tunnel path-mtu-discovery
```

- Configure the MIP security policy (Optional)

# Configure an FA2-Visitor security association.

```
[Quidway] mobile-ip secure foreign-agent visitor 1.1.1.3 spi 123 key abc
```

# Configure an FA2-HA security association.

```
[Quidway] mobile-ip secure foreign-agent home-agent 1.1.1.2 spi 123 key abc
```

- Configure the FA policy

# Enable the FA function and configure the care-of address.

```
[Quidway] mobile-ip foreign-agent care-of ethernet 0/0/1
```

# Enable FA service on interface Ethernet 0/0/1.

```
[Quidway] interface ethernet 0/0/1
[Quidway-Ethernet0/0/1] mobile-ip foreign-agent service
```

# Enable prefix-length extension on interface Ethernet 0/0/1. (Optional)

```
[Quidway-Ethernet0/0/1] mobile-ip prefix-length
```

# Set registration lifetime on interface Ethernet 0/0/1. (Optional)

```
[Quidway-Ethernet0/0/1] mobile-ip registration-lifetime 1600
```

- Configure the MIP route advertisement policy (Optional)

# Enable IRDP on interface Ethernet 0/0/1.

```
[Quidway-Ethernet0/0/1] mobile-ip irdp
```

4) Configure the MR

# Enable MIP.

```
<Quidway> system-view
[Quidway] mobile-ip
```

# Enable the MR function.

```
[Quidway] mobile-ip mobile-router
```

# Configure the home address of the MR.

```
[Quidway-MobileRouter] ip address 1.1.1.3 255.0.0.0
```

# Configure the HA of the MR.

```
[Quidway-MobileRouter] home-agent ip-address 1.1.1.2
```

# Configure the mobile network.

```
[Quidway-MobileRouter] mobile-network ethernet 2/0/0
```

Or

```
[Quidway-MobileRouter] mobile-network 3.0.0.0 255.0.0.0
```

# Configure an IP address on interface loopback1, which is the home address of the MR.

```
[Quidway-MobileRouter] quit
[Quidway] interface loopback 1
[Quidway-LoopBack1] ip address 1.1.1.3 255.255.255.255
```

# Configure the roaming function.

```
[Quidway-LoopBack1] quit
[Quidway] interface ethernet 0/0/1
[Quidway-Ethernet0/0/1] ip address 2.2.2.3 255.0.0.0
[Quidway-Ethernet0/0/1] mobile-ip mobile-router roam
```

# Configure agent solicitation parameters. (Optional)

```
[Quidway-Ethernet0/0/1] mobile-ip mobile-router solicit interval 30
```

# Configure an MR-HA security association.

```
[Quidway-Ethernet0/0/1] quit
[Quidway] mobile-ip secure mobile-router home-agent 1.1.1.2 spi 123 key abc
```

# Configure an MR-FA security association for FA1. (Optional)

```
[Quidway] mobile-ip secure mobile-router foreign-agent 2.2.2.2 spi 123 key
abc
```

# Configure an MR-FA security association for FA2. (Optional)

```
[Quidway] mobile-ip secure mobile-router foreign-agent 5.5.5.5 spi 123 key
abc
```

17.10.4 MIP Configuration with an MR Using a Co-located Care-Of Address

I. Network requirements

Enable MIP on four AR46 routers, setting them as the HA, FA, MR, and a usual router respectively. The MR can roam across networks connected to FA1 and the usual router, using its fixed IP address 1.1.1.3 and a co-located care-of address obtained through DHCP to communicate with a CN.

II. Network diagram

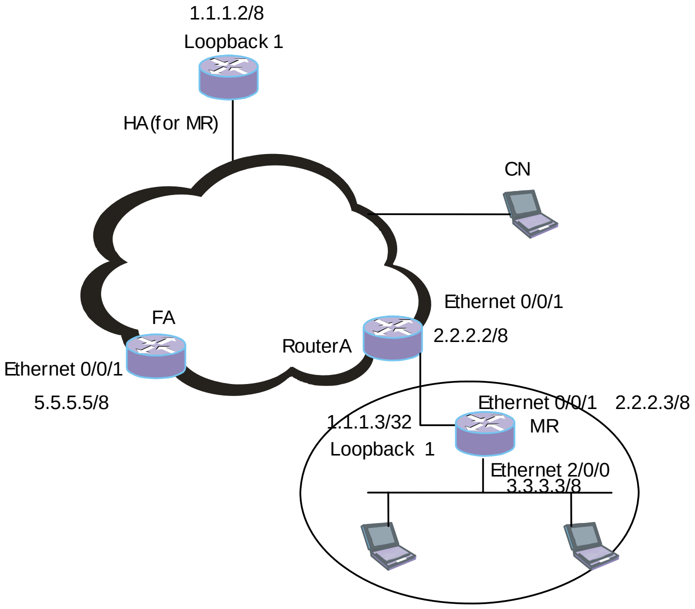


Figure 17-7 MIP configuration with an MR using a co-located care-of address

III. Configuration procedure

1) Configure the HA

- Configure the general MIP policy

# Enable MIP.

```
<Quidway> system-view
[Quidway] mobile-ip
```

# Set the PMTU update policy. (Optional)

```
[Quidway] mobile-ip tunnel path-mtu-discovery
```

- Configure the HA policy

# Enable the HA function.

```
[Quidway] mobile-ip home-agent
```

# Configure a virtual network.

```
[Quidway] mobile-ip virtual-network 1.0.0.0 255.0.0.0
```

# Define a logical interface and configure the IP address.

```
[Quidway] interface loopback 0
[Quidway-loopback0] ip address 1.1.1.2 255.255.255.255
```

# Define a virtual network, setting its HA address to the loopback address configured previously.

```
[Quidway-loopback0] quit
[Quidway] mobile-ip virtual-network 1.0.0.0 8 ha-address 1.1.1.2
```

- Configure the MN policy

# Configure MN attributes

```
[Quidway] mobile-ip node 1.1.1.3 virtual-network 1.0.0.0 255.0.0.0
```

- Configure the MR and the corresponding mobile network.

```
[Quidway] mobile-ip home-agent mobile-router 1
[Quidway-HA-MobileRouter1] ip address 1.1.1.3
[Quidway-HA-MobileRouter1] mobile-network 3.0.0.0 255.0.0.0
```

- Configure the MIP security policy

# Configure an HA-MN security association.

```
[Quidway] mobile-ip secure home-agent host 1.1.1.3 spi 123 key abc
```

# Configure an HA-FA security association. (Optional)

```
[Quidway] mobile-ip secure home-agent foreign-agent 5.5.5.5 spi 123 key abc
```

2) Configure RouterA

# Configure the DHCP server IP address pool and gateway.

```
<Quidway> system-view
[Quidway] dhcp server ip-pool abc
[Quidway-abc] network 2.0.0.0 mask 255.0.0.0
[Quidway-abc] gateway-list 2.2.2.2
```

# Configure the IP address of interface Ethernet 0/0/1.

```
[Quidway-Ethernet0/0/1] ip address 2.2.2.2 255.0.0.0
```

3) Configure the FA

- Configure the general MIP policy

# Enable MIP.

```
<Quidway> system-view
[Quidway] mobile-ip
```

# Set the PMTU update policy. (Optional)

```
[Quidway]mobile-ip tunnel path-mtu-discovery
```

- Configure the MIP security policy (Optional)

# Configure an FA-Visitor security association.

```
[Quidway] mobile-ip secure foreign-agent visitor 1.1.1.3 spi 123 key abc
```

# Configure an FA-HA security association.

```
[Quidway] mobile-ip secure foreign-agent home-agent 1.1.1.2 spi 123 key abc
```

- Configure the FA policy

# Enable the FA function and configure the care-of address.

```
[Quidway] mobile-ip foreign-agent care-of ethernet 0/0/1
```

# Enable FA service on interface Ethernet 0/0/1.

```
[Quidway-Ethernet0/0/1] mobile-ip foreign-agent service
```

# Enable prefix-length extension on interface Ethernet 0/0/1. (Optional)

```
[Quidway-Ethernet0/0/1] mobile-ip prefix-length
```

# Set registration lifetime on interface Ethernet 0/0/1. (Optional)

```
[Quidway-Ethernet0/0/1] mobile-ip registration-lifetime 1600
```

- Configure the MIP route advertisement policy (Optional)

# Enable IRDP on interface Ethernet 0/0/1.

```
[Quidway] ethernet 0/0/1
[Quidway-Ethernet0/0/1] mobile-ip irdp
```

# Enable DHCP service on the FA, setting the DHCP server IP address pool and gateway.

```
[Quidway] dhcp ser ip-pool abc
[Quidway-abc] network 5.0.0.0 mask 255.0.0.0
[Quidway-abc] gateway-list 5.5.5.5
```

4) Configure the MR

# Enable MIP.

```
<Quidway> system-view
[Quidway] mobile-ip
```

# Enable the MR function.

```
[Quidway] mobile-ip mobile-router
```

# Configure the home address of the MR.

```
[Quidway-MobileRouter] ip address 1.1.1.3 255.0.0.0
```

# Configure the HA of the MR.

```
[Quidway-MobileRouter] home-agent ip-address 1.1.1.2
```

# Configure an IP address on interface loopback1, which is the home address of the MR.

```
[Quidway-MobileRouter] quit
[Quidway] interface loopback 1
[Quidway-LoopBack1] ip address 1.1.1.3 255.255.255.255
```

# Configure the roaming function.

```
[Quidway-Ethernet0/0/0] ip address dhcp-alloc
[Quidway-Ethernet0/0/0] mobile-ip mobile-router roam
```

# Configure agent solicitation parameters. (Optional)

```
[Quidway-Ethernet0/0/0] mobile-ip mobile-router solicit interval 30
```

# Configure an MR-HA security association.

```
[Quidway] mobile-ip secure mobile-router home-agent 1.1.1.2 spi 123 key abc
```

# Configure an MR-FA security association. (Optional)

```
[Quidway] mobile-ip secure mobile-router foreign-agent 5.5.5.5 spi 123 key
abc
```

Chapter 18 QinQ Configuration

18.1 Introduction to QinQ

QinQ (802.1q in 802.1q) enables a packet of a customer network (private network) to go through the backbone network (public network) of the operator with two VLAN tags: the VLAN tag of the public network and that of the customer network, which is nested in the VLAN tag of the public network. In the public network, packets of this type are forwarded by their outer VLAN tags (that is, the VLAN tag of the public network) only, while the VLAN tag of the customer network remains untouched.

Figure 18-1 shows the structure of a packet with one VLAN tag.

6bytes	6bytes	4bytes	2bytes	0～1500 bytes	4bytes
DA	SA	User VLAN Tag	ETYPE	DATA	FCS

Figure 18-1 The structure of a packet with one VLAN tag

Figure 18-2 shows the structure of a packet with two VLAN tags.

6bytes	6bytes	4bytes	4bytes	2bytes	0～1500 bytes	4bytes
DA	SA	Nested VLAN Tag	User VLAN Tag	ETYPE	DATA	FCS

Figure 18-2 The structure of a packet with two VLAN tags

QinQ has the following features:

- It provides a simple way to implement layer-2 VPN tunnels.
- It can be implemented through static configurations, without the support of signaling protocols.

As QinQ is implemented on the trunk ports defined in 802.1q, 802.1q is required on all the devices involved. Thereby, QinQ is applicable to only small-sized enterprise networks with layer-3 switches as the backbone devices or small-sized metropolitan area network (MAN).

QinQ is mainly used to solve the following problems:

- Saves the public VLAN ID resource
- Enables customers to plan their own private network VLAN IDs, without running into conflicts with public network VLAN IDs.
- Provides a simple layer-2 VPN solution for small-sized MANs or enterprise networks.

To implement QinQ, configuration is required only on the access devices of the operator network. That is, QinQ is transparent to customer networks.

18.2 Configuring Outer VLAN Tag for QinQ

On QinQ-enabled bridge group interfaces, packets are processed as follows.

- Packets reaching these interfaces are tagged with an outer VLAN tag regardless of whether the packets are tagged.
- For packets to be forwarded through these interfaces, if the outer VLAN tag of a packet is the same as that configured for the interface, the outer VLAN tag of the packet is removed; otherwise, the packet is discarded.

18.2.1 Configuration Prerequisites

The devices support QinQ.

18.2.2 Configuring the Outer VLAN Tag

Table 18-1 Configure the outer VLAN tag

Operation	Command	Description
Enter system view	**system-view**	—
Enable the bridging function	**bridge enable**	Required By default, the bridging function is disabled.
Create a bridge group	**bridge** *bridge-set* **enable**	Required
Enter Ethernet interface view	**interface** *interface_type interface_num*	—
Add the interface to the bridge group	**bridge-set** *bridge-set*	Required
Enable QinQ.	**bridge qinq vid** *vlan-id*	Required By default, QinQ is disabled.

18.2.3 Outer VLAN Tag Configuration Examples

I. Network requirements

- Router A and Router B are QinQ-capable and are connected to the public network. Each of them has a LAN connected. A VLAN is created in the LANs of both sides. It is required that devices in the VLAN on both sides can communicate with one another through the bridging function.

- Packets to be sent from the VLAN on one side to the public network are tagged with the tag of VLAN 12 as the outer VLAN tags, and these packets are forwarded across the public network according to their outer VLAN tags, thus implementing layer-2 VPN.
- When packets tagged with the tag of VLAN 12 as the outer VLAN tags reach the other side of the public network, their outer VLAN tags are removed, and the packets are reinstated.

II. Network diagram

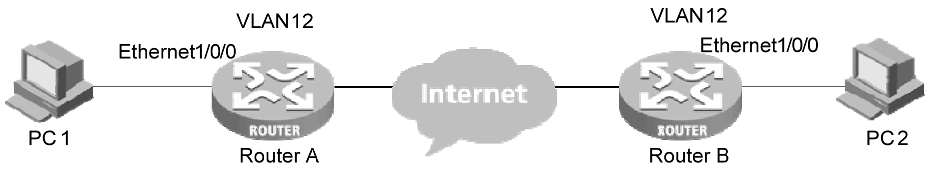


Figure 18-3 Network diagram for outer VLAN tag configuration

III. Configuration procedure

1) Configure Router A

# Enter system view.

```
<Router> system-view
```

# Enable the bridging function.

```
[Router] bridge enable
```

# Create a bridge group.

```
[Router] bridge 1 enable
```

# Enter Ethernet interface view.

```
[Router] interface ethernet 1/0/0
```

# Add Ethernet1/0/0 to bridge group 1.

```
[Router-Ethernet1/0/0] bridge-set 1
```

# Enable QinQ on Ethernet 1/0/0.

```
[Router-Ethernet1/0/0] bridge qinq vid 12
```

# Enable the VLAN ID transparent transmitting function on Ethernet 1/0/0.

```
[Router-Ethernet1/0/0] bridge vlanid-transparent-transmit enable
```

2) Configure Router B

The configuration on Router B is the same as that on Router A and is thus omitted.

📖 **Note:**

- With the above configurations performed, packets reaching Ethernet 1/0/0 are tagged with the tag of VLAN 12 as the outer VLAN tag. For packets to be forwarded through Ethernet 1/0/0 and with VLAN 12 tag as their outer VLAN tags, the outer VLAN tags are removed before they are forwarded; and those with their outer VLAN tags not being VLAN 12 tag are simply discarded.
- The VLAN ID transparent transmitting function is optional. You can enable it as required. For packets with inner VLAN tags, the VLAN ID transparent transmitting function is required to ensure the packets are transmitted properly in the customer network without changing their inner VLAN tags. Refer to the Link Layer Protocol part of this manual for information about the VLAN ID transparent transmitting function.
- This chapter only describes the outer VLAN tag configuration. Refer to the Link Layer Protocol part of this manual for information about bridging/bridge group configuration.

18.3 Configuring VLAN ID Dropping

18.3.1 Introduction to VLAN ID Dropping

The VLAN ID dropping function allows you to drop specific packets on the outgoing interfaces of a bridge group.

The VLAN ID dropping function processes packets as follows.

- For packets to be forwarded through layer-3 Ethernet sub-interfaces of a bridge group, those tagged with the tags of the VLANs of the sub-interfaces are forwarded, and others are discarded.
- For packets to be forwarded through the layer-3 primary Ethernet interface of a bridge group, those tagged with the tag of the VLAN of the sub-interface corresponding to the primary interface are discarded, and others are forwarded through the primary interface.
- For packets to be forwarded through virtual Ethernet interfaces of a bridge group, all the tagged packets are discarded. and only the untagged packets are forwarded.

📖 **Note:**

The VLAN ID transparent transmitting function cannot be enabled after the VLAN ID dropping function is enabled.

18.3.2 Configuring VLAN ID Dropping

I. Configuration prerequisites

The devices support the VLAN ID dropping function.

II. Configuring VLAN ID dropping

Table 18-2 Configure VLAN ID dropping

Operation	Command	Description
Enter system view	**system-view**	—
Enable the bridging function	**bridge enable**	Required By default, the bridging function is disabled.
Create a bridge group	**bridge** *bridge-set* **enable**	Required
Enter Ethernet interface view	**interface** *interface_type interface_num*	—
Add the interface to the bridge group	**bridge-set** *bridge-set*	Required
Enable the VLAN ID dropping function	**bridge vlanid-drop enable**	Required By default, the VLAN ID dropping function is disabled.

18.3.3 VLAN ID Dropping Configuration Example

I. Network requirements

Router A supports the bridging function. Configure Ethernet 1/0/0 to forward only the packets tagged with the tag of the VLAN configured on Ethernet 1/0/0. The VLAN ID dropping function is required to satisfy the requirement.

II. Network diagram

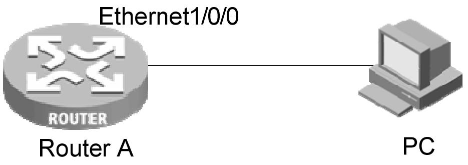


Figure 18-4 Network diagram for VLAN ID dropping configuration

III. Configuration procedure

# Enter system view.

```
<Router> system-view
```

# Enable the bridging function.

```
[Router] bridge enable
```

# Create a bridge group.

```
[Router] bridge 1 enable
```

# Enter Ethernet interface view.

```
[Router] interface Ethernet 1/0/0
```

# Add Ethernet 1/0/0 to bridge group 1.

```
[Router–Ethernet1/0/0] bridge-set 1
```

# Enable the VLAN ID dropping function on Ethernet 1/0/0.

```
[Router–Ethernet1/0/0] bridge vlanid-drop enable
```