

Table of Contents

Chapter 1 IP Address Configuration Commands.....	1-1
1.1 IP Address Configuration Commands.....	1-1
1.1.1 display ip host.....	1-1
1.1.2 display ip interface	1-1
1.1.3 ip address.....	1-2
1.1.4 ip host.....	1-4
Chapter 2 ARP Configuration Commands	2-1
2.1 ARP Configuration Commands.....	2-1
2.1.1 arp check enable	2-1
2.1.2 arp static.....	2-1
2.1.3 arp timer aging	2-3
2.1.4 debugging arp packet.....	2-3
2.1.5 display arp	2-4
2.1.6 display arp timer aging	2-5
2.1.7 reset arp	2-6
Chapter 3 Resilient ARP Configuration Commands.....	3-1
3.1.1 debugging resilient-arp.....	3-1
3.1.2 display resilient-arp	3-1
3.1.3 resilient-arp enable.....	3-2
3.1.4 resilient-arp interface vlan-interface	3-3
Chapter 4 BOOTP Client Configuration Commands.....	4-1
4.1.1 debugging dhcp irf xha.....	4-1
4.1.2 ip address bootp-alloc	4-1
Chapter 5 DHCP Configuration Commands	5-1
5.1 DHCP Client Configuration Commands.....	5-1
5.1.1 debugging dhcp client	5-1
5.1.2 debugging dhcp irf xha.....	5-1
5.1.3 display dhcp client.....	5-2
5.1.4 ip address dhcp-alloc	5-3
5.2 DHCP Relay Configuration Commands.....	5-3
5.2.1 address-check.....	5-3
5.2.2 debugging dhcp-relay.....	5-4
5.2.3 dhcp-security static.....	5-5
5.2.4 dhcp-security tracker	5-6
5.2.5 dhcp-server	5-7
5.2.6 dhcp-server ip.....	5-7

5.2.7 display dhcp-security	5-8
5.2.8 display dhcp-server	5-9
5.2.9 display dhcp-server interface vlan-interface	5-10
Chapter 6 Access Management Configuration Commands	6-1
6.1 Access Management Configuration Commands	6-1
6.1.1 am enable	6-1
6.1.2 am ip-pool	6-1
6.1.3 am trap enable	6-2
6.1.4 display am	6-3
6.1.5 display isolate port	6-4
6.1.6 port isolate	6-4
Chapter 7 UDP Helper Configuration Commands	7-1
7.1.1 debugging udp-helper	7-1
7.1.2 display udp-helper server	7-1
7.1.3 udp-helper enable	7-2
7.1.4 udp-helper port	7-2
7.1.5 udp-helper server	7-3
Chapter 8 IP Performance Configuration Commands	8-1
8.1 IP Performance Configuration Commands	8-1
8.1.1 display fib	8-1
8.1.2 display fib ip_address	8-2
8.1.3 display fib acl	8-3
8.1.4 display fib 	8-3
8.1.5 display fib ip-prefix	8-4
8.1.6 display fib statistics	8-4
8.1.7 display icmp statistics	8-5
8.1.8 display ip socket	8-6
8.1.9 display ip statistics	8-8
8.1.10 display tcp statistics	8-9
8.1.11 display tcp status	8-11
8.1.12 display udp statistics	8-11
8.1.13 reset ip statistics	8-12
8.1.14 reset tcp statistics	8-12
8.1.15 reset udp statistics	8-13
8.1.16 tcp timer fin-timeout	8-13
8.1.17 tcp timer syn-timeout	8-14
8.1.18 tcp window	8-15

Chapter 1 IP Address Configuration Commands

1.1 IP Address Configuration Commands

1.1.1 display ip host

Syntax

display ip host

View

Any view

Parameter

None

Description

Using **display ip host** command, you can view all the host names and the corresponding IP addresses.

Example

Display all hosts' name and corresponding IP address of the hosts.

```
<Quidway> display ip host
```

Host	Age	Flags	Address
My	0	static	1.1.1.1
Aa	0	static	2.2.2.4

1.1.2 display ip interface

Syntax

display ip interface [interface-type interface-number | brief]

View

Any view

Parameter

interface-type: Port type. *Interface-number*: Port number. See the description of the **interface** command for details.

brief: Brief summary of IP status and configuration.

Description

Using **display ip interface** command, you can view the information of an IP interface.

By default, the information about all the IP interfaces will be displayed if undo interface is specified. This command outputs all the information related to IP on the interface, which is useful for troubleshooting.

Example

Display the information related to interface VLAN-Interface 1.

```
<Quidway> display ip interface vlan-interface 1
Vlan-interfacel current state : DOWN
Line protocol current state : DOWN
Internet Address is 1.1.1.1/8 Primary
Broadcast address : 1.255.255.255
The Maximum Transmit Unit : 1500 bytes
input packets : 0, bytes : 0, multicasts : 0
output packets : 0, bytes : 0, multicasts : 0
TTL invalid packet number:          0
ICMP packet input number:           0
    Echo reply:                      0
    Unreachable:                     0
    Source quench:                   0
    Routing redirect:                0
    Echo request:                    0
    Router advert:                   0
    Router solicit:                  0
    Time exceed:                     0
    IP header bad:                   0
    Timestamp request:               0
    Timestamp reply:                 0
    Information request:              0
    Information reply:                0
    Netmask request:                 0
    Netmask reply:                   0
    Unknown type:                    0
```

1.1.3 ip address

Syntax

```
ip address ip-address { mask | mask-length } [ sub ]
undo ip address [ ip-address { mask | mask-length } [ sub ] ]
```

View

VLAN interface view or LoopBack interface view

Parameter

ip-address: IP address of VLAN interface.

mask: Corresponding subnet mask.

mask-length: Mask length, i.e. the length of "1" in the IP address.

sub: the secondary IP address of the VLAN interface or LoopBack interface.

Description

Using **ip address** command, you can configure an IP address for VLAN interface or LoopBack interface. Using **undo ip address** command, you can cancel an IP address of the VLAN interface or LoopBack interface.

By default, all interfaces' IP addresses are null.

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

- When you configure a primary IP address for an interface, which already has a primary IP address, the newly configured one will replace the old one.
- If you input **undo ip address** command without any parameter, the switch will delete both primary and secondary IP address of an interface. **undo ip address ip-address { mask | mask-length }** command can be used to delete the primary IP address, while **undo ip address ip-address { mask | mask-length } sub** command can be used to delete the secondary IP address.

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

For the related command, see **display ip interface**.

Example

Configure the IP address of interface VLAN interface 1 as 202.38.10.66 and subnet mask as 255.255.255.0.

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

```
System View: return to User View with Ctrl+Z.
```

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

```
[Quidway-vlan-interface1] ip address 202.38.10.66 255.255.255.0
```

1.1.4 ip host

Syntax

ip host *hostname ip-address*

undo ip host *hostname [ip-address]*

View

System view

Parameter

hostname: Name of the host, a character string consisting of 1 to 20 characters, including letters, numbers, or "_", and it must contain at least one letter.

ip-address: Host IP address (the corresponding IP address to the host name) in dotted decimal notation.

Description

Using **ip host** command, you can configure the host name and the host IP address. Using **undo ip host** command, you can cancel the host name and the host IP address.

By default, Host name and corresponding IP address are null.

For the related command, see **display ip host**.

Example

Set Lanswtich1's IP address to be 202.38.0.8.

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

```
System View: return to User View with Ctrl+Z.
```

```
[Quidway] ip host Lanswitch1 202.38.0.8
```

Chapter 2 ARP Configuration Commands

2.1 ARP Configuration Commands

2.1.1 arp check enable

Syntax

arp check enable
undo arp check enable

View

System view

Parameter

None

Description

Using **arp check enable** command, you can enable the checking of ARP entry, that is, the device does not learn the ARP entry where the MAC address is multicast MAC address. Using **undo arp check enable** command, you can disable the checking of ARP entry, that is, the device learns the ARP entry where the MAC address is multicast MAC address.

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

Example

Configure that the device learns the ARP entry where the MAC address is multicast MAC address.

```
<Quidway> system-view
System View: return to User View with Ctrl+Z.
[Quidway] undo arp check enable
```

2.1.2 arp static

Syntax

arp static *ip-address mac-address* [*vlan-id* { *interface-type interface-number* | *interface-name* }] (System view)

arp static *ip-address mac-address vlan-id* (Ethernet port view)

undo arp *ip-address* (System view or Ethernet port view)

View

System view or Ethernet port view

Parameter

ip-address: IP address of the ARP mapping entry.

mac-address: MAC address of ARP mapping entry, whose format is H-H-H (H indicates a hexadecimal number).

vlan-id: VLAN to which the static ARP entry belongs, which is in the range of 1 to 4094.

interface-name: Port to which the static ARP entry belong, represented with *interface-name*= *interface-type interface-number*. *interface-type* is port type and *interface-number* is port number. For details about *interface-type*, *interface-number* and *interface-name*, refer to the *Port Command Manual*.

Description

Using **arp static** command, you can configure the static ARP mapping entries in an ARP mapping table. Using **undo arp static** command, you can cancel a static ARP mapping entry from the ARP table

By default, the mapping table of the system ARP is empty and the switch can maintain its address mapping by means of dynamic ARP.

Note that:

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

For the related command, see **reset arp**, **display arp**, **debugging arp**.

Example

Associate the IP address 202.38.10.2 with the MAC address 00e0-fc01-0000, and the ARP mapping entry belongs to the Ethernet port GigabitEthernet1/0/1 on VLAN1.

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

```
System View: return to User View with Ctrl+Z.
```

```
[Quidway] arp static 202.38.0.10 00e0-fc01-0000 1 gigabitethernet1/0/1
```


2.1.3 arp timer aging

Syntax

arp timer aging *aging-time*

undo arp timer aging

View

System view

Parameter

aging-time: Aging time of dynamic ARP aging timer, which is in the range of 1 to 1440 minutes. By default, the aging time is 20 minutes.

Description

Using **arp timer aging** command, you can configure the dynamic ARP aging timer. Using **undo arp timer aging** command, you can restore the default dynamic ARP aging time.

For the related command, see **display arp timer aging**.

Example

Configure the dynamic ARP aging timer to 10 minutes.

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

```
System View: return to User View with Ctrl+Z.
```

```
[Quidway] arp timer aging 10
```

2.1.4 debugging arp packet

Syntax

debugging arp packet

undo debugging arp packet

View

User view

Parameter

None

Description

Using **debugging arp** command, you can enable ARP debugging. Using **undo debugging arp** command, you can disable the corresponding ARP debugging.

By default, undo ARP debugging is enabled.

For the related command, see **arp static**, **display arp**.

Example

Enable ARP packet debugging.

```
<Quidway> debugging arp packet
*0.771346-ARP-8-S1-arp_send:Send an ARP Packet, operation : 1,
sender_eth_addr :
00e0-fc00-3500, sender_ip_addr : 10.110.91.159, target_eth_addr :
0000-0000-0000
, target_ip_addr : 10.110.91.193
*0.771584-ARP-8-S1-arp_rcv:Receive an ARP Packet, operation : 2,
sender_eth_addr
: 0050-ba22-6fd7, sender_ip_addr : 10.110.91.193, target_eth_addr :
00e0-fc00-3
500, target_ip_addr : 10.110.91.159
```

Table 2-1 Description of the output information of the **debugging arp packet** command

Field	Description
operation	Kind of ARP packets: 1 ARP request packet; 2 ARP reply packet
sender_eth_addr	Ethernet address of the sender
sender_ip_addr	IP address of the sender
target_eth_addr	Target Ethernet address. If the packet is ARP request packet, the target IP address will be 0
target_ip_addr	Target IP address

2.1.5 display arp

Syntax

```
display arp [ ip-address | [ dynamic | static ] [ { begin | include | exclude } text ] ]
```

View

Any view

Parameter

dynamic: Display the dynamic ARP entries in ARP mapping table.

static: Display the static ARP entries in ARP mapping table.

ip-address: Display ARP mapping entries according to specified IP address.

begin: Start displaying from the first ARP entry that contains the specified character string “text”.

include: Display only the ARP entries that contain the specified character string “text”.

exclude: Display only the ARP entries that do not contain the specified character string “text”.

text: A character string. The ARP entries that contain this character string are displayed.

Description

Using **display arp** command, you can view the ARP mapping table.

For the related command, see **arp static**, **reset arp**, **debugging arp**.

Example

Display all the ARP entries.

```
<Quidway> display arp
                        Type: S-Static    D-Dynamic
IP Address            MAC Address        VLAN ID  Port Name            AgingType
10.1.1.2              00e0-fc01-0102    N/A      N/A                  N/A    S
10.110.91.175         0050-ba22-6fd7    1        GigabitEthernet1/0/1 20    D

---  2 entries found  ---
```

Table 2-2 Description of the output information of the **display arp** command

Field	Description
IP Address	IP address of the ARP mapping entry
MAC Address	MAC address of the ARP mapping entry
VLAN ID	VLAN to which the static ARP entry belongs
Port Name	Port to which the static ARP entry belongs
Aging	Aging time of dynamic ARP entry in minutes
Type	Type of ARP entry

2.1.6 display arp timer aging

Syntax

display arp timer aging

View

Any view

Parameter

vlan-id: VLAN interface ID.

Description

Using **display arp timer aging** command, you can view the current setting of the dynamic ARP map aging timer.

For the related command, see **arp timer aging**.

Example

Display the current setting of the ARP map aging timer.

```
<Quidway> display arp timer aging  
Current ARP aging time is 10 minute(s)
```

2.1.7 reset arp

Syntax

```
reset arp [ dynamic | static | interface { interface-type interface-number |  
interface-name } ]
```

View

User view

Parameter

dynamic: Clear the dynamic ARP mapping entries.

static: Clear the static ARP mapping entries

interface *interface-name*: Clear the ARP mapping entries that are related to the specified. port, represented with *interface-name*= *interface-type interface-number*. *interface-type* is port type and *interface-number* is port number. For details about *interface-type*, *interface-number* and *interface-name*, refer to the *Port Command Manual*.

Description

Using **reset arp** command, you can reset the ARP mapping entries.

For the related command, see **arp static**, **display arp**.

Example

Reset the static ARP entries.

```
<Quidway> reset arp static
```

Chapter 3 Resilient ARP Configuration Commands

3.1.1 debugging resilient-arp

Syntax

```
debugging resilient-arp { packet | state | error | all }  
undo debugging resilient-arp { packet | state | error | all }
```

View

User view

Parameter

packet: Enables debugging resilient ARP packets
state: Enables debugging resilient ARP state machine
error: Enables debugging resilient ARP errors (including packet errors)
all: Enables all resilient ARP debugging

Description

Using the **debugging resilient-arp** command, you can enable resilient ARP debugging. Using the **undo debugging resilient-arp** command, you can disable resilient ARP debugging.

By default, all resilient ARP debugging is disabled.

Example

```
# Enable debugging resilient ARP packets.  
<Qidway> debugging resilient-arp packet
```

3.1.2 display resilient-arp

Syntax

```
display resilient-arp [ unit unit-id ]
```

View

Any view

Parameter

unit-id: Unit ID, in the range of 1 to 8.

Description

Using the **display resilient-arp** command, you can view resilient ARP state information of the units, the resilient ARP packet-sending VLAN interfaces.

If no unit ID is specified, the system displays the resilient ARP state information of all units. Otherwise, the system only displays the resilient ARP state information of the designated units.

Example

Display resilient ARP state information of Unit 1.

```
<Quidway> display resilient-arp unit 1
```

```
The state of unit 1 is: L3Master
```

```
The sending interface(s):
```

```
Vlan-interface2
```

```
Vlan-interface1
```

3.1.3 resilient-arp enable

Syntax

resilient-arp enable

undo resilient-arp enable

View

System view

Parameter

None

Description

Using the **resilient-arp enable** command, you can enable resilient ARP function. Using the **undo resilient-arp enable** command, you can disable resilient ARP function.

By default, resilient ARP function is enabled.

For the related command, see **display resilient-arp**.

Example

Enable resilient ARP function.

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

```
System View: return to User View with Ctrl+Z.
```

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

3.1.4 resilient-arp interface vlan-interface

Syntax

```
resilient-arp interface vlan-interface vlan-id  
undo resilient-arp interface vlan-interface vlan-id
```

View

System view

Parameter

vlan-id: VLAN interface ID.

Description

Using the **resilient-arp interface vlan-interface** command, you can configure resilient ARP packet-sending VLAN interfaces. Using the **undo resilient-arp interface vlan-interface** command, you can delete such VLAN interface.

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

For the related command, see **display resilient-arp**.

Example

Set VLAN interface 2 to send resilient ARP packets.

```
<Quidway> system-view  
System View: return to User View with Ctrl+Z.  
[Quidway] resilient-arp interface vlan-interface 2
```

Chapter 4 BOOTP Client Configuration Commands

4.1.1 debugging dhcp irf xha

Syntax

```
debugging dhcp irf xha
undo debugging dhcp irf xha
```

View

User view

Parameter

None

Description

Using the **debugging dhcp irf xha** command, you can enable BOOTP client hot backup debugging. Using the **undo debugging dhcp irf xha** command, you can disable BOOTP client hot backup debugging.

By default, BOOTP client hot backup debugging is disabled.

Example

```
# Enable BOOTP client hot backup debugging.
<Quidway> debugging dhcp irf xha
```

4.1.2 ip address bootp-alloc

Syntax

```
ip address bootp-alloc
undo ip address bootp-alloc
```

View

VLAN interface view

Parameter

None

Description

Using the **ip address bootp-alloc** command, you can configure VLAN interface to obtain IP address using BOOTP. Using the **undo ip address bootp-alloc** command, you can remove the configuration.

By default, the VLAN interface does not obtain IP address using BOOTP.

For the related command, see **display bootp client**.

Example

Configure VLAN interface 1 to obtain IP address using BOOTP.

```
<Quidway> system-view
System View: return to User View with Ctrl+Z.
[Quidway] interface vlan-interface 1
[Quidway-Vlan-interface1] ip address bootp-alloc
```

Chapter 5 DHCP Configuration Commands

5.1 DHCP Client Configuration Commands

5.1.1 debugging dhcp client

Syntax

```
debugging dhcp client { all | error | event | packet }  
undo debugging dhcp client { all | error | event | packet }
```

View

User view

Parameter

all: All DHCP client debugging.

error: DHCP client error (including packet unrecognizable) debugging.

event: DHCP client event (including address allocation and data update) debugging.

packet: DHCP client packet debugging.

Description

Using the **debugging dhcp client** command, you can enable DHCP client debugging.
Using the **undo debugging dhcp client** command, you can disable DHCP client debugging.

By default, all DHCP client debugging is disabled.

Example

```
# Enable DHCP client event debugging.  
<Quidway> debugging dhcp client event
```

5.1.2 debugging dhcp irf xha

Syntax

```
debugging dhcp irf xha  
undo debugging dhcp irf xha
```

View

User view

Parameter

None

Description

Using the **debugging dhcp irf xha** command, you can enable DHCP client hot backup debugging. Using the **undo debugging dhcp irf xha** command, you can disable DHCP client hot backup debugging.

By default, DHCP client hot backup debugging is disabled.

Example

Enable DHCP client hot backup debugging.

```
<Quidway> debugging dhcp irf xha
```

5.1.3 display dhcp client

Syntax

display dhcp client [verbose]

View

Any view

Parameter

verbose: Displays detailed information about address allocation at DHCP client.

Description

Using the **display dhcp client** command, you can view detailed information about address allocation at DHCP client.

Example

Display detailed information about address allocation at DHCP client.

```
<Quidway> display dhcp client verbose
DHCP client statistic information:
Vlan-interface1:
Current machine state: BOUND
Alloced IP: 169.254.0.2 255.255.0.0
Alloced lease: 86400 seconds, T1: 43200 seconds, T2: 75600 seconds
Lease from 2002.09.20 01:05:03 to 2002.09.21 01:05:03
Server IP: 169.254.0.1
Transaction ID = 0x3d8a7431
Default router: 2.2.2.2
DNS server: 1.1.1.1
```

```
Domain name: huawei.com
Client ID: HUAWEI-00e0.fc0a.c3ef-Ethernet0/0
Next timeout will happen after 0 days 11 hours 56 minutes 1 seconds.
```

5.1.4 ip address dhcp-alloc

Syntax

```
ip address dhcp-alloc
undo ip address dhcp-alloc
```

View

VLAN interface view

Parameter

None

Description

Using the **ip address dhcp-alloc** command, you can configure VLAN interface to obtain IP address using DHCP. Using the **undo ip address dhcp-alloc** command, you can remove the configuration.

By default, the VLAN interface does not obtain IP address using DHCP.

Example

Configure VLAN interface to obtain IP address using DHCP.

```
<Quidway> system-view
System View: return to User View with Ctrl+Z.
[Quidway] interface vlan-interface 1
[Quidway-Vlan-interface1] ip address dhcp-alloc
```

5.2 DHCP Relay Configuration Commands

5.2.1 address-check

Syntax

```
address-check enable
address-check disable
```

View

VLAN interface view

Parameter

None

Description

Using the **address-check enable** command, you can enable DHCP relay security feature to check address validity for VLAN interface users. Using the **address-check disable** command, you can disable DHCP relay security feature.

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

Example

Enable DHCP security feature on VLAN interface 1.

```
<Quidway> system-view
System View: return to User View with Ctrl+Z.
[Quidway] interface vlan-interface 1
[Quidway-Vlan-interface1] address-check enable
```

5.2.2 debugging dhcp-relay

Syntax

debugging dhcp-relay

undo debugging dhcp-relay

View

User view

Parameter

None

Description

Using the **debugging dhcp-relay** command, you can enable DHCP relay debugging. Using the **undo debugging dhcp-relay** command, you can disable DHCP relay debugging.

By default, DHCP relay debugging is disabled.

For the related commands, see **dhcp-server ip**, **dhcp-server**, **display dhcp-server** and **display dhcp-server interface vlan-interface**.

Example

Enable DHCP relay debugging.

```
<Quidway> debugging dhcp-relay
*0.7200205-DHCP-8-dhcp_debug:
```

```
From client to server:
Interface: VLAN-Interface 1
ServerGroupNo: 0
Type: dhcp-request
ClientHardAddress: 0010-dc19-695d
      ServerIpAddress: 192.168.1.2

*0.7200230-DHCP-8-dhcp_debug:
From server to client:
Interface: VLAN-Interface 1
ServerGroupNo: 0
Type: dhcp-ack
ClientHardAddress: 0010-dc19-695d
      AllocatedIpAddress: 10.1.1.1

*0.7200580-DHCP-8-largehop:
Discard DHCP request packet because of too large hop count!

*0.7200725-DHCP-8-invalidpkt:
Wrong DHCP packet!
```

5.2.3 dhcp-security static

Syntax

```
dhcp-security static ip_address mac_address
undo dhcp-security { ip_address | all | dynamic | static }
```

View

System view

Parameter

ip_address: User IP address.

mac_address: User MAC address.

all: Deletes all user address entries.

dynamic: Deletes dynamic user address entries.

static: Deletes static user address entries.

Description

Using the **dhcp-security static** command, you can configure user address entries for the DHCP server group. Using the **undo dhcp-security** command, you can delete the user address entries.

For the related command, see **display dhcp-security**.

Example

Address a user address entry for DHCP server group, with IP 1.1.1.1 and MAC address 0005-5D02-F2B3.

```
<Quidway> system-view
System View: return to User View with Ctrl+Z.
[Quidway] dhcp-security static 1.1.1.1 0005-5D02-F2B3
```

5.2.4 dhcp-security tracker

Syntax

dhcp-security tracker { *interval* | **auto** }
undo dhcp-security tracker [*interval*]

View

System

Parameter

Interval: Time interval to update DHCP security entries, in the range of 1 to 120 seconds.

auto: DHCP security entries are updated automatically.

Description

Using the **dhcp-security tracker** command, you can define the time interval to update DHCP security entries. Using the **undo dhcp-security tracker** command, you can remove the configuration.

DHCP security entries are those in the dhcp-security table, which records the mapping of between dynamic IP addresses and MAC addresses on the DHCP relay and the mapping between the user-defined static IP addresses and MAC addresses. Regular update is required if there are dynamic IP entries in the dhcp-security table. A long interval is recommended to avoid severe impact on DHCP server by the switch if there are a large number of dynamic entries in the dhcp-security table.

You can also choose **auto** for the update mode of dynamic entries, and then the switch shall adjust the update interval depending on the number of the entries in the dhcp-security table. If no dynamic entries still exist in the dhcp-security table, the switch shall terminate automatic entry update.

Example

Define the time interval to update DHCP security entries to 60 seconds.

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

System View: return to User View with Ctrl+Z.

[Quidway] dhcp-security tracker 60

5.2.5 dhcp-server

Syntax

dhcp-server *groupNo*

undo dhcp-server

View

VLAN interface view

Parameter

groupNo: DHCP server group number, in the range of 0 to 19.

Description

Using the **dhcp-server** command, you can configure corresponding DHCP Server Group of the designate VLAN Interface. Using the **undo dhcp-server** command, you can remove the configuration.

For the related commands, see **dhcp-server ip**, **display dhcp-server**, **display dhcp-server interface vlan-interface** and **debugging dhcp-relay**.

Example

Configure VLAN interface 1 to belong to DHCP server group 1.

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

System View: return to User View with Ctrl+Z.

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

```
[Quidway-Vlan-interface1] dhcp-server 1
```

5.2.6 dhcp-server ip

Syntax

dhcp-server *groupNo* **ip** *ip_address1* [*ip_address2*]

undo dhcp-server *groupNo*

View

System view

Parameter

groupNo: DHCP server group number, in the range of 0 to 19.

ip_address1: IP address of the server1 in the group.

ip_address2: IP address of the server2 in the group.

Description

Using the **dhcp-server ip** command, you can configure IP address for the DHCP servers in the DHCP server group. Using the **undo dhcp-server** command, you can delete all IP addresses of the DHCP servers in the DHCP server group.

You can first view the configuration information of DHCP server group with the **display dhcp-server** command, and then configure or delete the IP addresses of the DHCP servers in the DHCP server group.

For the related command, see **dhcp-server**, **display dhcp-server** and **debugging dhcp-relay**.

Example

Configure the IP addresses of the server1 and server2 in DHCP server group 1 respectively as 1.1.1.1 and 2.2.2.2.

```
<Quidway> system-view
System View: return to User View with Ctrl+Z.
[Quidway] dhcp-server 1 ip 1.1.1.1 2.2.2.2
```

5.2.7 display dhcp-security

Syntax

display dhcp-security [*ip_address* | **dynamic** | **static** | **tracker**] [**unit** *unit-id*]

View

Any view

Parameter

ip_address: Display user address entries of the specified IP address.

dynamic: Display dynamic user address entries.

static: Display static user address entries.

tracker: Display the refresh interval of the DHCP security entries.

unit *unit-id*: Display user address entries of the specified unit ID, ranging from 1 to 8.

Description

Using the **display dhcp-security** command, you can view all valid use address information of the DHCP server group.

Example

Display all valid use address information of the DHCP server group.

```
<Quidway> display dhcp-security
Unit ID      IP Address      MAC Address      IP Address Type
1            2.2.2.3         0005-5d02-f2b2   Static
1            3.3.3.3         0005-5d02-f2b3   Dynamic
--- 2 dhcp-security item(s) of unit 1 found ---
```

5.2.8 display dhcp-server

Syntax

display dhcp-server *groupNo*

View

Any view

Parameter

groupNo: DHCP server group number, in the range of 0 to 19.

Description

Using the **display dhcp-server** command, you can view the information about DHCP server group.

For the related commands, see **dhcp-server ip**, **dhcp-server**, **display dhcp-server interface vlan-interface** and **debugging dhcp-relay**.

Example

Display the information about DHCP server group 0.

```
<Quidway> display dhcp-server 0
The first IP address of DHCP server group 0:      1.1.1.1
The second IP address of DHCP server group 0:     1.1.1.2
Messages from this server group: 0
Messages to this server group: 0
Messages from clients to this server group: 0
Messages from this server group to clients: 0
DHCP_OFFER messages: 0
DHCP_ACK messages: 0
DHCP_NAK messages: 0
DHCP_DECLINE messages: 0
DHCP_DISCOVER messages: 0
DHCP_REQUEST messages: 0
DHCP_INFORM messages: 0
DHCP_RELEASE messages: 0
BOOTP_REQUEST messages: 0
BOOTP_REPLY messages: 0
```

5.2.9 display dhcp-server interface vlan-interface

Syntax

display dhcp-server interface vlan-interface *vlan-id*

View

Any view

Parameter

vlan-id: VLAN interface ID.

Description

Using the **display dhcp-server interface vlan-interface** command, you can view the information about the DHCP server group corresponding to the VLAN interface.

For the related commands, see **dhcp-server**, **display dhcp-server** and **debugging dhcp-relay**.

Example

Display the information about the DHCP server group corresponding to the VLAN interface 2.

```
<Quidway> display dhcp-server interface vlan-interface 2  
The DHCP server group of this interface is 0
```

Chapter 6 Access Management Configuration Commands

6.1 Access Management Configuration Commands

6.1.1 am enable

Syntax

am enable
undo am enable

View

System view

Parameter

None

Description

Using **am enable** command, you can enable the access management function. Using **undo am enable** command, you can disable the function.

By default, Access management function disabled.

When using the access management function, It is recommended to cancel the static ARP configuration to ensure that the binding of IP address and Ethernet switch take effect. If you have configured the static ARP for an IP address in the current port IP address pool from some other port, the system will prompt to cancel the static ARP setting.

Example

Enable the access management function.

```
<Quidway> system-view  
System View: return to User View with Ctrl+Z.  
[Quidway] am enable
```

6.1.2 am ip-pool

Syntax

am ip-pool *address-list*

undo am ip-pool { all | *address-list* }

View

Ethernet port view

Parameter

all: Configures to operate on all the IP addresses (or IP address pools).

ip-pool: Configures IP address pool for access management.

address-list: Specifies IP address list in the *start_ip_address* [*ip_address_num*] & < 1-10 > format. *start_ip_address* is the start address of an IP address range in the pool. *ip_address_num* specifies how many IP addresses following *start_ip_address* in the range. & < 1-10 > means you can specify ten IP address ranges at most.

Description

Using **am ip-pool** command, you can configure the IP address pool for access management on a port. The packet whose source IP address is in the specified pool is allowed to be forwarded on Layer 3 via the port of the switch. Using **undo am ip-pool** command, you can cancel the access management IP pool of the port.

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

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

Example

Configure the access management IP address pool on GigabitEthernet1/0/1 and permits the addresses from 202.112.66.2 through 202.112.66.20 and the specified 202.112.65.1 to access the port.

```
<Quidway> system-view
System View: return to User View with Ctrl+Z.
[Quidway] interface gigabitethernet1/0/1
[Quidway-GigabitEthernet1/0/1] am ip-pool 202.112.66.2 19 202.112.65.1
```

6.1.3 am trap enable

Syntax

am trap enable

undo am trap enable

View

System view

Parameter

None

Description

Using **am trap enable** command, you can enable the access management trap function. Using **undo am trap enable** command, you can disable the access management trap function.

By default, the access management trap disabled.

Example

Enable the access management trap.

```
<Quidway> system-view
System View: return to User View with Ctrl+Z.
[Quidway] am trap enable
```

6.1.4 display am

Syntax

display am [*interface-list*]

View

Any view

Parameter

interface-list: Display the access management information of the specified port, in the { { *interface-type interface-number* | *interface-name* } [**to** { *interface-type interface-number* | *interface-name* }] } &<1-10> format. *interface-name*: Specified the port name, represented with *interface-name*= *interface-type interface-number*. *interface-type* is port type and *interface-number* is port number. For details about *interface-type*, *interface-number* and *interface-name*, refer to the *Port Command Manual*. &<1-10> indicates the preceding parameter can be input up to 10 times.

Description

Using **display am** command, you can view the status of access management function and configuration of IP address pool.

If no port is specified, the access management configurations of all the ports are displayed.

Example

Display the access management configurations on GigabitEthernet1/0/1.

```
<Quidway> display am gigabitethernet1/0/1
```

```
GigabitEthernet1/0/1
  Status      : disabled
  IP Pools    : (NULL)
```

Table 6-1 Description of output information of the **display am** command

Field	Description
Status	AM state on the port: enabled or disabled
IP Pools	IP pools. NULL represents no configuration. Each IP address section is represented in X.X.X.X (number), of these, "X.X.X.X" represents the first address, and "number" represents that "number" consecutive IP addresses from the beginning of this address are within the IP pools

6.1.5 display isolate port

Syntax

display isolate port

View

Any view

Parameter

None

Description

Using **display isolate port** command, you can view port isolation information.

Example

```
# Display port isolation information.
<Quidway> display isolate port
Isolated port(s) on UNIT 1:
  GigabitEthernet1/0/1
```

6.1.6 port isolate

Syntax

port isolate
undo port isolate

View

Ethernet port view

Parameter

None

Description

Using **port isolate** command, you can add a port to an isolation group using the following commands, and achieves port-to-port isolation between this port and other ports of this group, that is, Layer 2 forwarding between the isolated ports is not available. Using **undo port isolate** command, you can remove a port from an isolation group.

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

Example

Add GigabitEthernet1/0/1 and GigabitEthernet1/0/2 to isolation group.

```
<Quidway> system-view
System View: return to User View with Ctrl+Z.
[Quidway] interface gigaethernet1/0/1
[Quidway-GigabitEthernet1/0/1] port isolate
[Quidway-GigabitEthernet1/0/1] quit
[Quidway] interface gigaethernet1/0/2
[Quidway-GigabitEthernet1/0/2] port isolate
```


Chapter 7 UDP Helper Configuration Commands

7.1.1 debugging udp-helper

Syntax

```
debugging udp-helper { event | packet [ receive | send ] }  
undo debugging udp-helper { event | packet [ receive | send ] }
```

View

User view

Parameter

event: UDP Helper event debugging.
packet: UDP Helper packet debugging.
receive: UDP Helper inbound packet debugging.
send: UDP Helper outbound packet debugging.

Description

Using the **debugging udp-helper** command, you can enable UDP Helper debugging.
Using the **undo debugging udp-helper** command, you can disable UDP Helper debugging.

By default, UDP Helper debugging is disabled.

Example

```
# Enable UDP Helper packet debugging.  
<Quidway> debugging udp-helper packet
```

7.1.2 display udp-helper server

Syntax

```
display udp-helper server [ interface vlan-interface vlan-id ]
```

View

Any view

Parameter

vlan-id: VLAN interface ID.

Description

Using the **display udp-helper server** command, you can view the information of destination Helper server corresponding to the VLAN interface.

Example

Display the information of destination Helper server corresponding to the VLAN interface 1.

```
<Quidway> display udp-helper server interface vlan-interface 1
interface name      server address      packets send
Vlan-interface1    192.1.1.2          0
```

7.1.3 udp-helper enable

Syntax

```
udp-helper enable
undo udp-helper enable
```

View

System view

Parameter

None

Description

Using the **udp-helper enable** command, you can enable relay of UDP broadcast packets. Using the **undo udp-helper enable** command, you can disable this function.

By default, relay of UDP broadcast packets is not enabled.

Example

Enable UDP Helper function.

```
<Quidway> system-view
System View: return to User View with Ctrl+Z.
[Quidway] udp-helper enable
```

7.1.4 udp-helper port

Syntax

```
udp-helper port { port | dns | netbios-ds | netbios-ns | tacacs | tftp | time }
undo udp-helper port { port | dns | netbios-ds | netbios-ns | tacacs | tftp | time }
```

View

System view

Parameter

port: ID of the UDP port with relay function to be enabled, in the range of 1 to 65535.

dns: Domain name System, corresponding to UDP port 53.

netbios-ds: NetBios datagram service, corresponding to UDP port 138.

netbios-ns: NetBios name service, corresponding to UDP port 137.

tacacs: TAC access control system, corresponding to UDP port 49.

tftp: Trivial file transfer protocol, corresponding to UDP port 69.

time: Time service, corresponding to UDP port 37.

Description

Using the **udp-helper port** command, you can configure the UDP port with relay function. Using the **undo udp-helper port** command, you can remove the configuration.

Example

Configure the UDP port with relay function as the UDP port corresponding to DNS.

```
<Quidway> system-view
System View: return to User View with Ctrl+Z.
[Quidway] udp-helper port dns
```

7.1.5 udp-helper server

Syntax

udp-helper server *ip-address*

undo udp-helper server [*ip-address*]

View

VLAN interface view

Parameter

ip-address: IP address of the destination server, in dotted decimal format.

Description

Using the **udp-helper server** command, you can configure the relay destination server for UDP broadcast packets. Using the **undo udp-helper server** command, you can delete the relay destination server.

By default, no relay destination server is configured.

For the related command, see **display udp-helper server**.

Example

Configure the relay destination server with IP address 192.1.1.2.

```
<Quidway> system-view
System View: return to User View with Ctrl+Z.
[Quidway] interface vlan-interface 1
[Quidway-Vlan-interface1] udp-helper server 192.1.1.2
```

Chapter 8 IP Performance Configuration Commands

8.1 IP Performance Configuration Commands

8.1.1 display fib

Syntax

display fib

View

Any view

Parameter

None

Description

Using **display fib** command, you can view the summary of the Forwarding Information Base. The information includes: destination address/mask length, next hop, current flag, timestamp and outbound interface.

Example

Display the summary of the Forwarding Information Base.

```
<Quidway> display fib
```

Destination/Mask	Nexthop	Flag	TimeStamp	Interface
127.0.0.0/8	127.0.0.1	U	t[0]	InLoopBack0

Table 8-1 Description of the output information of the **display fib** command

Field	Description
Flag	The flag options include: B – Blackhole route D – Dynamic route G – Gateway route H – Local host route S – Static route U – Route in UP status R – Unreachable route L – Route generated by ARP or ISIS

8.1.2 display fib ip_address

Syntax

```
display fib ip_address1 [ { mask1 | mask-length1 } [ ip_address2 { mask2 | mask-length2 } ] longer ] | longer ]
```

View

Any view

Parameter

ip_address1, *ip_address2*: Destination IP address, in dotted decimal format. *ip_address1* and *ip_address2* jointly define the address range. The FIB entries in this address range will be displayed.

mask1, *mask2*, *mask-length1*, *mask-length2*: IP address mask, in dotted decimal format, or an integer in the range of 0 to 32 to represent the mask length.

longer: FIB entries matching specific network/mask.

Description

Using **display fib ip_address** command, you can view the FIB entries matching the destination IP address (range). Each line outputs a FIB entry and the display contents for each entry include destination address/mask length, next hop, current flag, timestamp and outbound interface.

Example

Display the FIB entries whose destination addresses match 169.253.0.0 in natural mask range.

```
<Quidway> display fib 169.253.0.0
```

```
Route Entry Count: 1
Destination/Mask  Nexthop      Flag    TimeStamp    Interface
169.253.0.0/16    2.1.1.1        U       t[0]         Vlan-interface1
```

Display the FIB entries whose destination addresses are in the range of 169.254.0.0/16 to 169.254.0.6/16.

```
<Quidway> display fib 169.254.0.0 255.255.0.0 169.254.0.6 255.255.0.0
```

```
Route Entry Count: 1
Destination/Mask  Nexthop      Flag    TimeStamp    Interface
169.254.0.1/16    2.1.1.1        U       t[0]         Vlan-interface1
```

For details about the display information, see Table 8-1.

8.1.3 display fib acl

Syntax

display fib acl *number*

View

Any view

Parameter

number: ACL in number form, in the range 2000 to 2999

Description

Using **display fib acl** command, you can view the FIB entries matching a specific ACL.

Example

Display the FIB entries matching ACL 2000.

```
<Quidway> display fib acl 2000
```

```
Route entry matched by access-list 2000:
```

```
Summary counts: 1
```

Destination/Mask	Nexthop	Flag	TimeStamp	Interface
127.0.0.0/8	127.0.0.1	U	t[0]	InLoopBack0

For details about the display information, see Table 8-1.

8.1.4 display fib |

Syntax

display fib | { { **begin** | **include** | **exclude** } *text* }

View

Any view

Parameter

begin: Display the FIB entries from the first one containing the character string *text*.

include: Display only those FIB entries containing the character string *text*.

exclude: Display only those FIB entries excluding the character string *text*.

text: String of specific characters.

Description

Using **display fib |** command, you can view the FIB entries which are output from the buffer according to regular expression and related to the specific character string.

Example

Display the lines starting from the first one containing the string 169.254.0.0

```
<Quidway> display fib | begin 169.254.0.0
```

Destination/Mask	Nexthop	Flag	TimeStamp	Interface
169.254.0.0/16	2.1.1.1	U	t[0]	Vlan-interface1
2.0.0.0/16	2.1.1.1	U	t[0]	Vlan-interface1

For details about the display information, see Table 8-1.

8.1.5 display fib ip-prefix

Syntax

display fib ip-prefix *listname*

View

Any view

Parameter

listname: Prefix list name, a string of one to 19 characters.

Description

Using **display fib** command, you can view the FIB entries matching the specific prefix list.

Example

Display the FIB entries matching prefix list abc0.

```
<Quidway> display fib ip-prefix abc0
```

Route Entry matched by prefix-list abc0:

Summary count: 3

Destination/Mask	Nexthop	Flag	TimeStamp	Interface
127.0.0.0/8	127.0.0.1	U	t[0]	InLoopBack0
127.0.0.1/32	127.0.0.1	U	t[0]	InLoopBack0
169.0.0.0/8	2.1.1.1	SU	t[0]	Vlan-interface1

For details about the display information, see Table 8-1.

8.1.6 display fib statistics

Syntax

display fib statistics [| { **begin** | **include** | **exclude** } *text*]

View

Any view

Parameter

begin: Display the FIB entries from the first one containing the character string *text*.

include: Display only those FIB entries containing the character string *text*.

exclude: Display only those FIB entries excluding the character string *text*.

text: String of specific characters.

Description

Using **display fib** command, you can view the total number of FIB entries.

Example

Display the total number of FIB entries.

```
<Quidway> display fib statistics
Route Entry Count : 30
```

8.1.7 display icmp statistics

Syntax

display icmp statistics

View

Any view

Parameter

None

Description

Using **display icmp statistics** command, you can view the statistics information about ICMP packets.

For the related command, see **display ip interface** , **reset ip statistics**.

Example

View statistics about ICMP packets.

```
<Quidway> display icmp statistics
Input: bad formats      0          bad checksum      0
      echo              5          destination unreachable 0
      source quench     0          redirects          0
      echo reply        10         parameter problem  0
      timestamp         0          information request  0
      mask requests     0          mask replies       0
      time exceeded     0
```

```

Output:echo          10          destination unreachable 0
      source quench 0          redirects          0
      echo reply    5          parameter problem  0
      timestamp     0          information reply   0
      mask requests 0          mask replies       0
      time exceeded 0
    
```

Table 8-2 Description of the output information of the **display icmp statistics** command

Field	Description
bad formats	Number of input packets in bad format
bad checksum	Number of input packets with wrong checksum
echo	Number of input/output echo request packets
destination unreachable	Number of input/output packets with unreachable destination
source quench	Number of input/output source quench packets
redirects	Number of input/output redirected packets
echo reply	Number of input/output echo reply packets
parameter problem	Number of input/output packets with parameter problem
timestamp	Number of input/output timestamp packets
information request	Number of input information request packets
mask requests	Number of input/output mask request packets
mask replies	Number of input/output mask reply packets
information reply	Number of output information reply packets
time exceeded	Number of time exceeded packets

8.1.8 display ip socket

Syntax

display ip socket [**socktype** *sock-type*] [*task-id* *socket-id*]

View

Any view

Parameter

sock-type: The type of a socket: (tcp:1, udp 2, raw ip 3).

task-id: The ID of a task, with the value ranging from 1 to 100.

socket-id: The ID of a socket, with the value ranging from 0 to 3072.

Description

Using the **display ip socket** command, you can display the information about the sockets in the current system.

Example

Display the information about the socket of TCP type.

```
<Quidway> display ip socket socktype 1
SOCK_STREAM:
Task = VTYPD(18), socketid = 1, Proto = 6,
LA = 0.0.0.0:23, FA = 0.0.0.0:0,
sndbuf = 8192, rcvbuf = 8192, sb_cc = 0, rb_cc = 0,
socket option = SO_ACCEPTCONN SO_KEEPAALIVE SO_SENDVFNID SO_SETKEEPAALIVE,
socket state = SS_PRIV SS_ASYNC

Task = VTYPD(18), socketid = 2, Proto = 6,
LA = 10.153.17.99:23, FA = 10.153.17.56:1161,
sndbuf = 8192, rcvbuf = 8192, sb_cc = 0, rb_cc = 0,
socket option = SO_KEEPAALIVE SO_OOBINLINE SO_SENDVFNID SO_SETKEEPAALIVE,
socket state = SS_ISCONNECTED SS_PRIV SS_ASYNC

Task = VTYPD(18), socketid = 3, Proto = 6,
LA = 10.153.17.99:23, FA = 10.153.17.82:1121,
sndbuf = 8192, rcvbuf = 8192, sb_cc = 0, rb_cc = 0,
socket option = SO_KEEPAALIVE SO_OOBINLINE SO_SENDVFNID SO_SETKEEPAALIVE,
socket state = SS_ISCONNECTED SS_PRIV SS_ASYNC
```

Table 8-3 Description of the output information of the **display ip socket** command

Field	Description
SOCK_STREAM	The socket type
Task	The ID of a task
socketid	The ID of a socket
Proto	The protocol number used by the socket
sndbuf	The sending buffer size of the socket
rcvbuf	The receiving buffer size of the socket
sb_cc	The current data size in the sending buffer. The value makes sense only for the socket of TCP type, because only TCP is able to cache data

Field	Description
rb_cc	The current data size in the receiving buffer
socket option	The option of the socket
socket state	The state of the socket

8.1.9 display ip statistics

Syntax

display ip statistics

View

Any view

Parameter

None

Description

Using **display ip statistics** command, you can view the statistics information about IP packets.

For the related command, see **display ip interface**, **reset ip statistics**.

Example

View statistics about IP packets.

```
<Quidway> display ip statistics
Input:  sum          7120          local          112
        bad protocol  0           bad format      0
        bad checksum  0           bad options     0
Output: forwarding   0           local          27
        dropped       0           no route        2
        compress fails 0
Fragment:input       0           output          0
        dropped       0
        fragmented    0           couldn't fragment 0
Reassembling:sum     0           timeouts        0
```

Table 8-4 Description of the output information of the **display ip statistics** command

Field		Description
Input:	sum	Sum of input packets
	local	Number of received packets whose destination is the local device
	bad protocol	Number of packets with wrong protocol number
	bad format	Number of packets in bad format
	bad checksum	Number of packets with wrong checksum
	bad options	Number of packets that has wrong options
Output:	forwarding	Number of forwarded packets
	local	Number of packets that are sent by the local device
	dropped	Number of dropped packets during transmission
	no route	Number of packets that cannot be routed
	compress fails	Number of packets that cannot be compressed
Fragment:	input	Number of input fragments
	output	Number of output fragments
	dropped	Number of dropped fragments
	fragmented	Number of packets that are fragmented
	couldn't fragment	Number of packets that cannot be fragmented
Reassembling:	sum	Number of packets that are reassembled
	timeouts	Number of packets that time out

8.1.10 display tcp statistics

Syntax

display tcp statistics

View

Any view

Parameter

None

Description

Using **display tcp statistics** command, you can view the statistics information about TCP packets.

The statistics information about TCP packets are divided into two major kinds which are Received packets and Sent packets. And each kind of packets are further divided into different kinds such as window probe packets, window update packets, duplicate packets, and out-of-order packets. Some statistics information that is closely related to TCP connection, such as window probe packets, window update packets, and data packets retransmitted is also displayed. All these displayed information are measured in packet.

For the related commands, see **display tcp status**, **reset tcp statistics**.

Example

View statistics about TCP packets.

```
<Quidway> display tcp statistics
Received packets:
Total: 753
packets in sequence: 412 (11032 bytes)
window probe packets: 0, window update packets: 0
checksum error: 0, offset error: 0, short error: 0
duplicate packets: 4 (88 bytes), partially duplicate packets: 5 (7 bytes)
out-of-order packets: 0 (0 bytes)
packets of data after window: 0 (0 bytes)
packets received after close: 0
ACK packets: 481 (8776 bytes)
duplicate ACK packets: 7, too much ACK packets: 0

Sent packets:
Total: 665
urgent packets: 0
control packets: 5 (including 1 RST)
window probe packets: 0, window update packets: 2
data packets: 618 (8770 bytes) data packets retransmitted: 0 (0 bytes)
ACK-only packets: 40 (28 delayed)

Retransmitted timeout: 0, connections dropped in retransmitted timeout: 0
Keepalive timeout: 0, keepalive probe: 0, Keepalive timeout, so connections
disconnected : 0
Initiated connections: 0, accepted connections: 0, established connections:
0
Closed connections: 0 (dropped: 0, initiated dropped: 0)
```

```
Packets dropped with MD5 authentication: 0
Packets permitted with MD5 authentication: 0
```

8.1.11 display tcp status

Syntax

display tcp status

View

Any view

Parameter

None

Description

Using **display tcp status** command, you can view the TCP connection state.

Example

Display the state of all TCP connections.

```
<Quidway> display tcp status

TCPCB      Local Add:port      Foreign Add:port      State
03e37dc4   0.0.0.0:4001         0.0.0.0:0             Listening
04217174   100.0.0.204:23       100.0.0.253:65508     Established
```

Table 8-5 Description of the output information of the **display tcp status** command

Information	Description
Local Add: port	Local IP address: local port
Foreign Add: port	Remote IP address; remote port
State	State of the TCP link

8.1.12 display udp statistics

Syntax

display udp statistics

View

Any view

Parameter

None

Description

Using the **display udp statistics** command, you can view UDP traffic statistic information.

For relate configuration, please refer to the **reset udp statistics** command.

Example

Display the UDP traffic statistic information.

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

8.1.13 reset ip statistics

Syntax

reset ip statistics

View

User view

Parameter

None

Description

Using **reset ip statistics** command, you can clear the IP statistics information.

For the related commands, see **display ip interface**, **display ip statistics**.

Example

Clear the IP statistics information.

```
<Quidway> reset ip statistics
```

8.1.14 reset tcp statistics

Syntax

reset tcp statistics

View

User view

Parameter

None

Description

Using **reset tcp statistics** command, you can clear the TCP statistics information.
For the related command, see **display tcp statistics**.

Example

```
# Clear the TCP statistics information.  
<Quidway> reset tcp statistics
```

8.1.15 reset udp statistics

Syntax

reset udp statistics

View

User view

Parameter

None

Description

Using the **reset udp statistics** command, you can clear the UDP statistics information.

Example

```
# Clear the UDP traffic statistics information.  
<Quidway> reset udp statistics
```

8.1.16 tcp timer fin-timeout

Syntax

tcp timer fin-timeout *time-value*
undo tcp timer fin-timeout

View

System view

Parameter

time-value: TCP finwait timer value in second, with the value ranging from 76 to 3600;
By default, 675 seconds.

Description

Using **tcp timer fin-timeout** command, you can configure the TCP finwait timer. Using **undo tcp timer fin-timeout** command, you can restore the default value of the TCP finwait timer.

When the TCP connection state changes from FIN_WAIT_1 to FIN_WAIT_2, the finwait timer is enabled. If the switch does not receive FIN packet before finwait timer timeouts, the TCP connection will be terminated.

For the related command, see **tcp timer syn-timeout**, **tcp window**.

Example

Configure the TCP finwait timer value as 800 seconds.

```
<Quidway> system-view
System View: return to User View with Ctrl+Z.
[Quidway] tcp timer fin-timeout 800
```

8.1.17 tcp timer syn-timeout

Syntax

tcp timer syn-timeout *time-value*
undo tcp timer syn-timeout

View

System view

Parameter

time-value: TCP synwait timer value measured in second, whose value ranges from 2 to 600. The default *time-value* is 75 seconds.

Description

Using **tcp timer syn-timeout** command, you can configure the TCP synwait timer. Using **undo tcp timer syn-timeout** command, you can restore the default value of the timer.

TCP will enable the synwait timer, if a SYN packet is sent. The TCP connection will be terminated If the response packet is not received.

For the related command, see **tcp timer fin-timeout**, **tcp window**.

Example

Configure the TCP synwait timer value as 80 seconds.

```
<Quidway> system-view
System View: return to User View with Ctrl+Z.
[Quidway] tcp timer syn-timeout 80
```

8.1.18 tcp window

Syntax

tcp window *window-size*

undo tcp window

View

System view

Parameter

window-size: The size of the transmission and receiving buffers measured in kilobytes (KB), whose value ranges from 1 to 32. By default, the *window-size* is 8KB.

Description

Using **tcp window** command, you can configure the size of the transmission and receiving buffers of the connection-oriented Socket. Using **undo tcp window** command, you can restore the default size of the buffer.

For the related command, see **tcp timer fin-timeout**, **tcp timer syn-timeout**.

Example

Configure the size of the transmission and receiving buffers as 3KB.

```
<Quidway> system-view
System View: return to User View with Ctrl+Z.
[Quidway] tcp window 3
```