Contents

DHCP commands

Common DHCP commands

dhcp dscp

Use **dhcp dscp** to set the DSCP value for DHCP packets sent by the DHCP server or the DHCP relay agent.

Use **undo dhcp dscp** to restore the default.

Syntax

dhcp dscp *dscp-value*

undo dhcp dscp

Default

The DSCP value in DHCP packets is 56.

Views

System view

Predefined user roles

network-admin

Parameters

dscp-value: Sets the DSCP value for DHCP packets, in the range of 0 to 63.

Usage guidelines

The DSCP value of a packet specifies the priority level of the packet and affects the transmission priority of the packet. A bigger DSCP value represents a higher priority.

Examples

# Set the DSCP value for DHCP packets to 30.

```
<Sysname> system-view
[Sysname] dhcp dscp 30
```

dhcp enable

Use **dhcp enable** to enable DHCP.

Use **undo dhcp enable** to disable DHCP.

Syntax

dhcp enable

undo dhcp enable

Default

DHCP is disabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

Enable DHCP before you perform DHCP server or relay agent configurations.

Examples

# Enable DHCP.

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

dhcp select

Use **dhcp select** to enable the DHCP server or DHCP relay agent on an interface.

Use **undo dhcp select** to disable the DHCP server or DHCP relay agent on an interface. The interface discards DHCP packets.

Syntax

dhcp select { **relay** | **server** }

undo dhcp select { **relay** | **server** }

Default

The interface operates in DHCP server mode and responds to DHCP requests with configuration parameters.

Views

Interface view

Predefined user roles

network-admin

Parameters

relay: Enables the DHCP relay agent on the interface.

server: Enables the DHCP server on the interface.

Usage guidelines

Before changing the DHCP server mode to the DHCP relay agent mode on an interface, use the **reset dhcp server ip-in-use** command to remove address bindings and authorized ARP entries. These bindings might conflict with ARP entries that are created after the DHCP relay agent is enabled.

Examples

# Enable the DHCP relay agent on VLAN-interface 2.

```
<Sysname> system-view
[Sysname] interface vlan-interface 2
[Sysname-Vlan-interface2] dhcp select relay
```

Related commands

reset dhcp server ip-in-use

DHCP server commands

The term "interface" in this section refers to VLAN interfaces.

address range

Use **address range** to configure an IP address range in a DHCP address pool for dynamic allocation.

Use **undo address range** to remove the IP address range in the DHCP address pool.

Syntax

address range *start-ip-address end-ip-address*

undo address range

Default

No IP address range is configured.

Views

DHCP address pool view

Predefined user roles

network-admin

Parameters

start-ip-address: Specifies the start IP address.

end-ip-address: Specifies the end IP address.

Usage guidelines

If no IP address range is specified, all IP addresses in the subnet specified by the **network** command in address pool view are assignable. If an IP address range is specified, only the IP addresses in the IP address range are assignable.

After you use the **address range** command, you cannot use the **network secondary** command to specify a secondary subnet in the address pool.

If you use the command multiple times, the most recent configuration takes effect.

The address range specified by the **address range** command must be within the subnet specified by the **network** command, and the addresses out of the address range cannot be assigned.

Examples

# Specify an address range of 192.168.8.1 through 192.168.8.150 in address pool 1.

```
<Sysname> system-view
[Sysname] dhcp server ip-pool 1
[Sysname-dhcp-pool-1] address range 192.168.8.1 192.168.8.150
```

Related commands

- **class**
- **dhcp class**
- **display dhcp server pool**
- **network**

bims-server

Use **bims-server** to specify the IP address, port number, and shared key of the BIMS server in a DHCP address pool.

Use **undo bims-server** to remove the specified BIMS server information.

Syntax

bims-server ip *ip-address* [**port** *port-number*] **sharekey** { **cipher | simple** } *key*

undo bims-server

Default

No BIMS server information is specified.

Views

DHCP address pool view

Predefined user roles

network-admin

Parameters

ip *ip-address*: Specifies the IP address of the BIMS server.

port *port-number*: Specifies the port number of the BIMS server, in the range of 1 to 65534.

cipher: Sets a ciphertext key.

simple: Sets a plaintext key.

key: Specifies the key string. This argument is case sensitive. If **simple** is specified, it must be a string of 1 to 16 characters. If **cipher** is specified, it must be a ciphertext string of 1 to 53 characters. The DHCP client uses the shared key to encrypt packets sent to the BIMS server.

Usage guidelines

If you use this command multiple times, the most recent configuration takes effect.

For security purposes, all passwords, including passwords configured in plaintext, are saved in ciphertext.

Examples

# Specify the BIMS server IP address 1.1.1.1, port number 80, and shared key **aabbcc** in address pool 0.

```
<Sysname> system-view
[Sysname] dhcp server ip-pool 0
[Sysname-dhcp-pool-0] bims-server ip 1.1.1.1 port 80 sharekey simple aabbcc
```

Related commands

display dhcp server pool

bootfile-name

Use **bootfile-name** to specify a configuration file name or URL.

Use **undo bootfile-name** to remove the configuration file name or URL.

Syntax

bootfile-name { *bootfile-name* | *url* }

undo bootfile-name

Default

No configuration file name or URL is specified.

Views

DHCP address pool view

Predefined user roles

network-admin

Parameters

bootfile-name: Specifies the configuration file name, a case-sensitive string of 1 to 63 characters.

url: Specifies the configuration file URL in the format of http://. It is a case-sensitive string of 1 to 63 characters.

Usage guidelines

If you use the **bootfile-name** command multiple times, the most recent configuration takes effect.

If the configuration file is on a TFTP server, specify the configuration file name, and the IP address or name of the TFTP server.

If the configuration file is on an HTTP server, specify the configuration file URL.

Examples

# Specify the boot file name **boot.cfg** in DHCP address pool 0.

```
<Sysname> system-view
[Sysname] dhcp server ip-pool 0
[Sysname-dhcp-pool-0] bootfile-name boot.cfg
```

# Specify the URL **http://10.1.1.1/boot.cfg** for the remote boot file in DHCP address pool 0.

```
<Sysname> system-view
[Sysname] dhcp server ip-pool 0
[Sysname-dhcp-pool-0] bootfile-name http://10.1.1.1/boot.cfg
```

Related commands

- **display dhcp server pool**
- **next-server**
- **tftp-server domain-name**
- **tftp-server ip-address**

class

Use **class** to specify an IP address range for a DHCP user class.

Use **undo class** to remove the IP address range for the DHCP user class.

Syntax

class *class-name* **range** *start-ip-address end-ip-address*

undo class *class-name*

Default

No IP address range is specified for a DHCP user class.

Views

DHCP address pool view

Predefined user roles

network-admin

Parameters

class-name: Specifies the name of a DHCP user class, a case-insensitive string of 1 to 63 characters. If the specified user class does not exist, the DHCP server will not assign the addresses in the address range specified for the user class to any client.

start-ip-address: Specifies the start IP address.

end-ip-address: Specifies the end IP address.

Usage guidelines

The **class** command enables you to divide an address range into multiple address ranges for different DHCP user classes. The address range for a user class must be within the primary subnet specified by the **network** command. If the DHCP client does not match any DHCP user class, the DHCP server selects an address in the IP address range specified by the **address range** command. If the address range has no assignable IP addresses or no address range is configured, the address allocation fails.

You can specify only one address range for a DHCP user class in an address pool. If you use the **class** command multiple times for a DHCP user class, the most recent configuration takes effect.

After you specify an address range for a user class, you cannot use the **network secondary** command to specify a secondary subnet in the address pool.

Examples

# Specify an IP address range of 192.168.8.1 through 192.168.8.150 for the DHCP user class **user** in DHCP address pool 1.

```
<Sysname> system-view
[Sysname] dhcp server ip-pool 1
[Sysname-dhcp-pool-1] class user range 192.168.8.1 192.168.8.150
```

Related commands

- **address range**
- **dhcp class**
- **display dhcp server pool**

dhcp class

Use **dhcp class** to create a DHCP user class and enter the DHCP user class view.

Use **undo dhcp class** to remove the specified DHCP user class.

Syntax

dhcp class *class-name*

undo dhcp class *class-name*

Default

No DHCP user class exists.

Views

System view

Predefined user roles

network-admin

Parameters

class-name: Specifies the name of a DHCP user class, a case-insensitive string of 1 to 63 characters.

Usage guidelines

You can also use this command to enter the view of an existing DHCP user class.

In the DHCP user class view, use the **if-match** command to configure a match rule to match specific clients. Then use the **class** command to specify an IP address range for the matching clients.

Examples

# Create a DHCP user class **test** and enter DHCP user class view.

```
<Sysname> system-view
[Sysname] dhcp class test
[Sysname-dhcp-class-test]
```

Related commands

- **address range**
- **class**
- **if-match**

dhcp server always-broadcast

Use **dhcp server always-broadcast** to enable the DHCP server to broadcast all responses.

Use **undo dhcp server always-broadcast** to restore the default.

Syntax

dhcp server always-broadcast

undo dhcp server always-broadcast

Default

The DHCP server reads the broadcast flag in a DHCP request to decide whether to broadcast or unicast the response.

Views

System view

Predefined user roles

network-admin

Usage guidelines

This command enables the DHCP server to ignore the broadcast flag in DHCP requests and broadcast all responses.

If a DHCP request is from a DHCP client that has an IP address (the **ciaddr** field is not 0), the DHCP server always unicasts a response (the destination address is **ciaddr**) to the DHCP client regardless of whether this command is executed.

If a DHCP request is from a DHCP relay agent (the **giaddr** field is not 0), the DHCP server always unicasts a response (the destination address is **giaddr**) to the DHCP relay agent regardless of whether this command is executed.

Examples

# Enable the DHCP server to broadcast all responses.

```
<Sysname> system-view
[Sysname] dhcp server always-broadcast
```

dhcp server apply ip-pool

Use **dhcp server apply ip-pool** to apply an address pool on an interface.

Use **undo dhcp server apply ip-pool** to remove the configuration.

Syntax

dhcp server apply ip-pool *pool-name*

undo dhcp server apply ip-pool

Default

No address pool is applied on an interface

Views

Interface view

Predefined user roles

network-admin

Parameters

pool-name: Specifies the name of a DHCP address pool, a case-insensitive string of 1 to 63 characters.

Usage guidelines

Upon receiving a DHCP request from the interface, the DHCP server searches for a static binding for the client from all address pools. If no static binding is found, the server assigns configuration parameters from the address pool applied on the interface to the client. If the address pool has no assignable IP address or does not exist, the DHCP client cannot obtain an IP address.

If you use the command multiple times, the most recent configuration takes effect.

Examples

# Apply DHCP address pool 0 on VLAN-interface 2.

```
<Sysname> system-view
[Sysname] interface vlan-interface 2
[Sysname-Vlan-interface2] dhcp server apply ip-pool 0
```

Related commands

dhcp server ip-pool

dhcp server bootp ignore

Use **dhcp server bootp ignore** to configure the DHCP server to ignore BOOTP requests.

Use **undo dhcp server bootp ignore** to restore the default.

Syntax

dhcp server bootp ignore

undo dhcp server bootp ignore

Default

The DHCP server does not ignore BOOTP requests.

Views

System view

Predefined user roles

network-admin

Usage guidelines

The lease duration of IP addresses obtained by BOOTP clients is unlimited. For scenarios that do not allow unlimited leases, you can configure the DHCP server to ignore BOOTP requests.

Examples

# Configure the DHCP server to ignore BOOTP requests.

```
<Sysname> system-view
[Sysname] dhcp server bootp ignore
```

dhcp server bootp reply-rfc-1048

Use **dhcp server bootp reply-rfc-1048** to enable the DHCP server to send BOOTP responses in RFC 1048 format when it receives RFC 1048-incompliant BOOTP requests for statically bound addresses.

Use **undo dhcp server bootp reply-rfc-1048** to disable this feature.

Syntax

dhcp server bootp reply-rfc-1048

undo dhcp server bootp reply-rfc-1048

Default

This feature is disabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

Not all BOOTP clients can send requests compliant with RFC 1048. By default, the DHCP server does not process the Vend field of RFC 1048-incompliant requests but copies the Vend field into responses.

Use this command to enable the DHCP server to fill in the Vend field using the RFC 1048-compliant format in DHCP responses to RFC 1048-incompliant requests sent by BOOTP clients that request statically bound addresses.

Examples

# Enable the DHCP server to send BOOTP responses in RFC 1048 format upon receiving BOOTP requests incompliant with RFC 1048.

```
<Sysname> system-view
[Sysname] dhcp server bootp reply-rfc-1048
```

dhcp server forbidden-ip

Use **dhcp server forbidden-ip** to exclude specific IP addresses from dynamic allocation.

Use **undo dhcp server forbidden-ip** to remove the configuration.

Syntax

dhcp server forbidden-ip *start-ip-address* [*end-ip-address*] [**vpn-instance** *vpn-instance-name*]

undo dhcp server forbidden-ip *start-ip-address* [*end-ip-address*] [**vpn-instance** *vpn-instance-name*]

Default

No IP addresses are excluded from dynamic allocation.

Views

System view

Predefined user roles

network-admin

Parameters

start-ip-address: Specifies the start IP address.

end-ip-address: Specifies the end IP address, which cannot be lower than the *start-ip-address*. If you do not specify this argument, only the *start-ip-address* is excluded from dynamic allocation.

vpn-instance *vpn-instance-name*: Specifies a VPN instance by its name, a case-sensitive string of 1 to 31 characters. If the excluded IP addresses belong to the public network, do not specify this option.

Usage guidelines

The IP addresses of some devices such as the gateway and FTP server cannot be assigned to clients. Use this command to exclude such addresses from dynamic allocation.

You can exclude multiple IP address ranges from dynamic allocation.

If the excluded IP address is in a static binding, the address can be still assigned to the client.

The address or address range specified in the **undo** form of the command must be the same as the address or address range specified in the command. To remove an IP address that has been specified as part of an address range, you must remove the entire address range.

Examples

# Exclude the IP addresses of 10.110.1.1 through 10.110.1.63 from dynamic allocation.

```
<Sysname> system-view
[Sysname] dhcp server forbidden-ip 10.110.1.1 10.110.1.63
```

Related commands

- **forbidden-ip**
- **static-bind**

dhcp server ip-pool

Use **dhcp server ip-pool** to create a DHCP address pool and enter its view.

Use **undo dhcp server ip-pool** to remove the specified DHCP address pool.

Syntax

dhcp server ip-pool *pool-name*

undo dhcp server ip-pool *pool-name*

Default

No DHCP address pool is created.

Views

System view

Predefined user roles

network-admin

Parameters

pool-name: Specifies the name for the DHCP address pool, a case-insensitive string of 1 to 63 characters used to uniquely identify this pool.

Usage guidelines

You can also use this command to enter the view of an existing DHCP address pool.

A DHCP address pool is used to store the configuration parameters to be assigned to DHCP clients.

Examples

# Create a DHCP address pool named **pool1**.

```
<Sysname> system-view
[Sysname] dhcp server ip-pool pool1
[Sysname-dhcp-pool-pool1]
```

Related commands

- **dhcp server apply ip-pool**
- **display dhcp server pool**

dhcp server ping packets

Use **dhcp server ping packets** to specify the maximum number of ping packets.

Use **undo dhcp server ping packets** to restore the default.

Syntax

dhcp server ping packets *number*

undo dhcp server ping packets

Default

The maximum number of ping packets is 1.

Views

System view

Predefined user roles

network-admin

Parameters

number: Specifies the maximum number of ping packets, in the range of 0 to 10. A value of 0 indicates that the DHCP server does not perform address conflict detection.

Usage guidelines

To avoid IP address conflicts, the DHCP server pings an IP address before assigning it to a DHCP client.

If a ping attempt succeeds, the server considers that the IP address is in use and picks a new IP address. If all the ping attempts are failed, the server assigns the IP address to the requesting DHCP client.

Examples

# Specify the maximum number of ping packets as 10.

```
<Sysname> system-view
```

```
[Sysname] dhcp server ping packets 10
```

Related commands

- **dhcp server ping timeout**
- **display dhcp server conflict**
- **reset dhcp server conflict**

dhcp server ping timeout

Use **dhcp server ping timeout** to configure the ping response timeout time on the DHCP server.

Use **undo dhcp server ping timeout** to restore the default.

Syntax

dhcp server ping timeout *milliseconds*

undo dhcp server ping timeout

Default

The ping response timeout time is 500 milliseconds.

Views

System view

Predefined user roles

network-admin

Parameters

milliseconds: Specifies the timeout time in the range of 0 to 10000 milliseconds. To disable the ping operation for address conflict detection, set the value to 0 milliseconds.

Usage guidelines

To avoid IP address conflicts, the DHCP server pings an IP address before assigning it to a DHCP client.

If a ping attempt succeeds, the server considers that the IP address is in use and picks a new IP address. If all the ping attempts are failed, the server assigns the IP address to the requesting DHCP client.

Examples

# Specify the response timeout time as 1000 milliseconds.

```
<Sysname> system-view
[Sysname] dhcp server ping timeout 1000
```

Related commands

- **dhcp server ping packets**
- **display dhcp server conflict**
- **reset dhcp server conflict**

dhcp server relay information enable

Use **dhcp server relay information enable** to enable the DHCP server to handle Option 82.

Use **undo dhcp server relay information enable** to configure the DHCP server to ignore Option 82.

Syntax

dhcp server relay information enable

undo dhcp server relay information enable

Default

The DHCP server handles Option 82.

Views

System view

Predefined user roles

network-admin

Usage guidelines

Upon receiving a DHCP request that contains Option 82, the server copies the original Option 82 into the response. If the server is configured to ignore Option 82, the response will not contain Option 82.

Examples

# Configure the DHCP server to ignore Option 82.

```
<Sysname> system-view
[Sysname] undo dhcp server relay information enable
```

display dhcp server conflict

Use **display dhcp server conflict** to display information about IP address conflicts.

Syntax

display dhcp server conflict [**ip** *ip-address*] [**vpn-instance** *vpn-instance-name*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

ip *ip-address*: Displays conflict information about the specified IP address. If you do not specify this option, this command displays information about all IP address conflicts.

vpn-instance *vpn-instance-name*: Specifies a VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, this command displays IP address conflict information for the public network.

Usage guidelines

The DHCP server creates IP address conflict information in the following conditions:

- Before assigning an IP address to a DHCP client, the DHCP server pings the IP address and discovers that it has been used by other host.
- The DHCP client sends a DECLINE packet to the DHCP server to inform the server of an IP address conflict.
- The DHCP server discovers that the only assignable address in the address pool is its own IP address.

Examples

# Display information about all IP address conflicts.

```
<Sysname> display dhcp server conflict
IP address          Detect time
4.4.4.1             Apr 25 16:57:20 2007
4.4.4.2             Apr 25 17:00:10 2007
```

Table 1 Command output

Field	Description
IP address	Conflicted IP address.
Detect time	Time when the conflict was discovered.

Related commands

reset dhcp server conflict

display dhcp server expired

Use **display dhcp server expired** to display the lease expiration information.

Syntax

display dhcp server expired [[**ip** *ip-address*] [**vpn-instance** *vpn-instance-name*] | **pool** *pool-name*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

ip *ip-address*: Displays lease expiration information about the specified IP address.

vpn-instance *vpn-instance-name*: Specifies a VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, this command displays lease expiration information about IP addresses for the public network.

pool *pool-name*: Displays lease expiration information about the specified address pool. The pool name is a case-insensitive string of 1 to 63 characters.

Usage guidelines

If you do not specify any parameters, this command displays lease expiration information about all address pools.

DHCP assigns these expired IP addresses to DHCP clients when all available addresses have been assigned.

Examples

# Display all lease expiration information.

```
<Sysname> display dhcp server expired
IP address       Client-identifier/Hardware address    Lease expiration
4.4.4.6          3030-3066-2e65-3230-302e-3130-3234    Apr 25 17:10:47 2007
                 -2d45-7468-6572-6e65-7430-2f31
```

Table 2 Command output

Field	Description
IP address	Expired IP address.
Client-identifier/Hardware address	Client ID or MAC address.
Lease expiration	Time when the lease expired.

Related commands

reset dhcp server expired

display dhcp server free-ip

Use **display dhcp server free-ip** to display information about assignable IP addresses.

Syntax

display dhcp server free-ip [**pool** *pool-name* **|** **vpn-instance** *vpn-instance-name*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

pool *pool-name*: Displays assignable IP addresses in the specified address pool. The pool name is a case-insensitive string of 1 to 63 characters. If you do not specify an address pool, this command displays all assignable IP addresses for all address pools.

vpn-instance *vpn-instance-name*: Specifies a VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, this command displays assignable IP addresses in address pools for the public network.

Examples

# Display assignable IP addresses in all address pools.

```
<Sysname> display dhcp server free-ip
Pool name: 1
  Network: 10.0.0.0 mask 255.0.0.0
    IP ranges from 10.0.0.10 to 10.0.0.100
    IP ranges from 10.0.0.105 to 10.0.0.255
  Secondary networks:
    10.1.0.0 mask 255.255.0.0
      IP ranges from 10.1.0.0 to 10.1.0.255
    10.2.0.0 mask 255.255.0.0
      IP Ranges from 10.2.0.0 to 10.2.0.255

Pool name: 2
  Network: 20.1.1.0 mask 255.255.255.0
    IP ranges from 20.1.1.0 to 20.1.1.255
```

Table 3 Command output

Field	Description
Pool name	Name of the address pool.
Network	Assignable network.
IP ranges	Assignable IP address range.
Secondary networks	Assignable secondary networks.

Related commands

- **address range**
- **dhcp server ip-pool**
- **network**

display dhcp server ip-in-use

Use **display dhcp server ip-in-use** to display binding information about assigned IP addresses.

Syntax

display dhcp server ip-in-use [[**ip** *ip-address*] [**vpn-instance** *vpn-instance-name*] **|** **pool** *pool-name*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

ip *ip-address*: Displays binding information about the specified IP address.

vpn-instance *vpn-instance-name*: Specifies a VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, this command displays binding information about assigned IP addresses for the public network.

pool *pool-name*: Displays binding information about the specified IP address pool. The pool name is a case-insensitive string of 1 to 63 characters.

Usage guidelines

If you do not specify any parameters, this command displays binding information about all assigned DHCP addresses.

If the lease deadline exceeds the year 2100, the lease expiration time is displayed as **After 2100**.

The client binding information can be used by other security modules such as IP source guard only when the DHCP server is configured on the gateway of DHCP clients.

Examples

# Display binding information about all assigned DHCP addresses.

```
<Sysname> display dhcp server ip-in-use
IP address       Client identifier/    Lease expiration      Type
                 Hardware address
10.1.1.1         4444-4444-4444        Not used              Static(F)
10.1.1.2         3030-3030-2e30-3030-  May 1 14:02:49 2009   Auto(C)
```

```
                 662e-3030-3033-2d45-
                 7468-6572-6e65-74
10.1.1.3         1111-1111-1111        After 2100            Static(C)
```

Table 4 Command output

Field	Description
IP address	IP address assigned.
Client identifier/Hardware address	Client ID or hardware address.
Lease expiration	Lease expiration time: • **Exact time (May 1 14:02:49 2009 in this example)**—Time when the lease will expire. • **Not used**—The IP address of the static binding has not been assigned to the specific client. • **Unlimited**—Infinite lease expiration time. • **After 2100**—The lease will expire after 2100.
Type	Binding types: • **Static(F)**—A free static binding whose IP address has not been assigned. • **Static(O)**—An offered static binding whose IP address has been selected and sent by the DHCP server in a DHCP-OFFER packet to the client. **Static(C)**—A committed static binding whose IP address has been assigned to the DHCP client. • **Auto(O)**—An offered temporary dynamic binding whose IP address has been dynamically selected by the DHCP server and sent in a DHCP-OFFER packet to the DHCP client. • **Auto(C)**—A committed dynamic binding whose IP address has been dynamically assigned to the DHCP client.

Related commands

reset dhcp server ip-in-use

display dhcp server pool

Use **display dhcp server pool** to display information about a DHCP address pool.

Syntax

display dhcp server pool [*pool-name* | **vpn-instance** *vpn-instance-name*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

pool-name: Displays information about the specified address pool. The pool name is a case-insensitive string of 1 to 63 characters. If you do not specify the *pool-name* argument, this command displays information about all address pools.

vpn-instance *vpn-instance-name*: Specifies a VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, this command displays information about address pools for the public network.

Examples

# Display information about all DHCP address pools.

```
<Sysname> display dhcp server pool
Pool name: 0
  Network 20.1.1.0 mask 255.255.255.0
  class a range 20.1.1.50 20.1.1.60
  bootfile-name abc.cfg
  dns-list 20.1.1.66 20.1.1.67 20.1.1.68
  domain-name www.aabbcc.com
  bims-server ip 192.168.0.51 sharekey cipher $c$3$K13OmQPi791YvQoF2Gs1E+65LOU=
  option 2 ip-address 1.1.1.1
  expired 1 2 3 0

Pool name: 1
  Network 20.1.1.0 mask 255.255.255.0
  secondary networks:
    20.1.2.0 mask 255.255.255.0
    20.1.3.0 mask 255.255.255.0
  bims-server ip 192.168.0.51 port 50 sharekey cipher $c$3$K13OmQPi791YvQoF2Gs1E+65LOU=
  forbidden-ip 20.1.1.22 20.1.1.36 20.1.1.37
  forbidden-ip 20.1.1.22 20.1.1.23 20.1.1.24
  gateway-list 1.1.1.1 2.2.2.2 4.4.4.4
  nbns-list 5.5.5.5 6.6.6.6 7.7.7.7
  netbios-type m-node
  option 2 ip-address 1.1.1.1
  expired 1 0 0 0

Pool name: 2
  Network 20.1.1.0 mask 255.255.255.0
  address range 20.1.1.1 to 20.1.1.15
  class departmentA range 20.1.1.20 to 20.1.1.29
  class departmentB range 20.1.1.30 to 20.1.1.40
  next-server 20.1.1.33
  tftp-server domain-name www.dian.org.cn
  tftp-server ip-address 192.168.0.120
  voice-config ncp-ip 10.1.1.2
  voice-config as-ip 10.1.1.5
  voice-config voice-vlan 3 enable
  voice-config fail-over 10.1.1.1 123*
  option 2 ip-address 1.1.1.3
  expired 1 0 0 0

Pool name: 3
  static bindings:
    ip-address 10.10.1.2 mask 255.0.0.0
```

```
      hardware-address 00e0-00fc-0001 ethernet
    ip-address 10.10.1.3 mask 255.0.0.0
      client-identifier aaaa-bbbb
  expired unlimited
```

Table 5 Command output

Field	Description
Pool name	Name of an address pool.
Network	Assignable network.
secondary networks	Assignable secondary networks.
address range	Assignable address range.
class *class-name* range	DHCP user class and its address range.
static bindings	Static IP-to-MAC/client ID bindings.
option	Customized DHCP option.
expired	Lease duration: 1 2 3 4 in this example refers to 1 day 2 hours 3 minutes 4 seconds.
bootfile-name	Boot file name
dns-list	DNS server IP address.
domain-name	Domain name suffix.
bims-server	BIMS server information.
forbidden-ip	IP addresses excluded from dynamic allocation.
gateway-list	Gateway addresses.
nbns-list	WINS server addresses.
netbios-type	NetBIOS node type.
next-server	Next server IP address.
tftp-server domain-name	TFTP server name.
tftp-server ip-address	TFTP server address.
voice-config ncp-ip	Primary network calling processor address.
voice-config as-ip	Backup network calling processor address.
voice-config voice-vlan	Voice VLAN.
voice-config fail-over	Failover route.

display dhcp server statistics

Use **display dhcp server statistics** to display the DHCP server statistics.

Syntax

display dhcp server statistics [**pool** *pool-name* **|** **vpn-instance** *vpn-instance-name*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

pool *pool-name*: Specifies an address pool by its name, a case-insensitive string of 1 to 63 characters. If you do not specify this option, this command displays information about all address pools.

vpn-instance *vpn-instance-name*: Specifies a VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, this command displays DHCP server statistics for the public network.

Examples

# Display the DHCP server statistics.

```
<Sysname> display dhcp server statistics
    Pool number:                        1
    Pool utilization:                   0.39%
    Bindings:
      Automatic:                        1
      Manual:                           0
      Expired:                          0
    Conflict:                           1
    Messages received:                 10
      DHCPDISCOVER:                     5
      DHCPREQUEST:                      3
      DHCPDECLINE:                      0
      DHCPRELEASE:                      2
      DHCPINFORM:                       0
      BOOTPREQUEST:                     0
    Messages sent:                      6
      DHCPOFFER:                        3
      DHCPACK:                          3
      DHCPNAK:                          0
      BOOTPREPLY:                       0
    Bad Messages:                       0
```

Table 6 Command output

Field	Description
Pool number	Total number of address pools. This field is not displayed when you display statistics for a specific address pool.
Pool utilization	Pool utilization rate: • If you display statistics for all address pools, this field displays the utilization rate of all address pools. • If you display statistics for an address pool, this field displays the pool utilization rate of the specified address pool.
Bindings	Bindings include the following types: • **Automatic**—Number of dynamic bindings. • **Manual**—Number of static bindings. • **Expired**—Number of expired bindings.

Field	Description
Conflict	Total number of conflict addresses. This field is not displayed if you display statistics for a specific address pool.
Messages received	DHCP packets received from clients: • DHCPDISCOVER. • DHCPREQUEST. • DHCPDECLINE. • DHCPRELEASE. • DHCPINFORM. • BOOTPREQUEST. This field is not displayed if you display statistics for a specific address pool.
Messages sent	DHCP packets sent to clients: • DHCPOFFER. • DHCPACK. • DHCPNAK. • BOOTPREPLY. This field is not displayed if statistics about a specific address pool are displayed.
Bad Messages	Number of bad messages. This field is not displayed if you display statistics for a specific address pool.

Related commands

reset dhcp server statistics

dns-list

Use **dns-list** to specify DNS server addresses in a DHCP address pool.

Use **undo dns-list** to remove DNS server addresses from a DHCP address pool.

Syntax

dns-list *ip-address*&<1-8>

undo dns-list [*ip-address*&<1-8>]

Default

No DNS server address is specified.

Views

DHCP address pool view

Predefined user roles

network-admin

Parameters

ip-address&<1-8>: Specifies DNS servers. &<1-8> indicates that you can specify up to eight DNS server addresses separated by spaces.

Usage guidelines

If you use the **dns-list** command multiple times, the most recent configuration takes effect.

If you do not specify any parameters, the **undo dns-list** command deletes all DNS server addresses in the DHCP address pool.

Examples

# Specify the DNS server address 10.1.1.254 in DHCP address pool 0.

```
<Sysname> system-view
[Sysname] dhcp server ip-pool 0
[Sysname-dhcp-pool-0] dns-list 10.1.1.254
```

Related commands

display dhcp server pool

domain-name

Use **domain-name** to specify a domain name in a DHCP address pool.

Use **undo domain-name** to remove the specified domain name.

Syntax

domain-name *domain-name*

undo domain-name

Default

No domain name is specified.

Views

DHCP address pool view

Predefined user roles

network-admin

Parameters

domain-name: Specifies the domain name, a case-sensitive string of 1 to 50 characters.

Usage guidelines

If you use the command multiple times, the most recent configuration takes effect.

Examples

# Specify the domain name **company.com** in address pool 0.

```
<Sysname> system-view
[Sysname] dhcp server ip-pool 0
[Sysname-dhcp-pool-0] domain-name company.com
```

Related commands

display dhcp server pool

expired

Use **expired** to specify the lease duration in a DHCP address pool.

Use **undo expired** to restore the default lease duration for a DHCP address pool.

Syntax

expired { **day** *day* [**hour** *hour* [**minute** *minute* [**second** *second*]]] **|** **unlimited** }

undo expired

Default

The lease duration of a dynamic DHCP address pool is one day.

Views

DHCP address pool view

Predefined user roles

network-admin

Parameters

day *day*: Specifies the number of days, in the range of 0 to 365.

hour *hour*: Specifies the number of hours, in the range of 0 to 23.

minute *minute*: Specifies the number of minutes, in the range of 0 to 59.

second *second*: Specifies the number of seconds, in the range of 0 to 59.

unlimited: Specifies the unlimited lease duration, which is actually 136 years.

Usage guidelines

The DHCP server assigns an IP address together with the lease duration to the DHCP client. Before the lease expires, the DHCP client must extend the lease duration.

- If the lease extension operation succeeds, the DHCP client can continue to use the IP address.
- If the lease extension operation does not succeed, both of the following events occur:
  - The DHCP client cannot use the IP address after the lease duration expires.
  - The DHCP server will label the IP address as an expired address.

Examples

# Specify the lease duration as 1 day, 2 hours, 3 minutes, and 4 seconds in DHCP address pool 0.

```
<Sysname> system-view
[Sysname] dhcp server ip-pool 0
[Sysname-dhcp-pool-0] expired day 1 hour 2 minute 3 second 4
```

Related commands

- **display dhcp server expired**
- **display dhcp server pool**
- **reset dhcp server expired**

forbidden-ip

Use **forbidden-ip** to exclude IP addresses from dynamic allocation in an address pool.

Use **undo forbidden-ip** to cancel the configuration.

Syntax

forbidden-ip *ip-address*&<1-8>

undo forbidden-ip [*ip-address*&<1-8>]

Default

No IP addresses are excluded from dynamic allocation in an address pool.

Views

DHCP address pool view

Predefined user roles

network-admin

Parameters

ip-address&<1-8>: Specifies excluded IP addresses. &<1-8> indicates that you can specify up to eight IP addresses, separated by spaces.

Usage guidelines

The excluded IP addresses in an address pool are still assignable in other address pools.

You can exclude a maximum of 4096 IP addresses in an address pool.

If you do not specify any parameters, the **undo forbidden-ip** command deletes all excluded IP addresses.

Examples

# Exclude IP addresses 192.168.1.3 and 192.168.1.10 from dynamic allocation in DHCP address pool 0.

```
<Sysname> system-view
[Sysname] dhcp server ip-pool 0
[Sysname-dhcp-pool-0] forbidden-ip 192.168.1.3 192.168.1.10
```

Related commands

- **dhcp server forbidden-ip**
- **display dhcp server pool**

gateway-list

Use **gateway-list** to specify gateway addresses in a DHCP address pool or a DHCP secondary subnet.

Use **undo gateway-list** to remove the specified gateway addresses from a DHCP address pool or a DHCP secondary subnet.

Syntax

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

undo gateway-list [*ip-address*&<1-8>]

Default

No gateway address is configured in a DHCP address pool or a DHCP secondary subnet.

Views

DHCP address pool view, DHCP secondary subnet view

Predefined user roles

network-admin

Parameters

ip-address&<1-8>: Specifies gateways. &<1-8> indicates that you can specify up to eight gateway addresses separated by spaces. Gateway addresses must reside on the same subnet as the assignable IP addresses.

Usage guidelines

If you use this command multiple times, the most recent configuration takes effect.

If you do not specify any parameters, the **undo gateway-list** command deletes all gateway addresses.

If you specify gateways in both address pool view and secondary subnet view, DHCP assigns the gateway addresses in the secondary subnet view to the clients on the secondary subnet.

If you specify gateways in address pool view but not in secondary subnet view, DHCP assigns the gateway addresses in address pool view to the clients on the secondary subnet.

Examples

# Specify the gateway address 10.1.1.1 in DHCP address pool 0.

```
<Sysname> system-view
[Sysname] dhcp server ip-pool 0
[Sysname-dhcp-pool-0] gateway-list 10.1.1.1
```

Related commands

display dhcp server pool

if-match

Use **if-match** to configure a match rule for a DHCP user class.

Use **undo if-match** to remove the match rule for a DHCP user class.

Syntax

if-match rule *rule-number* **option** *option-code* [**hex** *hex-string* [**mask** *mask* | **offset** *offset* **length** *length*]]

undo if-match rule *rule-number*

Default

No match rule is configured for the DHCP user class.

Views

DHCP user class view

Predefined user roles

network-admin

Parameters

rule *rule-number*: Assigns the match rule an ID in the range of 1 to 16. A smaller ID represents a higher match priority.

option *option-code*: Matches a DHCP option by a number in the range of 1 to 254.

hex *hex-string*: Matches the specified hexadecimal string in the option. The length of the hexadecimal string must be an even number in the range of 2 to 256. If you do not specify this option, the DHCP server only checks whether the specified option exists in the received packets.

mask *mask*: Specifies the mask used to match the option content. The *mask* argument is a hexadecimal string, whose length is an even number in the range of 2 to 256. The length of *mask* must be the same as that of *hex-string*.

offset *offset*: Specifies the offset used to match the option, in the range of 0 to 254 bytes. If you do not specify this option, the server matches the entire option with the rule.

length *length*: Matches the specified length of the option, in the range of 1 to 128 bytes. The specified length must be the same as the *hex-string* length.

Usage guidelines

You can configure multiple match rules for a DHCP user class. Each match rule is uniquely identified by a rule ID. Different match rules can include the same option code, but they cannot have the same matching criteria.

The DHCP server compares DHCP requests against the match rules. A DHCP client matches a DHCP user class when its request matches one of the specified match rules.

The match operation follows these guidelines:

- If only the *option-code* argument is specified in the rule, packets containing the option match the rule.
- If the *option-code* and *hex-string* arguments are specified in the rule, packets that have the specified hexadecimal string in the specified option match the rule.
- If the *option-code, hex-string*, *offset and length* arguments are specified in the rule, packets match the rule as long as their content from offset+1 bit to offset+length bit in the specified option is the same as the specified hexadecimal string.
- If the *option-code, hex-string*, and *mask* arguments are specified in the rule, the DHCP server ANDs the content from the first bit to the mask-1 bit in the specified option with the mask. Then the server compares the result with the result of the AND operation between *hex-string* and *mask*. If the two results are the same, the received packet matches the rule.

Examples

# Configure match rule **1** to match DHCP requests that contain Option 82 for DHCP user class **exam**.

```
<Sysname> system-view
[Sysname] dhcp class exam
[Sysname-dhcp-class-exam] if-match rule 1 option 82
```

# Configure match rule **2** to match DHCP requests that contain Option 82. Option 82's first three bytes are 0x13ae92 for the DHCP user class **exam**.

```
<Sysname> system-view
[Sysname] dhcp class exam
[Sysname-dhcp-class-exam] if-match rule 2 option 82 hex 13ae92 offset 0 length 3
```

# Configure match rule **3** to match DHCP requests that contain Option 82. Option 82's highest bit of the fourth byte is 1 for the DHCP user class **exam**.

```
<Sysname> system-view
[Sysname] dhcp class exam
[Sysname-dhcp-class-exam] if-match rule 3 option 82 hex 00000080 mask 00000080
```

Related commands

dhcp class

nbns-list

Use **nbns-list** to specify WINS server addresses in a DHCP address pool.

Use **undo nbns-list** to remove the specified WINS server addresses.

Syntax

nbns-list *ip-address*&<1-8>

undo nbns-list [*ip-address*&<1-8>]

Default

No WINS server address is specified.

Views

DHCP address pool view

Predefined user roles

network-admin

Parameters

ip-address&<1-8>: Specifies WINS server IP addresses. &<1-8> indicates that you can specify up to eight WINS server addresses separated by spaces.

Usage guidelines

If you use this command multiple times, the most recent configuration takes effect.

If you do not specify any parameters, the **undo nbns-list** command deletes all WINS server addresses.

Examples

# Specify the WINS server IP address 10.1.1.1 in DHCP address pool 0.

```
<Sysname> system-view
[Sysname] dhcp server ip-pool 0
[Sysname-dhcp-pool-0] nbns-list 10.1.1.1
```

Related commands

- **display dhcp server pool**
- **netbios-type**

netbios-type

Use **netbios-type** to specify the NetBIOS node type in a DHCP address pool.

Use **undo netbios-type** to remove the specified NetBIOS node type.

Syntax

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

undo netbios-type

Default

No NetBIOS node type is specified.

Views

DHCP address pool view

Predefined user roles

network-admin

Parameters

b-node: Specifies the broadcast node. A b-node client sends the destination name in a broadcast message to get the name-to-IP mapping from a server.

h-node: Specifies the hybrid node. An h-node client unicasts the destination name to a WINS server. If it does not receive a response, the h-node client broadcasts the destination name to get the mapping from a server.

m-node: Specifies the mixed node. An m-node client broadcasts the destination name. If it does not receive a response, the m-node client unicasts the destination name to the WINS server to get the mapping.

p-node: Specifies the peer-to-peer node. A p-node client sends the destination name in a unicast message to get the mapping from the WINS server.

Usage guidelines

If you use the command multiple times, the most recent configuration takes effect.

Examples

# Specify the NetBIOS node type as p-node in DHCP address pool 0.

```
<Sysname> system-view
[Sysname] dhcp server ip-pool 0
[Sysname-dhcp-pool-0] netbios-type p-node
```

Related commands

- **display dhcp server pool**
- **nbns-list**

network

Use **network** to specify the subnet for dynamic allocation in a DHCP address pool.

Use **undo network** to remove the specified subnet.

Syntax

network *network-address* [*mask-length* **| mask** *mask*] [**secondary**]

undo network *network-address* [*mask-length* **| mask** *mask*] [**secondary**]

Default

No subnet is specified in a DHCP address pool.

Views

DHCP address pool view

Predefined user roles

network-admin

Parameters

network-address: Specifies the subnet for dynamic allocation. If no mask length or mask is specified, the natural mask will be used.

mask-length: Specifies the mask length in the range of 1 to 30.

mask *mask*: Specifies the mask in dotted decimal format.

secondary: Specifies the subnet as a secondary subnet. If you do not specify this keyword, this command specifies the primary subnet. If the addresses in the primary subnet are used up, the DHCP server can select addresses from a secondary subnet for clients.

Usage guidelines

You can use the **secondary** keyword to specify a secondary subnet and enter its view, where you can specify gateways by using the **gateway-list** command for DHCP clients in the secondary subnet.

You can specify only one primary subnet for a DHCP address pool. If you use the **network** command multiple times, the most recent configuration takes effect.

You can specify up to 32 secondary subnets for a DHCP address pool.

The primary subnet and secondary subnets in a DHCP address pool must not have the same network address and mask.

If you have used the **address range** or **class** command in an address pool, you cannot specify a secondary subnet in the same address pool.

Modifying or removing the **network** configuration deletes the assigned addresses from the current address pool.

Examples

# Specify primary subnet 192.168.8.0/24 and secondary subnet 192.168.10.0/24 in DHCP address pool 0.

```
<Sysname> system-view
[Sysname] dhcp server ip-pool 0
[Sysname-dhcp-pool-0] network 192.168.8.0 mask 255.255.255.0
[Sysname-dhcp-pool-0] network 192.168.10.0 mask 255.255.255.0 secondary
[Sysname-dhcp-pool-0-secondary]
```

Related commands

- **display dhcp server pool**
- **gateway-list**

next-server

Use **next-server** to specify the IP address of a server in a DHCP address pool.

Use **undo next-server** to remove the server's IP address from the DHCP address pool.

Syntax

next-server *ip-address*

undo next-server

Default

No server's IP address is specified in an address pool.

Views

DHCP address pool view

Predefined user roles

network-admin

Parameters

ip-address: Specifies the IP address of a server.

Usage guidelines

Upon startup, the DHCP client obtains an IP address and the specified server IP address. Then it contacts the specified server, such as a TFTP server, to get other boot information.

If you use the **next-server** command multiple times, the most recent configuration takes effect.

Examples

# Specify a server's IP address 10.1.1.254 in DHCP address pool 0.

```
<Sysname> system-view
[Sysname] dhcp server ip-pool 0
[Sysname-dhcp-pool-0] next-server 10.1.1.254
```

Related commands

display dhcp server pool

option

Use **option** to customize a DHCP option.

Use **undo option** to remove a customized DHCP option.

Syntax

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

undo option *code*

Default

No DHCP option is customized.

Views

DHCP address pool view

Predefined user roles

network-admin

Parameters

code: Specifies the number of the customized option, in the range of 2 to 254, excluding 50 through 54, 56, 58, 59, 61, and 82.

ascii *ascii-string*: Specifies an ASCII string of 1 to 255 characters as the option content.

hex *hex-string*: Specifies a hexadecimal string of even numbers from 2 to 256 as the option content.

ip-address *ip-address*&<1-8>: Specifies the IP addresses as the option content. &<1-8> indicates that you can specify up to eight IP addresses separated by spaces.

Usage guidelines

The DHCP server fills the customized option with the specified ASCII string, hexadecimal string, or IP addresses, and sends it in a response to the client.

If you use the **option** command with the same *code* specified, the most recent configuration takes effect.

You can customize options for the following purposes:

- Add newly released options.
- Add options for which the vendor defines the contents, for example, Option 43.
- Add options for which the CLI does not provide a dedicated configuration command. For example, you can use the **option 4 ip-address 1.1.1.1** command to define the time server address 1.1.1.1 for DHCP clients.
- Add all option values if the actual requirement exceeds the limit for a dedicated option configuration command. For example, the **dns-list** command can specify up to eight DNS servers. To specify more than eight DNS server, you must use the **option 6** command to define all DNS servers.

If a DHCP option is specified by both the dedicated command and the **option** command, the DHCP server assigns the content specified by the dedicated command. For example, if a DNS server address is specified by the **dns-list** command and the **option 6** command, the server uses the address specified by **dns-list** command.

Examples

# Configure Option 7 to specify the log server address 2.2.2.2 in address pool 0.

```
<Sysname> system-view
[Sysname] dhcp server ip-pool 0
[Sysname-dhcp-pool-0] option 7 ip-address 2.2.2.2
```

Related commands

display dhcp server pool

reset dhcp server conflict

Use **reset dhcp server conflict** to clear IP address conflict information.

Syntax

reset dhcp server conflict [**ip** *ip-address*] [**vpn-instance** *vpn-instance-name*]

Views

User view

Predefined user roles

network-admin

Parameters

ip *ip-address*: Clears conflict information about the specified IP address. If you do not specify this option, this command clears all address conflict information.

vpn-instance *vpn-instance-name*: Specifies a VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, this command clears conflict information about IP addresses for the public network.

Usage guidelines

Address conflicts occur when dynamically assigned IP addresses have been statically configured for other hosts. After you modify the address pool configuration, the conflicted addresses might become assignable. To assign these addresses, use the **reset dhcp server conflict** command to clear the conflict information first.

Examples

# Clear all IP address conflict information.

```
<Sysname> reset dhcp server conflict
```

Related commands

display dhcp server conflict

reset dhcp server expired

Use **reset dhcp server expired** to clear binding information about expired IP addresses.

Syntax

reset dhcp server expired [[**ip** *ip-address*] [**vpn-instance** *vpn-instance-name*] | **pool** *pool-name*]

Views

User view

Predefined user roles

network-admin

Parameters

ip *ip-address*: Clears binding information about the specified expired IP address.

vpn-instance *vpn-instance-name*: Specifies a VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, this command clears lease expiration information about IP addresses for the public network.

pool *pool-name*: Clears binding information about the expired IP addresses in the specified address pool. The pool name is a case-insensitive string of 1 to 63 characters.

Usage guidelines

If you do not specify any parameters, this command clears binding information about all expired IP addresses.

Examples

# Clear binding information about all expired IP addresses.

```
<Sysname> reset dhcp server expired
```

Related commands

display dhcp server expired

reset dhcp server ip-in-use

Use **reset dhcp server ip-in-use** to clear binding information about assigned IP addresses.

Syntax

reset dhcp server ip-in-use [[**ip** *ip-address*] [**vpn-instance** *vpn-instance-name*] | **pool** *pool-name*]

Views

User view

Predefined user roles

network-admin

Parameters

ip *ip-address*: Clears binding information about the specified assigned IP address.

vpn-instance *vpn-instance-name*: Specifies a VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, this command clears binding information for the public network.

pool *pool-name*: Clears binding information about the specified address pool. The pool name is a case-insensitive string of 1 to 63 characters.

Usage guidelines

If you do not specify any parameters, this command clears binding information about all assigned IP addresses.

If you use this command to clear information about an assigned static binding, the static binding becomes an unassigned static binding.

Examples

# Clear binding information about the IP address 10.110.1.1.

```
<Sysname> reset dhcp server ip-in-use ip 10.110.1.1
```

Related commands

display dhcp server ip-in-use

reset dhcp server statistics

Use **reset dhcp server statistics** to clear DHCP server statistics.

Syntax

reset dhcp server statistics [**vpn-instance** *vpn-instance-name*]

Views

User view

Predefined user roles

network-admin

Parameters

vpn-instance *vpn-instance-name*: Specifies a VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, this command clears DHCP server statistics for the public network.

Examples

# Clear DHCP server statistics.

```
<Sysname> reset dhcp server statistics
```

Related commands

`display dhcp server statistics`

static-bind

Use **static-bind** to statically bind a client ID or MAC address to an IP address.

Use **undo static-bind** to remove a static binding.

Syntax

static-bind ip-address *ip-address* [*mask-length* **| mask** *mask*] { **client-identifier** *client-identifier* **| hardware-address** *hardware-address* [**ethernet | token-ring**] }

undo static-bind ip-address *ip-address*

Default

No static binding is specified in a DHCP address pool.

Views

DHCP address pool view

Predefined user roles

network-admin

Parameters

ip-address *ip-address*: Specifies the IP address of the static binding. The natural mask is used if no mask length or mask is specified.

mask-length: Specifies the mask length in the range of 1 to 30.

mask *mask*: Specifies the mask, in dotted decimal format.

client-identifier *client-identifier*: Specifies the client ID of the static binding, a string of 4 to 254 characters that can contain only hexadecimal numbers and hyphen (-), in the format of H-H-H…., in which the last H can be a two-digit or four-digit hexadecimal number while the other Hs must be all four-digit hexadecimal numbers. For example, aabb-cccc-dd is a correct ID, while aabb-c-dddd and aabb-cc-dddd are incorrect IDs.

hardware-address *hardware-address*: Specifies the client hardware address of the static binding, a string of 4 to 79 characters that can contain only hexadecimal numbers and hyphen (-), in the format of H-H-H…, in which the last H can be a two-digit or four-digit hexadecimal number while the other Hs must be all four-digit hexadecimal numbers. For example, aabb-cccc-dd is a correct hardware address, while aabb-c-dddd and aabb-cc-dddd are incorrect hardware addresses.

ethernet: Specifies the client hardware address type as Ethernet. The default type is Ethernet.

token-ring: Specifies the client hardware address type as token ring.

Usage guidelines

The IP address of a static binding must not be an interface address of the DHCP server. Otherwise, an IP address conflict occurs, and the bound client cannot obtain the IP address.

You can specify multiple static bindings in an address pool. The total number of static bindings in all address pools cannot exceed 8192.

You cannot modify bindings. To change the binding for a DHCP client, you must delete the existing binding first and create a new binding.

Examples

# Bind the IP address 10.1.1.1/24 to the client ID 00aa-aabb in DHCP address pool 0.

```
<Sysname> system-view
[Sysname] dhcp server ip-pool 0
[Sysname-dhcp-pool-0] static-bind ip-address 10.1.1.1 mask 255.255.255.0
client-identifier 00aa-aabb
```

Related commands

display dhcp server pool

tftp-server domain-name

Use **tftp-server domain-name** to specify a TFTP server name in a DHCP address pool.

Use **undo tftp-server domain-name** to remove the TFTP server name from a DHCP address pool.

Syntax

tftp-server domain-name *domain-name*

undo tftp-server domain-name

Default

No TFTP server name is specified.

Views

DHCP address pool view

Predefined user roles

network-admin

Parameters

domain-name: Specifies the TFTP server name, a case-sensitive string of 1 to 63 characters.

Usage guidelines

If you use this command multiple times, the most recent configuration takes effect.

Examples

# Specify the TFTP server name **aaa** in DHCP address pool 0.

```
<Sysname> system-view
[Sysname] dhcp server ip-pool 0
[Sysname-dhcp-pool-0] tftp-server domain-name aaa
```

Related commands

- **display dhcp server pool**
- **tftp-server ip-address**

tftp-server ip-address

Use **tftp-server ip-address** to specify a TFTP server address in a DHCP address pool.

Use **undo tftp-server ip-address** to remove the TFTP server address from a DHCP address pool.

Syntax

tftp-server ip-address *ip-address*

undo tftp-server ip-address

Default

No TFTP server address is specified.

Views

DHCP address pool view

Predefined user roles

network-admin

Parameters

ip-address: Specifies the IP address of a TFTP server.

Usage guidelines

If you use this command multiple times, the most recent configuration takes effect.

Examples

# Specify the TFTP server address 10.1.1.1 in DHCP address pool 0.

```
<Sysname> system-view
[Sysname] dhcp server ip-pool 0
[Sysname-dhcp-pool-0] tftp-server ip-address 10.1.1.1
```

Related commands

- **display dhcp server pool**
- **tftp-server domain-name**

voice-config

Use **voice-config** to configure the content for Option 184 in a DHCP address pool.

Use **undo voice-config** to remove the Option 184 content from a DHCP address pool.

Syntax

voice-config { **as-ip** *ip-address* **| fail-over** *ip-address dialer-string* **| ncp-ip** *ip-address* **| voice-vlan** *vlan-id* { **disable | enable** } }

undo voice-config [**as-ip | fail-over | ncp-ip | voice-vlan**]

Default

No Option 184 content is configured in a DHCP address pool.

Views

DHCP address pool view

Predefined user roles

network-admin

Parameters

as-ip *ip-address*: Specifies the IP address of the backup network calling processor.

fail-over *ip-address dialer-string*: Specifies the failover IP address and dialer string. The *dialer-string* is a string of 1 to 39 characters, which can include numbers 0 through 9 and asterisk (*).

ncp-ip *ip-address*: Specifies the IP address of the primary network calling processor.

voice-vlan *vlan-id*: Specifies the voice VLAN ID in the range of 2 to 4094.

- **disable**: Disables the specified VLAN. DHCP clients will not take this VLAN as their voice VLAN.
- **enable**: Enables the specified VLAN. DHCP clients will take this VLAN as their voice VLAN.

Usage guidelines

If you use the command multiple times, the most recent configuration takes effect.

Examples

# Configure Option 184 in DHCP address pool 0. The primary and backup network calling processors are at 10.1.1.1 and 10.2.2.2, respectively. The voice VLAN 3 is enabled. The failover IP address is 10.3.3.3. The dialer string is 99*.

```
<Sysname> system-view
[Sysname] dhcp server ip-pool 0
[Sysname-dhcp-pool-0] voice-config ncp-ip 10.1.1.1
[Sysname-dhcp-pool-0] voice-config as-ip 10.2.2.2
[Sysname-dhcp-pool-0] voice-config voice-vlan 3 enable
[Sysname-dhcp-pool-0] voice-config fail-over 10.3.3.3 99*
```

Related commands

display dhcp server pool

vpn-instance

Use **vpn-instance** to apply a DHCP address pool to a VPN instance.

Use **undo vpn-instance** to restore the default.

Syntax

vpn-instance *vpn-instance-name*

undo vpn-instance

Default

The DHCP address pool is not applied to any VPN instance.

Views

DHCP address pool view

Predefined user roles

network-admin

Parameters

vpn-instance-name: Specifies a VPN instance by its name, a case-sensitive string of 1 to 31 characters.

Usage guidelines

If a DHCP address pool is applied to a VPN instance, the DHCP server assigns IP addresses in this address pool to clients in the specified VPN instance.

The DHCP server identifies the VPN instance to which a DHCP client belongs according to the following information:

- The client's VPN information stored in authentication modules.
- The VPN information of the DHCP server's interface that receives DHCP packets from the client.

The VPN information from authentication modules takes priority over the VPN information of the receiving interface.

Examples

# Apply DHCP address pool 0 to VPN instance **abc**.

```
<Sysname> system-view
[Sysname] dhcp server ip-pool 0
[Sysname-dhcp-pool-0] vpn-instance abc
```

DHCP relay agent commands

The term "interface" in this section refers to VLAN interfaces.

dhcp relay check mac-address

Use **dhcp relay check mac-address** to enable MAC address check on the relay agent.

Use **undo dhcp relay check mac-address** to disable MAC address check on the relay agent.

Syntax

dhcp relay check mac-address

undo dhcp relay check mac-address

Default

The MAC address check feature is disabled.

Views

Interface view

Predefined user roles

network-admin

Usage guidelines

This feature enables the DHCP relay agent to compare the **chaddr** field of a received DHCP request with the source MAC address in the frame header. If they are the same, the DHCP relay agent forwards the request to the DHCP server. If they are not the same, the DHCP relay agent discards the request.

The MAC address check feature takes effect only when the **dhcp select relay** command has already been configured on the interface.

Enable the MAC address check feature only on the DHCP relay agent directly connected to the DHCP clients. A DHCP relay agent changes the source MAC address of DHCP packets before sending them. If you enable this feature on an intermediate relay agent, it might discard valid DHCP packet, and the sending clients will not obtain IP addresses.

Examples

# Enable MAC address check on the relay agent.

```
<Sysname> system-view
[Sysname] interface vlan-interface 10
```

```
[Sysname-Vlan-interface10] dhcp relay check mac-address
```

Related commands

dhcp select relay

dhcp relay check mac-address aging time

Use **dhcp relay check mac-address aging time** to configure the aging time for MAC address check entries on the DHCP relay agent.

Use **undo dhcp relay check mac-address aging time** to restore the default.

Syntax

dhcp relay check mac-address aging-time *time*

undo dhcp relay check mac-address aging-time

Default

The aging time is 30 seconds.

Views

System view

Predefined user roles

network-admin

Parameters

time: Specifies the aging time for MAC address check entries in seconds, in the range of 30 to 600.

Usage guidelines

This command takes effect only after you execute the **dhcp relay check mac-address** command.

Examples

# Set the aging time for MAC address check entries on the DHCP relay agent to 60 seconds.

```
<Sysname> system-view
[Sysname] dhcp relay check mac-address aging-time 60
```

dhcp relay client-information record

Use **dhcp relay client-information record** to enable recording client information in relay entries. A relay entry contains information about a client such as the client's IP and MAC addresses.

Use **undo dhcp relay client-information record** to disable the feature.

Syntax

dhcp relay client-information record

undo dhcp relay client-information record

Default

The DHCP relay agent does not record client information in relay entries.

Views

System view

Predefined user roles

network-admin

Usage guidelines

Disabling recording of client information deletes all recorded relay entries.

Client information is recorded only when the DHCP relay agent is configured on the gateway of DHCP clients.

Examples

# Enable recording of relay entries on the relay agent.

```
<Sysname> system-view
[Sysname] dhcp relay client-information record
```

Related commands

- **dhcp relay client-information refresh**
- **dhcp relay client-information refresh enable**

dhcp relay client-information refresh

Use **dhcp relay client-information refresh** to configure the interval at which the DHCP relay agent periodically refreshes relay entries.

Use **undo dhcp relay client-information refresh** to restore the default.

Syntax

dhcp relay client-information refresh [**auto** | **interval** *interval*]

undo dhcp relay client-information refresh

Default

The refresh interval is automatically calculated based on the number of relay entries.

Views

System view

Predefined user roles

network-admin

Parameters

auto: Automatically calculates the refresh interval. The more the entries, the shorter the refresh interval. The shortest interval must not be less than 500 ms.

interval *interval*: Specifies the refresh interval in the range of 1 to 120 seconds.

Usage guidelines

If you use this command multiple times, the most recent configuration takes effect.

Examples

# Set the refresh interval to 100 seconds.

```
<Sysname> system-view
[Sysname] dhcp relay client-information refresh interval 100
```

Related commands

- **dhcp relay client-information record**
- **dhcp relay client-information refresh enable**

dhcp relay client-information refresh enable

Use **dhcp relay client-information refresh enable** to enable the DHCP relay agent to periodically refresh dynamic relay entries.

Use **undo dhcp relay client-information refresh enable** to disable the DHCP relay agent to periodically refresh dynamic relay entries.

Syntax

dhcp relay client-information refresh enable

undo dhcp relay client-information refresh enable

Default

The DHCP relay agent periodically refreshes relay entries.

Views

System view

Predefined user roles

network-admin

Usage guidelines

A DHCP client unicasts a DHCP-RELEASE message to the DHCP server to release its IP address. The DHCP relay agent conveys the message to the DHCP server and does not remove the IP-to-MAC entry of the client.

With this feature, the DHCP relay agent uses the IP address of a client and the MAC address of the DHCP relay interface to periodically send a DHCP-REQUEST message to the DHCP server.

- If the server returns a DHCP-ACK message or does not return any message within an interval, the DHCP relay agent performs the following operations:
  - Removes the relay entry.
  - Sends a DHCP-RELEASE message to the DHCP server to release the IP address.
- If the server returns a DHCP-NAK message, the relay agent keeps the entry.

With this feature disabled, the DHCP relay agent does not remove relay entries automatically. After a DHCP client releases its IP address, you must use the **reset dhcp relay client-information** on the relay agent to remove the corresponding relay entry.

Examples

# Disable periodic refresh of relay entries.

```
<Sysname> system-view
[Sysname] undo dhcp relay client-information refresh enable
```

Related commands

- **dhcp relay client-information record**
- **dhcp relay client-information refresh**
- **reset dhcp relay client-information**

dhcp relay information circuit-id

Use **dhcp relay information circuit-id** to configure the padding mode and padding format for the Circuit ID sub-option of Option 82.

Use **undo dhcp relay information circuit-id** to restore the default.

Syntax

dhcp relay information circuit-id { **string** *circuit-id* | { **normal** | **verbose** [**node-identifier** { **mac** | **sysname** | **user-defined** *node-identifier* }] } [**format** { **ascii** | **hex** }] }

undo dhcp relay information circuit-id

Default

The padding mode is **normal** and the padding format is **hex**.

Views

Interface view

Predefined user roles

network-admin

Parameters

string *circuit-id*: Specifies the string mode that uses a case-sensitive string of 3 to 63 characters as the content of the Circuit ID sub-option.

normal: Specifies the normal mode, in which the padding content consists of the VLAN ID and port number.

verbose: Specifies the verbose mode. The padding content includes the VLAN ID and interface number.

node-identifier { **mac** | **sysname** | **user-defined** *node-identifier* }: Specifies the access node identifier. The padding content includes the node identifier, Ethernet type (fixed to **eth**), interface number, and VLAN ID. The node identifier varies by keyword **mac**, **sysname**, and **user-defined**.

- **mac**: Uses the MAC address of the access node as the node identifier. It is the default node identifier.
- **sysname**: Uses the device name as the node identifier. You can set the device name by using the **sysname** command in system view. The padding format for the device name is always ASCII regardless of the specified padding format.

NOTE:

If **sysname** is used as the node identifier, do not include any space when you set the device name. Otherwise, the DHCP relay agent fails to add or replace the Option 82.

- **user-defined** *node-identifier:* Uses a case-sensitive string of 1 to 50 characters as the node identifier. The padding format for the specified character string is always ASCII regardless of the specified padding format.

format: Specifies the padding format for the Circuit ID sub-option.

ascii: Specifies the padding format as ASCII.

hex: Specifies the padding format as hex.

Usage guidelines

If you use this command multiple times, the most recent configuration takes effect.

The padding format for the user-defined string, the normal mode, or the verbose modes varies by command configuration. Table 7 shows how the padding format is determined for different modes.

Table 7 Padding format for different modes

Keyword (mode)	If no padding format is specified	If the padding format is ascii	If the padding format is hex
string *circuit-id*	You cannot specify a padding format, and the padding format is always ASCII.	N/A	N/A
normal	Hex.	ASCII.	Hex.
verbose	Hex for the VLAN ID. ASCII for the node identifier, Ethernet type, and interface number.	ASCII.	ASCII for the node identifier and Ethernet type. Hex for the interface number and VLAN ID.

Examples

# Specify the padding mode as verbose, node identifier as the device name, and the padding format as ASCII for the Circuit ID sub-option.

```
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] dhcp relay information enable
[Sysname-Vlan-interface10] dhcp relay information strategy replace
[Sysname-Vlan-interface10] dhcp relay information circuit-id verbose node-identifier
sysname format ascii
```

Related commands

- **dhcp relay information enable**
- **dhcp relay information strategy**
- **display dhcp relay information**

dhcp relay information enable

Use **dhcp relay information enable** to enable the relay agent to support Option 82.

Use **undo dhcp relay information enable** to disable Option 82 support.

Syntax

dhcp relay information enable

undo dhcp relay information enable

Default

The DHCP relay agent does not support Option 82.

Views

Interface view

Predefined user roles

network-admin

Usage guidelines

This command enables the DHCP relay agent to add Option 82 to DHCP requests that do not contain Option 82 before forwarding the requests to the DHCP server. The content of Option 82 is determined by the **dhcp relay information circuit-id** and **dhcp relay information remote-id** commands. If the DHCP requests contain Option 82, the relay agent handles the requests according to the strategy configured with the **dhcp relay information strategy** command.

If this feature is disabled, the relay agent forwards requests that contain or do not contain Option 82 to the DHCP server.

Examples

# Enable Option 82 support on the relay agent.

```
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] dhcp relay information enable
```

Related commands

- **dhcp relay information circuit-id**
- **dhcp relay information remote-id**
- **dhcp relay information strategy**
- **display dhcp relay information**

dhcp relay information remote-id

Use **dhcp relay information remote-id** to configure the padding mode and padding format for the Remote ID sub-option of Option 82.

Use **undo dhcp relay information remote-id** to restore the default.

Syntax

dhcp relay information remote-id { **normal** [**format** { **ascii** | **hex** }] | **string** *remote-id* | **sysname** }

undo dhcp relay information remote-id

Default

The padding mode is **normal** and the padding format is **hex**.

Views

Interface view

Predefined user roles

network-admin

Parameters

normal: Specifies the normal mode in which the padding content is the MAC address of the receiving interface.

format: Specifies the padding format for the Remote ID sub-option. The default padding format is hex.

ascii: Specifies the padding format as ASCII.

hex: Specifies the padding format as hex.

string *remote-id*: Specifies the string mode that uses a case-sensitive string of 1 to 63 characters as the content of the Remote ID sub-option.

sysname: Specifies the sysname mode that uses the device name as the content of the Remote ID sub-option. You can set the device name by using the **sysname** command.

Usage guidelines

The padding format for the specified character string (**string**) or the device name (**sysname**) is always ASCII. The padding format for the **normal** mode is determined by the command.

If you use the command multiple times, the most recent configuration takes effect.

Examples

# Specify the padding content for the Remote ID sub-option of Option 82 as **device001**.

```
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] dhcp relay information enable
[Sysname-Vlan-interface10] dhcp relay information strategy replace
[Sysname-Vlan-interface10] dhcp relay information remote-id string device001
```

Related commands

- **dhcp relay information enable**
- **dhcp relay information strategy**
- **display dhcp relay information**

dhcp relay information strategy

Use **dhcp relay information strategy** to configure the strategy for the DHCP relay agent to handle messages containing Option 82.

Use **undo dhcp relay information strategy** to restore the default handling strategy.

Syntax

dhcp relay information strategy { **drop** | **keep** | **replace** }

undo dhcp relay information strategy

Default

The handling strategy for messages that contain Option 82 is **replace**.

Views

Interface view

Predefined user roles

network-admin

Parameters

drop: Drops DHCP messages that contain Option 82 messages.

keep: Keeps the original Option 82 intact.

replace: Replaces the original Option 82 with the configured Option 82.

Usage guidelines

This command takes effect only on DHCP requests that contain Option 82.

When enabled to support Option 82, the DHCP relay agent always adds Option 82 into DHCP requests that do not contain Option 82 before forwarding the requests to the DHCP.

Examples

# Specify the handling strategy for Option 82 as **keep**.

```
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] dhcp relay information enable
[Sysname-Vlan-interface10] dhcp relay information strategy keep
```

Related commands

- **dhcp relay information enable**
- **display dhcp relay information**

dhcp relay release ip

Use **dhcp relay release ip** to release a specific client IP address.

Syntax

dhcp relay release ip *client-ip* [**vpn-instance** *vpn-instance-name*]

Views

System view

Predefined user roles

network-admin

Parameters

client-ip: Specifies the IP address to be released.

vpn-instance *vpn-instance-name*: Specifies the VPN instance of the IP address. The *vpn-instance-name* is a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, this command releases the IP address in the public network.

Usage guidelines

After you execute this command, the relay agent sends a DHCP-RELEASE packet to the DHCP server and removes the relay entry of the IP address. Upon receiving the packet, the server removes binding information about the specified IP address to release the IP address.

Examples

# Release the IP address 1.1.1.1.

```
<Sysname> system-view
[Sysname] dhcp relay release ip 1.1.1.1
```

dhcp relay server-address

Use **dhcp relay server-address** to specify DHCP servers on the DHCP relay agent.

Use **undo dhcp relay server-address** to remove DHCP servers.

Syntax

dhcp relay server-address *ip-address*

undo dhcp relay server-address [*ip-address*]

Default

No DHCP server is specified on the DHCP relay agent.

Views

Interface view

Predefined user roles

network-admin

Parameters

ip-address: Specifies the IP address of a DHCP server. The DHCP relay agent forwards DHCP packets received from DHCP clients to this DHCP server.

Usage guidelines

The specified IP address of the DHCP server must not reside on the same subnet as the IP address of the DHCP relay agent interface. Otherwise, the DHCP clients might fail to obtain IP addresses.

You can specify a maximum of eight DHCP servers on an interface. The DHCP relay agent forwards the packets from the clients to all the specified DHCP servers.

If you do not specify an IP address, the **undo dhcp relay server-address** command removes all DHCP servers on the interface.

Examples

# Specify the DHCP server 1.1.1.1 on the relay agent interface VLAN-interface 10.

```
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] dhcp relay server-address 1.1.1.1
```

Related commands

- **dhcp select relay**
- **display dhcp relay interface**

dhcp smart-relay enable

Use **dhcp smart-relay enable** to enable the DHCP smart relay feature.

Use **undo dhcp smart-relay enable** to disable the DHCP smart relay feature.

Syntax

dhcp smart-relay enable

undo dhcp smart-relay enable

Default

The DHCP smart relay feature is disabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

The smart relay feature allows the relay agent to use secondary IP addresses as the gateway address when the DHCP server does not reply the DHCP-OFFER message. The relay agent initially inserts its primary IP address in the **giaddr** field before forwarding a request to the DHCP server. If no DHCP-OFFER is returned after two retries, the relay agent switches to secondary IP addresses.

Without this feature, the relay agent always uses the primary IP address as the gateway address.

Examples

# Enable the DHCP smart relay feature.

```
<Sysname> system-view
[Sysname] dhcp smart-relay enable
```

display dhcp relay check mac-address

Use **display dhcp relay check mac-address** to display MAC address check entries on the relay agent.

Syntax

display dhcp relay check mac-address

Views

Any view

Predefined user roles

network-admin

network-operator

Examples

# Display MAC address check entries on the DHCP relay agent.

```
<Sysname> display dhcp relay check mac-address
Source-MAC        Interface                 Aging-time
23f3-1122-adf1    XGE1/0/1                  10
23f3-1122-2230    XGE1/0/2                  30
```

Table 8 Command output

Field	Description
Source MAC	Source MAC address of the attacker.
Interface	Interface where the attack comes from.
Aging-time	Aging time of the MAC address check entry, in seconds.

display dhcp relay client-information

Use **display dhcp relay client-information** to display relay entries on the relay agent.

Syntax

display dhcp relay client-information [**interface** *interface-type interface-number* **|** **ip** *ip-address* [**vpn-instance** *vpn-instance-name*]]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

interface *interface-type interface-number*: Displays relay entries on the specified interface.

ip *ip-address*: Displays the relay entry for the specified IP address.

vpn-instance *vpn-instance-name*: Displays the relay entry for the specified IP address in the specified VPN instance. The *vpn-instance-name* is a case-sensitive string of 1 to 31 characters.

Usage guidelines

The DHCP relay agent records relay entries only when the **dhcp relay client-information record** command has been issued.

If you do not specify any parameters, the **display dhcp relay client-information** command displays all relay entries on the relay agent.

Examples

# Display all relay entries on the relay agent.

```
<Sysname> display dhcp relay client-information
Total number of client-information items: 2
Total number of dynamic items: 1
Total number of temporary items: 1
IP address       MAC address      Type        Interface           VPN name
10.1.1.1         00e0-0000-0001   Dynamic     Vlan1               VPN1
10.1.1.5         00e0-0000-0000   Temporary   Vlan2               VPN2
```

Table 9 Command output

Field	Description
Total number of client-information items	Total number of relay entries.
Total number of dynamic items	Total number of dynamic relay entries.
Total number of temporary items	Total number of temporary relay entries.
IP address	IP address of the DHCP client.
MAC address	MAC address of the DHCP client.
Type	Relay entry type: • **Dynamic**—The relay agent creates a dynamic relay entry upon receiving an ACK response from the DHCP server. • **Temporary**—The relay agent creates a temporary relay entry upon receiving a REQUEST packet from a DHCP client.
Interface	Layer 3 interface connected to the DHCP client. **N/A** is displayed for relay entries without interface information.

Related commands

- **dhcp relay client-information record**
- **reset dhcp relay client-information**

display dhcp relay information

Use **display dhcp relay information** to display Option 82 configuration information for the DHCP relay agent.

Syntax

display dhcp relay information [**interface** *interface-type interface-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

interface *interface-type interface-number*: Displays Option 82 configuration information for the specified interface. If you do not specify an interface, this command displays Option 82 configuration information about all interfaces.

Examples

# Display Option 82 configuration information for all interfaces.

```
<Sysname> display dhcp relay information
Interface: Vlan-interface100
   Status: Enable
   Strategy: Replace
   Circuit ID Pattern: Verbose
   Remote ID Pattern: Sysname
   Circuit ID format-type: Undefined
   Remote ID format-type: ASCII
   Node identifier: aabbcc
Interface: Vlan-interface200
   Status: Enable
   Strategy: Replace
   Circuit ID Pattern: User Defined
   Remote ID Pattern: User Defined
   Circuit ID format-type: ASCII
   Remote ID format-type: ASCII
   User defined:
   Circuit ID: vlan100
   Remote ID: device001
```

Table 10 Command output

Field	Description
Interface	Interface name.
Status	Option 82 states: • **Enable**—DHCP relay agent support for Option 82 is enabled. • **Disable**—DHCP relay agent support for Option 82 is disabled.
Strategy	Handling strategy for request messages containing Option 82, **Drop**, **Keep**, or **Replace**.
Circuit ID Pattern	Padding content mode of the Circuit ID sub-option, **Verbose**, **Normal**, or **User Defined**.
Remote ID Pattern	Padding content mode of the Remote ID sub-option, **Sysname**, **Normal**, or **User Defined**.
Circuit ID format-type	Padding format of the Circuit ID sub-option, **ASCII**, **Hex**, or **Undefined**.
Remote ID format-type	Padding format of the Remote ID sub-option, **ASCII**, **Hex**, or **Undefined**.
Node identifier	Access node identifier.
User defined	Content of the user-defined sub-options.
Circuit ID	User-defined content of the Circuit ID sub-option.
Remote ID	User-defined content of the Remote ID sub-option.

display dhcp relay server-address

Use **display dhcp relay server-address** to display DHCP server addresses configured on an interface.

Syntax

display dhcp relay server-address [**interface** *interface-type interface-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

interface *interface-type interface-number*: Displays DHCP server addresses on the specified interface. If you do not specify an interface, this command displays DHCP server addresses on all interfaces operating in DHCP relay agent mode.

Examples

# Display DHCP server addresses on all interfaces.

```
<Sysname> display dhcp relay server-address
Interface name                  Server IP address
Vlan1                           2.2.2.2
```

Table 11 Command output

Field	Description
Interface name	Interface name.
Server IP address	DHCP server IP address.

Related commands

dhcp relay server-address

display dhcp relay statistics

Use **display dhcp relay statistics** to display DHCP packet statistics on the DHCP relay agent.

Syntax

display dhcp relay statistics [**interface** *interface-type interface-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

interface *interface-type interface-number*: Displays DHCP packet statistics on the specified interface. If you do not specify an interface, this command displays all DHCP packet statistics on the DHCP relay agent.

Examples

# Display all DHCP packet statistics on the DHCP relay agent.

```
<Sysname> display dhcp relay statistics
DHCP packets dropped:                  0
DHCP packets received from clients:    0
   DHCPDISCOVER:                       0
   DHCPREQUEST:                        0
   DHCPINFORM:                         0
   DHCPRELEASE:                        0
   DHCPDECLINE:                        0
   BOOTPREQUEST:                       0
DHCP packets received from servers:    0
   DHCPOFFER:                          0
   DHCPACK:                            0
   DHCPNAK:                            0
   BOOTPREPLY:                         0
DHCP packets relayed to servers:       0
   DHCPDISCOVER:                       0
   DHCPREQUEST:                        0
   DHCPINFORM:                         0
   DHCPRELEASE:                        0
   DHCPDECLINE:                        0
   BOOTPREQUEST:                       0
DHCP packets relayed to clients:       0
   DHCPOFFER:                          0
   DHCPACK:                            0
   DHCPNAK:                            0
   BOOTPREPLY:                         0
DHCP packets sent to servers:          0
   DHCPDISCOVER:                       0
   DHCPREQUEST:                        0
   DHCPINFORM:                         0
   DHCPRELEASE:                        0
   DHCPDECLINE:                        0
   BOOTPREQUEST:                       0
DHCP packets sent to clients:          0
   DHCPOFFER:                          0
   DHCPACK:                            0
   DHCPNAK:                            0
   BOOTPREPLY:                         0
```

Related commands

reset dhcp relay statistics

reset dhcp relay client-information

Use **reset dhcp relay client-information** to clear relay entries on the DHCP relay agent.

Syntax

reset dhcp relay client-information [**interface** *interface-type interface-number* **|** **ip** *ip-address* [**vpn-instance** *vpn-instance-name*]]

Views

User view

Predefined user roles

network-admin

Parameters

interface *interface-type interface-number*: Clears relay entries on the specified interface.

ip *ip-address*: Clears the relay entry for the specified IP address.

vpn-instance *vpn-instance-name*: Clears the relay entry for the specified IP address in the specified VPN instance. The *vpn-instance-name* is a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, this command clears the relay entry in the public network.

Usage guidelines

If you do not specify any parameters, this command clears all relay entries on the DHCP relay agent.

Examples

# Clear all relay entries on the DHCP relay agent.

```
<Sysname> reset dhcp relay client-information
```

Related commands

display dhcp relay client-information

reset dhcp relay statistics

Use **reset dhcp relay statistics** to clear relay agent statistics.

Syntax

reset dhcp relay statistics [**interface** *interface-type interface-number*]

Views

User view

Predefined user roles

network-admin

Parameters

interface *interface-type interface-number*: Clears DHCP relay agent statistics on the specified interface. If you do not specify an interface, this command clears all DHCP relay agent statistics.

Examples

# Clear all DHCP relay agent statistics.

```
<Sysname> reset dhcp relay statistics
```

Related commands

display dhcp relay statistics

DHCP client commands

dhcp client dad enable

Use **dhcp client dad enable** to enable duplicate address detection.

Use **undo dhcp client dad enable** to disable duplicate address detection.

Syntax

dhcp client dad enable

undo dhcp client dad enable

Default

Duplicate address detection is enabled on an interface.

Views

System view

Predefined user roles

network-admin

Usage guidelines

DHCP client detects IP address conflict through ARP packets. An attacker can act as the IP address owner to send an ARP reply, which makes the client unable to use the IP address assigned by the server. As a best practice, disable duplicate address detection when ARP attacks exist on the network.

Examples

# Disable the duplicate address.

```
<Sysname> system-view
[Sysname] undo dhcp client dad enable
```

dhcp client dscp

Use **dhcp client dscp** to set the DSCP value for DHCP packets sent by the DHCP client.

Use **undo dhcp client dscp** to restore the default.

Syntax

dhcp client dscp *dscp-value*

undo dhcp client dscp

Default

The DSCP value in DHCP packets is 56.

Views

System view

Predefined user roles

network-admin

Parameters

dscp-value: Sets the DSCP value for DHCP packets, in the range of 0 to 63.

Usage guidelines

The DSCP value of a packet specifies the priority level of the packet and affects the transmission priority of the packet. A bigger DSCP value represents a higher priority.

Examples

# Set the DSCP value for DHCP packets sent by the DHCP client to 30.

```
<Sysname> system-view
[Sysname] dhcp client dscp 30
```

dhcp client identifier

Use **dhcp client identifier** to configure a DHCP client ID for an interface.

Use **undo dhcp client identifier** to restore the default.

Syntax

dhcp client identifier { **ascii** *string* **|** **hex** *string* **|** **mac** *interface-type interface-number* }

undo dhcp client identifier

Default

An interface generates an ASCII character string as the DHCP client ID based on its MAC address and the interface name.

Views

Interface view

Predefined user roles

network-admin

Parameters

ascii *string*: Specifies a case-sensitive ASCII string of 1 to 63 characters as the client ID.

hex *string*: Specifies a hexadecimal string of 4 to 64 characters as the client ID.

mac *interface-type interface-number*: Uses the MAC address of the specified interface as a DHCP client ID. The *interface-type interface-number* argument specifies an interface by its type and number.

Usage guidelines

A DHCP client ID is added to the DHCP option 61. A DHCP server can specify IP addresses for clients based on the DHCP client ID. You can specify a DHCP client ID by performing one of the following operations:

- Naming an ASCII string or hexadecimal string as the client ID.
- Using the MAC address of an interface to generate a client ID.

Whichever method you use, make sure the IDs for different DHCP clients are unique.

Examples

# Specify the hexadecimal string of FFFFFFF as the client ID for VLAN-interface 10.

```
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] dhcp client identifier hex FFFFFFFF
```

Related commands

display dhcp client

display dhcp client

Use **display dhcp client** to display DHCP client information.

Syntax

display dhcp client [**verbose**] [**interface** *interface-type interface-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

verbose: Displays verbose DHCP client information.

interface *interface-type interface-number*: Specifies an interface by its type and number.

Usage guidelines

If you do not specify an interface, this command displays DHCP client information about all interfaces.

Examples

# Display DHCP client information about all interfaces.

```
<Sysname> display dhcp client
Vlan-interface10 DHCP client information:
 Current state: BOUND
 Allocated IP: 40.1.1.20 255.255.255.0
 Allocated lease: 259200 seconds, T1: 129600 seconds, T2: 226800 seconds
 DHCP server: 40.1.1.2
```

# Display verbose DHCP client information.

```
<Sysname> display dhcp client verbose
Vlan-interface10 DHCP client information:
 Current state: BOUND
 Allocated IP: 40.1.1.20 255.255.255.0
 Allocated lease: 259200 seconds, T1: 129600 seconds, T2: 226800 seconds
 Lease from May 21 19:00:29 2012   to   May 31 19:00:29 2012
 DHCP server: 40.1.1.2
 Transaction ID: 0x1c09322d
 Default router: 40.1.1.2
 Classless static routes:
   Destination: 1.1.0.1, Mask: 255.0.0.0, NextHop: 192.168.40.16
   Destination: 10.198.122.63, Mask: 255.255.255.255, NextHop: 192.168.40.16
 DNS servers: 44.1.1.11 44.1.1.12
 Domain name: ddd.com
 Boot servers: 200.200.200.200  1.1.1.1
 Client ID type: acsii(type value=00)
 Client ID value: 000c.29d3.8659-Vlan1
 Client ID (with type) hex: 0030-3030-632e-3239-
                            6433-2e38-3635-392d-
```

```
                         4574-6830-2f30-2f32
 T1 will timeout in 1 day 11 hours 58 minutes 52 seconds.
```

Table 12 Command output

Field	Description
Vlan-interface10 DHCP client information	Information about the interface that acts as the DHCP client.
Current state	Current state of the DHCP client: • **HALT**—The client stops applying for an IP address. • **INIT**—The initialization state. • **SELECTING**—The client has sent out a DHCP-DISCOVER message in search for a DHCP server and is waiting for the response from DHCP servers. • **REQUESTING**—The client has sent out a DHCP-REQUEST message requesting for an IP address and is waiting for the response from DHCP servers. • **BOUND**—The client has received the DHCP-ACK message from a DHCP server and obtained an IP address successfully. • **RENEWING**—The T1 timer expires. • **REBOUNDING**—The T2 timer expires.
Allocated IP	IP address allocated by the DHCP server.
Allocated lease	Allocated lease time.
T1	1/2 lease time (in seconds) of the DHCP client IP address.
T2	7/8 lease time (in seconds) of the DHCP client IP address.
Lease from….to….	Start and end time of the lease.
DHCP server	DHCP server IP address that assigned the IP address.
Transaction ID	Transaction ID, a random number chosen by the client to identify an IP address allocation.
Default router	Gateway address assigned to the client.
Classless static routes	Classless static routes assigned to the client.
Static routes	Classful static routes assigned to the client.
DNS servers	DNS server address assigned to the client.
Domain name	Domain name suffix assigned to the client.
Boot servers	PXE server addresses (up to 16 addresses) specified for the DHCP client, which are obtained through Option 43.
Client ID type	DHCP client ID type: • If an ASCII string is used as the client ID value, the type value is 00. • If the MAC address of a specific interface is used as the client ID value, the type value is 01. • If a hexadecimal string is used as the client ID value, the type value is the first two characters in the string.
Client ID value	Value of the DHCP client ID.
Client ID (with type) hex	DHCP client ID with the type field, a hexadecimal string.
T1 will timeout in 1 day 11 hours 58 minutes 52 seconds.	How long the T1 (1/2 lease time) timer will timeout.

Related commands

- **dhcp client identifier**
- **ip address dhcp-alloc**

ip address dhcp-alloc

Use **ip address dhcp-alloc** to configure an interface to use DHCP for IP address acquisition.

Use **undo ip address dhcp-alloc** to cancel an interface from using DHCP.

Syntax

ip address dhcp-alloc

undo ip address dhcp-alloc

Default

An interface does not use DHCP for IP address acquisition.

Views

Interface view

Predefined user roles

network-admin

Usage guidelines

When you execute the **undo ip address dhcp-alloc** command, the interface sends a DHCP-RELEASE message to release the IP address obtained through DHCP. If the interface is down, the message cannot be sent out.

Examples

# Configure VLAN-interface 10 to use DHCP for IP address acquisition.

```
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] ip address dhcp-alloc
```

DHCP snooping commands

DHCP snooping works between the DHCP client and the DHCP server or between the DHCP client and the relay agent. DHCP snooping does not work between the DHCP server and the DHCP relay agent.

dhcp snooping binding database filename

Use **dhcp snooping binding database filename** to configure the DHCP snooping device to back up DHCP snooping entries to a file.

Use **undo dhcp snooping binding database filename** to disable the auto backup and remove the backup file.

Syntax

dhcp snooping binding database filename { *filename* | **url** *url* [**username** *username* [**password** { **cipher** | **simple** } *key*]] }

undo dhcp snooping binding database filename

Default

The DHCP snooping device does not back up DHCP snooping entries.

Views

System view

Predefined user roles

network-admin

Parameters

filename: Specifies the name of a local file. For information about the *filename* argument, see *Fundamentals Configuration Guide*.

url *url*: Specifies the URL of a remote file. Do not include any username or password in the URL. Case sensitivity and the supported path format type vary by server.

username *username*: Specifies the username for logging in to the remote device.

cipher: Sets a ciphertext password.

simple: Sets a plaintext password.

key: Specifies the key string. This argument is case sensitive. If **simple** is specified, it must be a string of 1 to 32 characters. If **cipher** is specified, it must be a ciphertext string of 1 to 73 characters.

Usage guidelines

For security purposes, all passwords, including passwords configured in plaintext, are saved in ciphertext.

With this command executed, the DHCP snooping device backs up DHCP snooping entries immediately and runs auto backup. The command automatically creates the file if you specify a non-existent file. The DHCP snooping device, by default, waits 300 seconds after a DHCP snooping entry change to update the backup file. To change the waiting period, use the **dhcp snooping binding database update interval** command. If no DHCP snooping entry changes, the backup file is not updated.

When the file is on a remote device, follow these restrictions and guidelines to specify the URL, username, and password:

- If the file is on an FTP server, enter URL in the following format: ftp://*server address:port/file path*, where the port number is optional.
- If the file is on a TFTP server, enter URL in the following format: tftp://*server address:port/file path*, where the port number is optional.
- The username and password must be the same as those configured on the FTP or TFTP server. If the server authenticates only the username, the password can be omitted. For example, enter URL **ftp://1.1.1.1/database.dhcp username admin** to specify the URL and username options at the CLI.
- If the IP address of the server is an IPv6 address, enclose the address in a pair of brackets, for example, **ftp://[1::1]/database.dhcp**.
- You can also specify the DNS domain name for the server address field, for example, **ftp://company/database.dhcp**.

Examples

# Configure the DHCP snooping device to back up DHCP snooping entries to the file **database.dhcp**.

```
<Sysname> system-view
[Sysname] dhcp snooping binding database filename database.dhcp
```

# Configure the DHCP snooping device to back up DHCP snooping entries to the file **database.dhcp** in the working directory of the FTP server at 10.1.1.1.

```
<Sysname> system-view
[Sysname] dhcp snooping binding database filename url ftp://10.1.1.1/database.dhcp
username 1 password simple 1
```

# Configure the DHCP snooping device to back up DHCP snooping entries to the file **database.dhcp** in the working directory of the TFTP server at 10.1.1.1.

```
<Sysname> system-view
[Sysname] dhcp snooping binding database filename tftp://10.1.1.1/database.dhcp
```

Related commands

dhcp snooping binding database update interval

dhcp snooping binding database update interval

Use **dhcp snooping binding database update interval** to set the waiting time after a DHCP snooping entry change for the DHCP snooping device to update the backup file.

Use **undo dhcp snooping binding database update interval** to restore the default.

Syntax

dhcp snooping binding database update interval *seconds*

undo dhcp snooping binding database update interval

Default

The DHCP snooping device waits 300 seconds after a DHCP snooping entry change to update the backup file. If no DHCP snooping entry changes, the backup file is not updated.

Views

System view

Predefined user roles

network-admin

Parameters

seconds: Sets the waiting time in seconds, in the range of 60 to 864000.

Usage guidelines

When a DHCP snooping entry is learned, updated, or removed, the waiting period starts. The DHCP snooping device updates the backup file when the waiting period is reached. All changed entries during the period will be saved to the backup file.

The waiting time does not take effect if you do not configure the DHCP snooping entry auto backup by using the **dhcp snooping binding database filename** command.

Examples

# Set the waiting time to 600 seconds for the DHCP snooping device to update the backup file.

```
<Sysname> system-view
[Sysname] dhcp snooping binding database update interval 600
```

Related commands

dhcp snooping binding database filename

dhcp snooping binding database update now

Use **dhcp snooping binding database update now** to manually save DHCP snooping entries to the backup file.

Syntax

dhcp snooping binding database update now

Views

System view

Predefined user roles

network-admin

Usage guidelines

This command does not take effect if you do not configure the DHCP snooping entry auto backup by using the **dhcp snooping binding database filename** command.

Examples

# Manually save DHCP snooping entries to the backup file.

```
<Sysname> system-view
[Sysname] dhcp snooping binding database update now
```

Related commands

dhcp snooping binding database filename

dhcp snooping binding record

Use **dhcp snooping binding record** to enable recording of client information in DHCP snooping entries.

Use **undo dhcp snooping binding record** to disable recording of client information in DHCP snooping entries.

Syntax

dhcp snooping binding record

undo dhcp snooping binding record

Default

DHCP snooping does not record client information.

Views

Layer 2 Ethernet interface/Layer 2 aggregate interface view

S-channel interface

VSI interface

Predefined user roles

network-admin

Usage guidelines

This command enables DHCP snooping on the port directly connecting to the clients to record client information in DHCP snooping entries.

Examples

# Enable recording of client information in DHCP snooping entries.

```
<Sysname> system-view
[Sysname] interface Ten-GigabitEthernet 1/0/1
[Sysname-Ten-GigabitEthernet1/0/1] dhcp snooping binding record
```

dhcp snooping check mac-address

Use **dhcp snooping check mac-address** to enable MAC address check for DHCP snooping.

Use **undo dhcp snooping check mac-address** to disable MAC address check for DHCP snooping.

Syntax

dhcp snooping check mac-address

undo dhcp snooping check mac-address

Default

MAC address check for DHCP snooping is disabled.

Views

Layer 2 Ethernet interface/Layer 2 aggregate interface view

S-channel interface

VSI interface

Predefined user roles

network-admin

Usage guidelines

With MAC address check enabled, DHCP snooping compares the **chaddr** field of a received DHCP request with the source MAC address field in the frame header. If they are the same, DHCP snooping considers this request valid and forwards it to the DHCP server. If they are not the same, DHCP snooping discards the DHCP request.

Examples

# Enable MAC address check for DHCP snooping.

```
<Sysname> system-view
[Sysname] interface Ten-GigabitEthernet 1/0/1
[Sysname-Ten-GigabitEthernet1/0/1] dhcp snooping check mac-address
```

dhcp snooping check request-message

Use **dhcp snooping check request-message** to enable DHCP-REQUEST check for DHCP snooping.

Use **undo dhcp snooping check request-message** to disable DHCP-REQUEST check for DHCP snooping.

Syntax

dhcp snooping check request-message

undo dhcp snooping check request-message

Default

DHCP-REQUEST check is disabled for DHCP snooping.

Views

Layer 2 Ethernet interface/Layer 2 aggregate interface view

S-channel interface

VSI interface

Predefined user roles

network-admin

Usage guidelines

DHCP-REQUEST packets include lease renewal packets, DHCP-DECLINE packets, and DHCP-RELEASE packets. This feature prevents unauthorized clients that forge DHCP-REQUEST packets from attacking the DHCP server.

With this feature enabled, DHCP snooping looks for a matching DHCP snooping entry for each received DHCP-REQUEST message.

- If a match is found, DHCP snooping compares the entry with the message. If they have consistent information, DHCP snooping considers the packet valid and forwards it to the DHCP server. If they have different information, DHCP snooping considers the message invalid and discards it.
- If no match is found, DHCP snooping forwards the message to the DHCP server.

Examples

# Enable DHCP-REQUEST check for DHCP snooping.

```
<Sysname> system-view
[Sysname] interface Ten-GigabitEthernet 1/0/1
[Sysname-Ten-GigabitEthernet1/0/1] dhcp snooping check request-message
```

dhcp snooping deny

Use **dhcp snooping deny** to configure a port as DHCP packet blocking port.

Use **undo dhcp snooping deny** to restore the default.

Syntax

dhcp snooping deny

undo ipv6 dhcp snooping deny

Default

A port does not block DHCP packets.

Views

Layer 2 Ethernet interface view, Layer 2 aggregate interface view

Predefined user roles

network-admin

Usage guidelines

DHCP clients connected to DHCP packet blocking ports cannot obtain IP addresses and other configuration parameters from the DHCP server.

Do not configure a port as both a trusted port and a DHCP packet blocking port.

Examples

# Configure Layer 2 Ethernet interface Ten-GigabitEthernet 1/0/1 as a DHCP packet blocking port.

```
<Sysname> system-view
[Sysname] interface Ten-GigabitEthernet 1/0/1
[Sysname-Ten-GigabitEthernet1/0/1] dhcp snooping deny
```

dhcp snooping enable

Use **dhcp snooping enable** to enable DHCP snooping.

Use **undo dhcp snooping enable** to disable DHCP snooping.

Syntax

dhcp snooping enable

undo dhcp snooping enable

Default

DHCP snooping is disabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

Use the DHCP snooping feature together with trusted port configuration. Before trusted ports are configured, all ports on the DHCP snooping device are untrusted and the device discards all responses sent from DHCP servers.

When DHCP snooping is disabled, the device forwards all responses from DHCP servers.

Examples

# Enable DHCP snooping.

```
<Sysname> system-view
[Sysname] dhcp snooping enable
```

dhcp snooping information circuit-id

Use **dhcp snooping information circuit-id** to configure the padding mode and padding format for the Circuit ID sub-option.

Use **undo dhcp snooping information circuit-id** to restore the default.

Syntax

dhcp snooping information circuit-id { [**vlan** *vlan-id*] **string** *circuit-id* **|** { **normal** **|** **verbose** [**node-identifier** { **mac | sysname | user-defined** *node-identifier* }] } [**format** { **ascii | hex** }] }

undo dhcp snooping information circuit-id [**vlan** *vlan-id*]

Default

The padding mode is normal and the padding format is hex.

Views

Layer 2 Ethernet interface view, Layer 2 aggregate interface view

Predefined user roles

network-admin

Parameters

vlan *vlan-id*: Specifies a VLAN ID for the Circuit ID sub-option.

string *circuit-id*: Specifies the string mode, in which the padding content for the Circuit ID sub-option is a case-sensitive string of 3 to 63 characters.

normal: Specifies the normal mode. The padding content includes the VLAN ID and interface number.

verbose: Specifies the verbose mode.

node-identifier { **mac** | **sysname** | **user-defined** *node-identifier* }: Specifies the access node identifier. The padding content includes the node identifier, Ethernet type (fixed to **eth**), interface number, and VLAN ID. The node identifier varies by keyword **mac**, **sysname**, and **user-defined**.

- **mac**: Uses the MAC address of the access node as the node identifier. It is the default node identifier.
- **sysname**: Uses the device name as the node identifier. You can set the device name by using the **sysname** command in system view. The padding format for the device name is always ASCII regardless of the specified padding format.

NOTE:

If **sysname** is used as the node identifier, do not include any space when you set the device name. Otherwise, the DHCP snooping device fails to add or replace the Option 82.

- **user-defined** *node-identifier*: Uses a case-sensitive string of 1 to 50 characters as the node identifier. The padding format for the specified character string is always ASCII regardless of the specified padding format.

format: Specifies the padding format for the Circuit ID sub-option.

ascii: Specifies the padding format as ASCII.

hex: Specifies the padding format as hex.

Usage guidelines

If you use this command multiple times, the most recent configuration takes effect.

The padding format for the user-defined string, the normal mode, or the verbose modes varies by command configuration. Table 13 shows how the padding format is determined for different modes.

Table 13 Padding format for different modes

Keyword (mode)	If no padding format is specified	If the padding format is ascii	If the padding format is hex
string *circuit-id*	You cannot specify a padding format, and the padding format is always ASCII.	N/A	N/A
normal	Hex.	ASCII.	Hex.
verbose	Hex for the VLAN ID. ASCII for the node identifier, Ethernet type, and interface number.	ASCII.	ASCII for the node identifier and Ethernet type. Hex for the interface number and VLAN ID.

If **replace** is configured as the handling strategy for DHCP requests that contain Option 82, you must specify the padding mode and padding format for the Circuit ID sub-option. If the handling strategy is **keep** or **drop**, you do not need to specify the padding mode and padding format for the Circuit ID sub-option.

Examples

# Configure verbose as the padding mode, device name as the node identifier, and ASCII as the padding format for the Circuit ID sub-option.

```
<Sysname> system-view
[Sysname] interface Ten-GigabitEthernet 1/0/1
```

```
[Sysname-Ten-GigabitEthernet1/0/1] dhcp snooping information enable
[Sysname-Ten-GigabitEthernet1/0/1] dhcp snooping information strategy replace
[Sysname-Ten-GigabitEthernet1/0/1] dhcp snooping information circuit-id verbose
node-identifier sysname format ascii
```

Related commands

- **dhcp snooping information enable**
- **dhcp snooping information strategy**
- **display dhcp snooping information**

dhcp snooping information enable

Use **dhcp snooping information enable** to enable DHCP snooping to support Option 82.

Use **undo dhcp snooping information enable** to disable this feature.

Syntax

dhcp snooping information enable

undo dhcp snooping information enable

Default

DHCP snooping does not support Option 82.

Views

Layer 2 Ethernet interface view, Layer 2 aggregate interface view

Predefined user roles

network-admin

Usage guidelines

This command enables DHCP snooping to add Option 82 into DHCP request packets that do not contain Option 82 before forwarding the requests to the DHCP server. The content of Option 82 is determined by the **dhcp snooping information circuit-id** and **dhcp snooping information remote-id** commands. If the received DHCP request packets contain Option 82, DHCP snooping handles the packets according to the strategy configured with the **dhcp snooping information strategy** command.

If this feature is disabled, DHCP snooping forwards requests that contain or do not contain Option 82 to the DHCP server.

Examples

# Enable DHCP snooping to support Option 82.

```
<Sysname> system-view
[Sysname] interface Ten-GigabitEthernet1/0/1
[Sysname-Ten-GigabitEthernet1/0/1] dhcp snooping information enable
```

Related commands

- **dhcp snooping information circuit-id**
- **dhcp snooping information remote-id**
- **dhcp snooping information strategy**

dhcp snooping information remote-id

Use **dhcp snooping information remote-id** to configure the padding mode and padding format for the Remote ID sub-option.

Use **undo dhcp snooping information remote-id** to restore the default.

Syntax

dhcp snooping information remote-id { **normal** [**format** { **ascii** | **hex** }] | [**vlan** *vlan-id*] { **string** *remote-id* | **sysname** } }

undo dhcp snooping information remote-id [**vlan** *vlan-id*]

Default

The padding mode is normal and the padding format is hex.

Views

Layer 2 Ethernet interface view, Layer 2 aggregate interface view

Predefined user roles

network-admin

Parameters

vlan *vlan-id*: Specifies the VLAN ID as the Remote ID sub-option.

string *remote-id*: Specifies the string mode that uses a case-sensitive string of 1 to 63 characters as the content of the Remote ID sub-option.

sysname: Specifies the sysname mode that uses the device name as the Remote ID sub-option. You can configure the device name by using the **sysname** command in system view.

normal: Specifies the normal mode. The padding content is the MAC address of the receiving interface.

format: Specifies the padding format for the Remote ID sub-option. The default padding format is hex.

ascii: Specifies the padding format as ASCII.

hex: Specifies the padding format as hex.

Usage guidelines

DHCP snooping uses ASCII to pad the specified string or device name for the Remote ID sub-option. The padding format for the normal padding mode is determined by the command configuration.

If you use this command multiple times, the most recent configuration takes effect.

Examples

# Pad the Remote ID sub-option with the character string **device001**.

```
<Sysname> system-view
[Sysname] interface Ten-GigabitEthernet 1/0/1
[Sysname-Ten-GigabitEthernet1/0/1] dhcp snooping information enable
[Sysname-Ten-GigabitEthernet1/0/1] dhcp snooping information strategy replace
[Sysname-Ten-GigabitEthernet1/0/1] dhcp snooping information remote-id string device001
```

Related commands

- **dhcp snooping information enable**
- **dhcp snooping information strategy**
- **display dhcp snooping information**

dhcp snooping information strategy

Use **dhcp snooping information strategy** to configure the handling strategy for Option 82 in request messages.

Use **undo dhcp snooping information strategy** to restore the default.

Syntax

dhcp snooping information strategy { **drop** | **keep** | **replace** }

undo dhcp snooping information strategy

Default

The handling strategy for Option 82 in request messages is **replace**.

Views

Layer 2 Ethernet interface view, Layer 2 aggregate interface view

Predefined user roles

network-admin

Parameters

drop: Drops DHCP messages that contain Option 82.

keep: Keeps the original Option 82 intact.

replace: Replaces the original Option 82 with the configured Option 82.

Usage guidelines

This command takes effect only on DHCP requests that contain Option 82.

When enabled to support Option 82, the DHCP relay agent always adds Option 82 into DHCP requests that do not contain Option 82 before forwarding the requests to the DHCP.

Examples

# Specify the handling strategy for Option 82 in request messages as **keep**.

```
<Sysname> system-view
[Sysname] interface Ten-GigabitEthernet1/0/1
[Sysname-Ten-GigabitEthernet1/0/1] dhcp snooping information enable
[Sysname-Ten-GigabitEthernet1/0/1] dhcp snooping information strategy keep
```

Related commands

- **dhcp snooping information circuit-id**
- **dhcp snooping information remote-id**

dhcp snooping log enable

Use **dhcp snooping log enable** to enable DHCP snooping logging.

Use **undo dhcp snooping log enable** to restore the default.

Syntax

dhcp snooping log enable

undo dhcp snooping log enable

Default

DHCP snooping logging is disabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

This command enables the DHCP snooping device to generate DHCP snooping logs and send them to the information center. For information about the log destination and output rule configuration in the information center, see *Network Management and Monitoring Configuration Guide*.

As a best practice, disable this feature if the log generation affects the device performance.

Examples

# Enable DHCP snooping logging.

```
<Sysname> system-view
[Sysname] dhcp snooping log enable
```

dhcp snooping max-learning-num

Use **dhcp snooping max-learning-num** to set the maximum number of DHCP snooping entries for an interface to learn.

Use **undo dhcp snooping max-learning-num** to restore the default.

Syntax

dhcp snooping max-learning-num *number*

undo dhcp snooping max-learning-num

Default

The maximum number of DHCP snooping entries for an interface to learn is not limited.

Views

Layer 2 Ethernet interface/Layer 2 aggregate interface view

S-channel interface

VSI interface

Predefined user roles

network-admin

Parameters

number: Specifies the maximum number of DHCP snooping entries for an interface to learn. The value range is 1 to 4294967295.

Examples

# Set the maximum number of DHCP snooping entries for the Layer 2 Ethernet interface Ten-GigabitEthernet 1/0/1 to learn to 1000.

```
<Sysname> system-view
[Sysname] interface Ten-GigabitEthernet 1/0/1
[Sysname-Ten-GigabitEthernet1/0/1] dhcp snooping max-learning-num 1000
```

dhcp snooping rate-limit

Use **dhcp snooping rate-limit** to configure the maximum rate at which an interface can receive DHCP packets.

Use **undo dhcp snooping rate-limit** to remove the configured rate limit.

Syntax

dhcp snooping rate-limit *rate*

undo dhcp snooping rate-limit

Default

Incoming DHCP packets on an interface are not rate limited.

Views

Layer 2 Ethernet interface/Layer 2 aggregate interface view

S-channel interface

VSI interface

Predefined user roles

network-admin

Parameters

rate: Specifies the maximum rate for an interface to receive DHCP packets, in Kbps. The value must be an integer multiple of 8 in the range of 64 to 512.

Usage guidelines

This command takes effect only when DHCP snooping is enabled.

With the rate limit feature, the interface discards DHCP packets that exceed the maximum rate.

If you configure this command on a Layer 2 Ethernet interface that is a member port of a Layer 2 aggregate interface, the Layer 2 Ethernet interface uses the DHCP packet maximum rate configured on the Layer 2 aggregate interface. If the Layer 2 Ethernet interface leaves the aggregation group, it uses its own DHCP packet maximum rate.

Examples

# Set the maximum rate at which the Layer 2 Ethernet interface Ten-GigabitEthernet 1/0/1 can receive DHCP packet to 64 Kbps.

```
<Sysname> system-view
[Sysname] interface Ten-GigabitEthernet 1/0/1
[Sysname-Ten-GigabitEthernet1/0/1] dhcp snooping rate-limit 64
```

dhcp snooping trust

Use **dhcp snooping trust** to configure a port as a trusted port.

Use **undo dhcp snooping trust** to restore the default state of a port.

Syntax

dhcp snooping trust

undo dhcp snooping trust

Default

After you enable DHCP snooping, all ports are untrusted.

Views

Layer 2 Ethernet interface view, Layer 2 aggregate interface view

Predefined user roles

network-admin

Usage guidelines

Specify the ports facing the DHCP server as trusted ports and specify the other ports as untrusted ports so DHCP clients can obtain valid IP addresses.

Examples

# Specify the Layer 2 Ethernet interface Ten-GigabitEthernet 1/0/1 as a trusted port.

```
<Sysname> system-view
[Sysname] interface Ten-GigabitEthernet 1/0/1
[Sysname-Ten-GigabitEthernet1/0/1] dhcp snooping trust
```

Related commands

display dhcp snooping trust

display dhcp snooping binding

Use **display dhcp snooping binding** to display DHCP snooping entries.

Syntax

display dhcp snooping binding [**ip** *ip-address* [**vlan** *vlan-id*]]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

ip *ip-address*: Displays the DHCP snooping entry for the specified IP address.

vlan *vlan-id*: Specifies the VLAN ID where the IP address resides.

Usage guidelines

If you do not specify any parameters, this command displays all DHCP snooping entries.

Examples

# Display all DHCP snooping entries.

```
<Sysname> display dhcp snooping binding
 2 DHCP snooping entries found
 IP address      MAC address    Lease        VLAN  SVLAN Interface
 =============== ============== ============ ===== ===== =================
 1.1.1.7         0000-0101-0107 16907533     2     3     XGE1/0/1
 1.1.1.11        0000-0101-010b 16907537     2     3     XGE1/0/3
```

Table 14 Command output

Field	Description
DHCP snooping entries found	Number of DHCP snooping entries.

Field	Description
IP address	IP address assigned to the DHCP client.
MAC address	MAC address of the DHCP client.
Lease	Remaining lease duration in seconds.
VLAN	When both DHCP snooping and QinQ are enabled or the DHCP packet contains two VLAN tags, this field identifies the outer VLAN tag. Otherwise, it identifies the VLAN where the port connecting the DHCP client resides.
SVLAN	When both DHCP snooping and QinQ are enabled or the DHCP packet contains two VLAN tags, this field identifies the inner VLAN tag. Otherwise, it displays **N/A**.
Interface	Port connected to the DHCP client.

Related commands

- **dhcp snooping enable**
- **reset dhcp snooping binding**

display dhcp snooping binding database

Use **display dhcp snooping binding database** to display information about DHCP snooping entry auto backup.

Syntax

display dhcp snooping binding database

Views

Any view

Predefined user roles

network-admin

network-operator

Examples

# Display information about DHCP snooping entry auto backup.

```
<Sysname> display dhcp snooping binding database
File name                :   database.dhcp
Username                 :
Password                 :
Update interval          :   600 seconds
Latest write time        :   Feb 27 18:48:04 2012
Status                   :   Last write succeeded.
```

Table 15 Command output

Field	Description
File name	Name of the DHCP snooping entry backup file.
Username	Username for accessing the URL of the remote backup file.
Password	Password for accessing the URL of the remote backup file. This field displays ****** if a password is configured.

Field	Description
Update interval	Waiting time in seconds after a DHCP snooping entry change for the DHCP snooping device to update the backup file.
Latest write time	Time of the latest update.
Status	Status of the update: • **Writing**—The backup file is being updated. • **Last write succeeded**—The backup file was successfully updated. • **Last write failed**—The backup file failed to be updated.

display dhcp snooping information

Use **display dhcp snooping information** to display Option 82 configuration on the DHCP snooping device.

Syntax

display dhcp snooping information { **all** | **interface** *interface-type interface-number* }

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

all: Displays Option 82 configuration on all Layer 2 Ethernet interfaces.

interface *interface-type interface-number*: Specifies an interface by its type and number.

Examples

# Display Option 82 configuration on all interfaces.

```
<Sysname> display dhcp snooping information all
Interface: Bridge-Aggregation1
   Status: Disable
   Strategy: Drop
   Circuit ID:
     Padding format: User Defined
       User defined: abcd
     Format: ASCII
   Remote ID:
     Padding format: Normal
     Format: ASCII
   VLAN 10:
     Circuit ID: abcd
     Remote ID: company
```

Table 16 Command output

Field	Description
Interface	Interface name.

Field	Description
Status	Option 82 status, **Enable** or **Disable**.
Strategy	Handling strategy for DHCP requests that contain Option 82, **Drop**, **Keep**, or **Replace**.
Circuit ID	Content of the Circuit ID sub-option.
Padding format	Padding format of Option 82: • For Circuit ID sub-option, the padding format can be **Normal**, **User Defined**, **Verbose (sysname)**, **Verbose (MAC)**, or **Verbose (user defined)**. • For Remote ID sub-option, the padding format can be **Normal**, **Sysname**, or **User Defined**.
Node identifier	Access node identifier.
User defined	Content of the user-defined sub-option.
Format	Code type of Option 82 sub-option: • For Circuit ID sub-option, the code type can be **ASCII**, **Default**, or **Hex**. • For Remote ID sub-option, the code type can be **ASCII** or **Hex**.
Remote ID	Content of the Remote ID sub-option.
VLAN	Pads Circuit ID sub-option and Remote ID sub-option in the DHCP packets received in the specified VLAN.

display dhcp snooping packet statistics

Use **display dhcp snooping packet statistics** to display DHCP packet statistics for DHCP snooping.

Syntax

display dhcp snooping packet statistics [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

slot *slot-number*: Specifies an IRF member device by its member ID.

Usage guidelines

If you do not specify the **slot** *slot-number* option, this command displays DHCP packet statistics for the device where the command is executed.

Examples

# Display DHCP packet statistics for DHCP snooping.

```
<Sysname> display dhcp snooping packet statistics
 DHCP packets received                  : 100
 DHCP packets sent                      : 200
 Invalid DHCP packets dropped           : 0
```

Related commands

reset dhcp snooping packet statistics

display dhcp snooping trust

Use **display dhcp snooping trust** to display information about trusted ports.

Syntax

display dhcp snooping trust

Views

Any view

Predefined user roles

network-admin

network-operator

Examples

# Display information about trusted ports.

```
<Sysname> display dhcp snooping trust
 DHCP snooping is enabled.
 Interface                                              Trusted
 =========================                              ============
 Ten-GigabitEthernet1/0/1                               Trusted
```

Related commands

dhcp snooping trust

reset dhcp snooping binding

Use **reset dhcp snooping binding** to clear DHCP snooping entries.

Syntax

reset dhcp snooping binding { **all** | **ip** *ip-address* [**vlan** *vlan-id*] }

Views

User view

Predefined user roles

network-admin

Parameters

all: Clears all DHCP snooping entries.

ip *ip-address*: Clears the DHCP snooping entry for the specified IP address.

vlan *vlan-id*: Clears DHCP snooping entries for the specified VLAN.

Examples

# Clear all DHCP snooping entries.

```
<Sysname> reset dhcp snooping binding all
```

Related commands

display dhcp snooping binding

reset dhcp snooping packet statistics

Use **reset dhcp snooping packet statistics** to clear DHCP packet statistics for DHCP snooping.

Syntax

reset dhcp snooping packet statistics [**slot** *slot-number*]

Views

User view

Predefined user roles

network-admin

Parameters

slot *slot-number*: Specifies an IRF member device by its member ID.

Usage guidelines

If you do not specify the **slot** *slot-number* option, this command clears DHCP packet statistics for the device where the command is executed.

Examples

# Clear DHCP packet statistics for DHCP snooping.

```
<Sysname> reset dhcp snooping packet statistics
```

Related commands

display dhcp snooping packet statistics

BOOTP client commands

display bootp client

Use **display bootp client** to display information about a BOOTP client.

Syntax

display bootp client [**interface** *interface-type interface-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

interface *interface-type interface-number*: Specifies an interface by its type and number.

Usage guidelines

If you do not specify an interface, this command displays BOOTP client information about all interfaces.

Examples

# Display BOOTP client information about VLAN-interface 10.

```
<Sysname> display bootp client interface vlan-interface 10
Vlan-interface10 BOOTP client information:
```

```
Allocated IP: 169.254.0.2 255.255.0.0
Transaction ID: 0x3d8a7431
MAC Address: 00e0-fc0a-c3ef
```

Table 17 Command output

Field	Description
Vlan-interface10 BOOTP client information	Information about the interface that acts as a BOOTP client.
Allocated IP	BOOTP client's IP address allocated by the BOOTP server.
Transaction ID	Value of the **XID** field in a BOOTP message, which is a random number chosen when the BOOTP client sends a BOOTP request to the BOOTP server. It is used to match a response message from the BOOTP server. If the values of the **XID** field are different in the BOOTP response and request, the BOOTP client drops the BOOTP response.
Mac Address	MAC address of a BOOTP client.

Related commands

ip address bootp-alloc

ip address bootp-alloc

Use **ip address bootp-alloc** to configure an interface to use BOOTP for IP address acquisition.

Use **undo ip address bootp-alloc** to cancel an interface from using BOOTP.

Syntax

ip address bootp-alloc

undo ip address bootp-alloc

Default

An interface does not use BOOTP for IP address acquisition.

Views

Interface view

Predefined user roles

network-admin

Examples

# Configure VLAN-interface 10 to use BOOTP for IP address acquisition.

```
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] ip address bootp-alloc
```

Related commands

display bootp client