Content

CHAPTER 1 COMMANDS FOR DHCP 1-1

1.1 COMMANDS FOR DHCP SERVER CONFIGURATION 1-1

1.1.1 bootfile 1-1
1.1.2 clear ip dhcp binding 1-1
1.1.3 clear ip dhcp conflict 1-2
1.1.4 clear ip dhcp server statistics 1-2
1.1.5 client-identifier 1-2
1.1.6 debug ip dhcp client 1-3
1.1.7 debug ip dhcp relay 1-3
1.1.8 debug ip dhcp server 1-3
1.1.9 default-router 1-4
1.1.10 dns-server 1-4
1.1.11 domain-name 1-4
1.1.12 hardware-address 1-5
1.1.13 host 1-5
1.1.14 ip dhcp conflict logging 1-6
1.1.15 ip dhcp disable 1-6
1.1.16 ip dhcp excluded-address 1-6
1.1.17 ip dhcp pool 1-7
1.1.18 ip dhcp conflict ping-detection enable 1-7
1.1.19 ip dhcp ping packets 1-8
1.1.20 ip dhcp ping timeout 1-8
1.1.21 lease 1-9
1.1.22 max-lease-time 1-9
1.1.23 netbios-name-server 1-10
1.1.24 netbios-node-type 1-10
1.1.25 network-address 1-10
1.1.26 next-server 1-11
1.1.27 option 1-11
1.1.28 service dhcp 1-12
1.1.29 show ip dhcp binding 1-12
1.1.30 show ip dhcp conflict 1-13
1.1.31 show ip dhcp relay information option 1-13

1.1.32 show ip dhcp server statistics....1-13

1.2 COMMANDS FOR DHCP RELAY CONFIGURATION....1-15

1.2.1 ip dhcp broadcast suppress....1-15
1.2.2 ip dhcp relay share-vlan <vlanid> sub-vlan <vlanlist>....1-15
1.2.3 ip forward-protocol udp bootps....1-16
1.2.4 ip helper-address....1-16
1.2.5 show ip forward-protocol....1-16
1.2.6 show ip helper-address....1-17

CHAPTER 2 COMMANDS FOR DHCPV6....2-1

2.1 CLEAR IPV6 DHCP BINDING....2-1
2.2 CLEAR IPV6 DHCP CONFLICT....2-1
2.3 CLEAR IPV6 DHCP STATISTICS....2-2
2.4 DEBUG IPV6 DHCP CLIENT PACKET....2-2
2.5 DEBUG IPV6 DHCP DETAIL....2-2
2.6 DEBUG IPV6 DHCP RELAY PACKET....2-3
2.7 DEBUG IPV6 DHCP SERVER....2-3
2.8 DNS-SERVER....2-3
2.9 DOMAIN-NAME....2-4
2.10 EXCLUDED-ADDRESS....2-4
2.11 IPV6 ADDRESS....2-5
2.12 IPV6 DHCP CLIENT PD....2-5
2.13 IPV6 DHCP CLIENT PD HINT....2-6
2.14 IPV6 DHCP POOL....2-6
2.15 IPV6 DHCP RELAY DESTINATION....2-7
2.16 IPV6 DHCP SERVER....2-8
2.17 IPV6 GENERAL-PREFIX....2-8
2.18 IPV6 LOCAL POOL....2-9
2.19 LIFETIME....2-9
2.20 NETWORK-ADDRESS....2-10
2.21 PREFIX-DELEGATION....2-11

2.22 PREFIX-DELEGATION POOL 2-11
2.23 SERVICE DHCPV6 2-12
2.24 SHOW IPV6 DHCP 2-13
2.25 SHOW IPV6 DHCP BINDING 2-13
2.26 SHOW IPV6 DHCP CONFLICT 2-13
2.27 SHOW IPV6 DHCP INTERFACE 2-14
2.28 SHOW IPV6 DHCP POOL 2-14
2.29 SHOW IPV6 DHCP STATISTICS 2-15
2.30 SHOW IPV6 GENERAL-PREFIX 2-17
2.31 SHOW IPV6 LOCAL POOL 2-17

CHAPTER 3 COMMANDS FOR DHCP OPTION 60 AND OPTION 43 3-1

3.1 OPTION 43 ASCII LINE 3-1
3.2 OPTION 43 HEX WORD 3-1
3.3 OPTION 43 IP A.B.C.D 3-2
3.4 OPTION 60 ASCII LINE 3-2
3.5 OPTION 60 HEX WORD 3-2
3.6 OPTION 60 IP A.B.C.D 3-3

CHAPTER 4 COMMANDS FOR DHCP OPTION 82 4-1

4.1 DEBUG IP DHCP RELAY PACKET 4-1
4.2 IP DHCP RELAY INFORMATION OPTION 4-1
4.3 IP DHCP RELAY INFORMATION OPTION DELIMITER 4-2
4.4 IP DHCP RELAY INFORMATION OPTION REMOTE-ID 4-2
4.5 IP DHCP RELAY INFORMATION OPTION REMOTE-ID FORMAT 4-2
4.6 IP DHCP RELAY INFORMATION OPTION SELF-DEFINED REMOTE-ID 4-3
4.7 IP DHCP RELAY INFORMATION OPTION SELF-DEFINED REMOTE-ID FORMAT 4-4
4.8 IP DHCP RELAY INFORMATION OPTION SELF-DEFINED SUBSCRIBER-ID 4-4

4.9 IP DHCP RELAY INFORMATION OPTION SELF-DEFINED SUBSCRIBER-ID FORMAT 4-5
4.10 IP DHCP RELAY INFORMATION OPTION SUBSCRIBER-ID 4-5
4.11 IP DHCP RELAY INFORMATION OPTION SUBSCRIBER-ID FORMAT 4-6
4.12 IP DHCP RELAY INFORMATION POLICY 4-7
4.13 IP DHCP SERVER RELAY INFORMATION ENABLE 4-7
4.14 SHOW IP DHCP RELAY INFORMATION OPTION 4-8

CHAPTER 5 COMMANDS FOR DHCP SNOOPING 5-1

5.1 DEBUG IP DHCP SNOOPING BINDING 5-1
5.2 DEBUG IP DHCP SNOOPING EVENT 5-1
5.3 DEBUG IP DHCP SNOOPING PACKET 5-1
5.4 DEBUG IP DHCP SNOOPING PACKET INTERFACE 5-2
5.5 DEBUG IP DHCP SNOOPING UPDATE 5-2
5.6 ENABLE TRUSTVIEW KEY 5-2
5.7 IP DHCP SNOOPING 5-3
5.8 IP DHCP SNOOPING ACTION 5-3
5.9 IP DHCP SNOOPING ACTION MAXNUM 5-4
5.10 IP DHCP SNOOPING BINDING 5-4
5.11 IP DHCP SNOOPING BINDING ARP 5-5
5.12 IP DHCP SNOOPING BINDING DOT1X 5-5
5.13 IP DHCP SNOOPING BINDING USER 5-6
5.14 IP DHCP SNOOPING BINDING USER-CONTROL 5-6
5.15 IP DHCP SNOOPING BINDING USER-CONTROL MAX-USER 5-7
5.16 IP DHCP SNOOPING INFORMATION ENABLE 5-8
5.17 IP DHCP SNOOPING INFORMATION OPTION ALLOW-UNTRUSTED (REPLACE|) 5-8
5.18 IP DHCP SNOOPING INFORMATION OPTION DELIMITER 5-9
5.19 IP DHCP SNOOPING INFORMATION OPTION REMOTE-ID 5-9
5.20 IP DHCP SNOOPING INFORMATION OPTION SELF-DEFINED REMOTE-ID 5-10

5.21 IP DHCP SNOOPING INFORMATION OPTION SELF-DEFINED REMOTE-ID FORMAT 5-10

5.22 IP DHCP SNOOPING INFORMATION OPTION SELF-DEFINED SUBSCRIBER-ID 5-11

5.23 IP DHCP SNOOPING INFORMATION OPTION SELF-DEFINED SUBSCRIBER-ID FORMAT 5-11

5.24 IP DHCP SNOOPING INFORMATION OPTION SUBSCRIBER-ID 5-12

5.25 IP DHCP SNOOPING INFORMATION OPTION SUBSCRIBER-ID FORMAT 5-12

5.26 IP DHCP SNOOPING TRUST 5-13

5.27 IP USER HELPER-ADDRESS 5-14

5.28 IP USER PRIVATE PACKET VERSION TWO 5-15

5.29 SHOW IP DHCP SNOOPING 5-15

5.30 SHOW IP DHCP SNOOPING BINDING ALL 5-18

5.31 SHOW TRUSTVIEW STATUS 5-19

CHAPTER 6 COMMANDS FOR DHCPV6 SNOOPING 6-1

6.1 CLEAR IPV6 DHCP SNOOPING BINDING 6-1

6.2 DEBUG IPV6 DHCP SNOOPING BINDING 6-1

6.3 DEBUG IPV6 DHCP SNOOPING EVENT 6-2

6.4 DEBUG IPV6 DHCP SNOOPING PACKET 6-2

6.5 IPV6 DHCP SNOOPING ACTION 6-4

6.6 IPV6 DHCP SNOOPING ACTION MAXNUM 6-4

6.7 IPV6 DHCP SNOOPING BINDING ENABLE 6-5

6.8 IPV6 DHCP SNOOPING BINDING ND 6-5

6.9 IPV6 DHCP SNOOPING BINDING USER 6-6

6.10 IPV6 DHCP SNOOPING BINDING USER-CONTROL 6-7

6.11 IPV6 DHCP SNOOPING BINDING-LIMIT 6-7

6.12 IP DHCP SNOOPING TRUST 6-8

6.13 SHOW IPV6 DHCP SNOOPING BINDING 6-8

6.14 SHOW IPV6 DHCP SNOOPING INTERFACE 6-9

CHAPTER 7 COMMANDS FOR DHCPV6 OPTION 52 7-1

7.1 OPTION 52 ASCII LINE 7-1

7.2 OPTION 52 HEX WORD 7-1

7.3 OPTION 52 IPV6 X:X::X:X 7-2

Chapter 1 Commands for DHCP

1.1 Commands for DHCP Server Configuration

1.1.1 bootfile

Command: bootfile *<filename>*

no bootfile

Function: Sets the file name for DHCP client to import on boot up; the "**no bootfile** "command deletes this setting.

Parameters: *<filename>* is the name of the file to be imported, up to 255 characters are allowed.

Command Mode: DHCP Address Pool Mode

Usage Guide: Specify the name of the file to be imported for the client. This is usually used for diskless workstations that need to download a configuration file from the server on boot up. This command is together with the "next sever".

Example: The path and filename for the file to be imported is "c:\temp\nos.img"

Switch(dhcp-1-config)#bootfile c:\temp\nos.img

Related Command: next-server

1.1.2 clear ip dhcp binding

Command: clear ip dhcp binding {<*address*> | all}

Function: Deletes the specified IP address-hardware address binding record or all IP address-hardware address binding records.

Parameters: *<address>* is the IP address that has a binding record in decimal format. **all** refers to all IP addresses that have a binding record.

Command mode: Admin Mode.

Usage Guide: "**show ip dhcp binding**" command can be used to view binding information for IP addresses and corresponding DHCP client hardware addresses. If the DHCP server is informed that a DHCP client is not using the assigned IP address for some reason before the lease period expires, the DHCP server would not remove the binding information automatically. The system administrator can use this command to delete that IP address-client hardware address binding manually, if "all" is specified, then all auto binding records will be deleted, thus all addresses in the DHCP address pool will

be reallocated.

Example: Removing all IP-hardware address binding records.

Switch#clear ip dhcp binding all

Related Command: show ip dhcp binding

1.1.3 clear ip dhcp conflict

Command: clear ip dhcp conflict {<*address*> | all }

Function: Deletes an address present in the address conflict log.

Parameters: <*address*> is the IP address that has a conflict record; **all** stands for all addresses that have conflict records.

Command mode: Admin Mode.

Usage Guide: "**show ip dhcp conflict**" command can be used to check which IP addresses are conflicting for use. The **"clear ip dhcp conflict"** command can be used to delete the conflict record for an address. If "all" is specified, then all conflict records in the log will be removed. When records are removed from the log, the addresses are available for allocation by the DHCP server.

Example: The network administrator finds 10.1.128.160 that has a conflict record in the log and is no longer used by anyone, so he deletes the record from the address conflict log.

Switch#clear ip dhcp conflict 10.1.128.160

Related Command: ip dhcp conflict logging, show ip dhcp conflict

1.1.4 clear ip dhcp server statistics

Command: clear ip dhcp server statistics

Function: Deletes the statistics for DHCP server, clears the DHCP server count.

Parameters: None

Command mode: Admin Mode.

Usage Guide: DHCP count statistics can be viewed with "**show ip dhcp server statistics**" command, all information is accumulated. You can use the "**clear ip dhcp server statistics**" command to clear the count for easier statistics checking.

Example: Clearing the count for DHCP server.

Switch#clear ip dhcp server statistics

Related Command: show ip dhcp server statistics

1.1.5 client-identifier

Command: client-identifier <*unique-identifier*>

no client-identifier

Function: Specifies the unique ID of the user when binding an address manually; the "**no client-identifier**" command deletes the identifier.

Parameters: <*unique-identifier*> is the user identifier, in dotted Hex format.

Command Mode: DHCP Address Pool Mode

Usage Guide: This command is used with "host" when binding an address manually. If the requesting client identifier matches the specified identifier, DHCP server assigns the IP address defined in "host" command to the client.

Example: Specifying the IP address 10.1.128.160 to be bound to user with the unique id of 00-10-5a-60-af-12 in manual address binding.

Switch(dhcp-1-config)#client-identifier 00-10-5a-60-af-12

Switch(dhcp-1-config)#host 10.1.128.160 24

Related Command: host

1.1.6 debug ip dhcp client

Command: debug ip dhcp client {event | packet}

no debug ip dhcp server {event | packet}

Function: Enable the debugging of DHCP client, **no** command disables the debugging of DHCP client.

Command mode: Admin Mode

Default: Disable the debugging.

1.1.7 debug ip dhcp relay

Command: debug ip dhcp server packet

no debug ip dhcp server packet

Function: Enable the debugging of DHCP relay, **no** command disables the debugging of DHCP relay.

Command mode: Admin Mode

Default: Disable the debugging.

1.1.8 debug ip dhcp server

Command: debug ip dhcp server { events | linkage | packets }

no debug ip dhcp server { events | linkage | packets }

Function: Enables DHCP server debug information: the "**no debug ip dhcp server {events | linkage | packets}**" command disables the debug information for DHCP server**.**

Default: Debug information is disabled by default.

Command mode: Admin Mode.

1.1.9 default-router

Command: default-router <*address1*>[<*address2*>[…<*address8*>]]

no default-router

Function: Configures default gateway(s) for DHCP clients; the "**no default-router**" command deletes the default gateway.

Parameters: <*address1*>…<*address8*> are IP addresses, in decimal format.

Default: No default gateway is configured for DHCP clients by default.

Command Mode: DHCP Address Pool Mode

Usage Guide: The IP address of default gateway(s) should be in the same subnet as the DHCP client IP, the switch supports up to 8 gateway addresses. The gateway address assigned first has the highest priority, and therefore address1 has the highest priority, and address2 has the second, and so on.

Example: Configuring the default gateway for DHCP clients to be 10.1.128.2 and 10.1.128.100.

Switch(dhcp-1-config)#default-router 10.1.128.2 10.1.128.100

1.1.10 dns-server

Command: dns-server <*address1*>[<*address2*>[…<*address8*>]]

no dns-server

Function: Configure DNS servers for DHCP clients; the "**no dns-server**" command deletes the default gateway.

Parameters: <*address1*>…<*address8*> are IP addresses, in decimal format.

Default: No DNS server is configured for DHCP clients by default.

Command Mode: DHCP Address Pool Mode

Usage Guide: Up to 8 DNS server addresses can be configured. The DNS server address assigned first has the highest priority, therefore address 1 has the highest priority, and address 2 has the second, and so on.

Example: Set 10.1.128.3 as the DNS server address for DHCP clients.

Switch(dhcp-1-config)#dns-server 10.1.128.3

1.1.11 domain-name

Command: domain-name <*domain*>

no domain-name

Function: Configures the Domain name for DHCP clients; the "**no domain-name**"

command deletes the domain name.

Parameters: <*domain*> is the domain name, up to 255 characters are allowed.

Command Mode: DHCP Address Pool Mode

Default: None

Usage Guide: Specifies a domain name for the client.

Example: Specifying “digitalchina.com.cn" as the DHCP clients’ domain name.

Switch(dhcp-1-config)#domain-name digitalchina.com.cn

1.1.12 hardware-address

Command: hardware-address <*hardware-address*> [{Ethernet | IEEE802|<*type-number*>}]

no hardware-address

Function: Specifies the hardware address of the user when binding address manually; the “**no hardware-address**” command deletes the setting.

Parameters: <*hardware-address*> is the hardware address in Hex; **Ethernet | IEEE802** is the Ethernet protocol type, **<*type-number*>** should be the RFC number defined for protocol types, from 1 to 255, e.g., 0 for Ethernet and 6 for IEEE 802.

Default: The default protocol type is Ethernet,

Command Mode: DHCP Address Pool Mode

Usage Guide: This command is used with the “host” when binding address manually. If the requesting client hardware address matches the specified hardware address, the DHCP server assigns the IP address defined in “host” command to the client.

Example: Specify IP address 10.1.128.160 to be bound to the user with hardware address 00-00-e2-3a-26-04 in manual address binding.

Switch(dhcp-1-config)#hardware-address 00-00-e2-3a-26-04

Switch(dhcp-1-config)#host 10.1.128.160 24

Related Command: host

1.1.13 host

Command: host <*address*> [<*mask*> | <*prefix-length*>]

no host

Function: Specifies the IP address to be assigned to the user when binding addresses manually; the “**no host**” command deletes the IP address.

Parameters: <*address*> is the IP address in decimal format; **<*mask*>** is the subnet mask in decimal format; **<*prefix-length*>** means mask is indicated by prefix. For example, mask 255.255.255.0 in prefix is “24”, and mask 255.255.255.252 in prefix is “30”.

Command Mode: DHCP Address Pool Mode

Default: None

Usage Guide: If no mask or prefix is configured when configuring the IP address, and no information in the IP address pool indicates anything about the mask, the system will assign a mask automatically according to the IP address class.

This command is used with “hardware address” command or “client identifier” command when binding addresses manually. If the identifier or hardware address of the requesting client matches the specified identifier or hardware address, the DHCP server assigns the IP address defined in “host” command to the client.

Example: Specifying IP address 10.1.128.160 to be bound to user with hardware address 00-10-5a-60-af-12 in manual address binding.

Switch(dhcp-1-config)#hardware-address 00-10-5a-60-af-12

Switch(dhcp-1-config)#host 10.1.128.160 24

Related command: hardware-address, client-identifier

1.1.14 ip dhcp conflict logging

Command: ip dhcp conflict logging

no ip dhcp conflict logging

Function: Enables logging for address conflicts detected by the DHCP server; the “**no ip dhcp conflict logging”** command disables the logging.

Default: Logging for address conflict is enabled by default.

Command mode: Global Mode

Usage Guide: When logging is enabled, once the address conflict is detected by the DHCP server, the conflicting address will be logged. Addresses present in the log for conflicts will not be assigned dynamically by the DHCP server until the conflicting records are deleted.

Example: Disable logging for DHCP server.

Switch(config)#no ip dhcp conflict logging

Related Command: clear ip dhcp conflict

1.1.15 ip dhcp disable

This command is not supported by the switch.

1.1.16 ip dhcp excluded-address

Command: ip dhcp excluded-address <*low-address*> [<*high-address*>]

no ip dhcp excluded-address <*low-address*> [<*high-address*>]

Function: Specifies addresses excluding from dynamic assignment; the “**no ip dhcp**

excluded-address <*low-address*> [<*high-address*>]" command cancels the setting.

Parameters: <*low-address*> is the starting IP address, **[<*high-address*>]** is the ending IP address.

Default: Only individual address is excluded by default.

Command mode: Global Mode

Usage Guide: This command can be used to exclude one or several consecutive addresses in the pool from being assigned dynamically so that those addresses can be used by the administrator for other purposes.

Example: Reserving addresses from 10.1.128.1 to 10.1.128.10 from dynamic assignment.

Switch(config)#ip dhcp excluded-address 10.1.128.1 10.1.128.10

1.1.17 ip dhcp pool

Command: ip dhcp pool <*name*>

no ip dhcp pool <*name*>

Function: Configures a DHCP address pool and enter the pool mode; the "**no ip dhcp pool <*name*>**"command deletes the specified address pool.

Parameters: <*name*> is the address pool name, up to 32 characters are allowed.

Command mode: Global Mode

Usage Guide: This command is used to configure a DHCP address pool under Global Mode and enter the DHCP address configuration mode.

Example: Defining an address pool named "1".

Switch(config)#ip dhcp pool 1

Switch(dhcp-1-config)#

1.1.18 ip dhcp conflict ping-detection enable

Command: ip dhcp conflict ping-detection enable

no ip dhcp conflict ping-detection enable

Function: Enable Ping-detection of conflict on DHCP server; the **no** operation of this command will disable the function.

Parameters: None.

Default Settings: By default, Ping-detection of conflict is disabled.

Command Mode: Global Configuration Mode.

Usage Guide: To enable Ping-detection of conflict, one should enable the log of conflict addresses, when which is disabled, so will the ping-detection of conflict. When a client is unable to receive Ping request messages (when blocked by firewall, for example), this function will check local ARP according to allocated IP: if a designated IP has a

corresponding ARP, then an address conflict exists; otherwise, allocate it to the client.

Examples: Enable Ping-detection of conflict.

Switch(config)#ip dhcp conflict ping-detection enable

Related Command: ip dhcp conflict logging, ip dhcp ping packets, ip dhcp ping timeout

1.1.19 ip dhcp ping packets

Command: ip dhcp ping packets *<request-num>*

no ip dhcp ping packets

Function: Set the max number of Ping request (Echo Request) message to be sent in Ping-detection of conflict on DHCP server, whose default value is 2; the **no** operation of this command will restore the default value.

Parameters: *<request-num>* is the number of Ping request message to be sent in Ping-detection of conflict.

Default Settings: No more than 2 Ping request messages will be sent by default.

Command Mode: Global Configuration Mode.

Examples: Set the max number of Ping request (Echo Request) message to be sent in Ping-detection of conflict on DHCP server as 3.

Switch(config)#ip dhcp ping packets 3

Related Command: ip dhcp conflict ping-detection enable, ip dhcp ping timeout

1.1.20 ip dhcp ping timeout

Command: ip dhcp ping timeout *<timeout-value>*

no ip dhcp ping timeout

Function: Set the timeout period (in ms) of waiting for a reply message (Echo Request) after each Ping request message (Echo Request) in Ping-detection of conflict on DHCP server, whose default value is 500ms. The **no** operation of this command will restore the default value.

Parameters: *<timeout-value>* is the timeout period of waiting for a reply message after each Ping request message in Ping-detection of conflict.

Default Settings: The timeout period is 500ms by default.

Command Mode: Global Configuration Mode.

Examples: Set the timeout period (in ms) of waiting for each reply message (Echo Request) in Ping-detection of conflict on DHCP server as 600ms.

Switch(config)# ip dhcp ping time out 600

Related Command: ip dhcp conflict ping-detection enable, ip dhcp ping packets

1.1.21 lease

Command: lease { [<*days*>] [<*hours*>][<*minutes*>] | infinite }

no lease

Function: Sets the lease time for addresses in the address pool; the "**no lease**" command restores the default setting.

Parameters: <*days*> is number of days from 0 to 365; **<*hours*>** is number of hours from 0 to 23; **<*minutes*>** is number of minutes from 0 to 59; **infinite** means perpetual use.

Default: The default lease duration is 1 day.

Command Mode: DHCP Address Pool Mode

Usage Guide: DHCP is the protocol to assign network addresses dynamically instead of permanently, hence the introduction of ease duration. Lease settings should be decided based on network conditions: too long lease duration offsets the flexibility of DHCP, while too short duration results in increased network traffic and overhead. The default lease duration of switch is 1 day.

Example: Setting the lease of DHCP pool "1" to 3 days 12 hours and 30 minutes.

Switch(dhcp-1-config)#lease 3 12 30

1.1.22 max-lease-time

Command: max-lease-time {[<*days*>] [<*hours*>] [<*minutes*>] | infinite}

no max-lease-time

Function: Set the maximum lease time for the addresses in the address pool; the no command restores the default setting.

Parameters: <*days*> is number of days from 0 to 365; **<*hours*>** is number of hours from 0 to 23; **<*minutes*>** is number of minutes from 0 to 59; **infinite** means perpetual use.

Default: The default lease time is 1 day.

Command Mode: DHCP Address Pool Mode

Usage Guide: This command is used to DHCP request packets with option51. If the lease time (user requests the address) exceeds the maximum lease time configured, the lease that DHCP server assigns the address is the maximum lease time configured. If the lease time requested by the user is less than the maximum lease time configured, the lease that DHCP server assigns the address is the lease time requested by the user. The maximum lease time is able to be set by the administrator according to the actual network condition, and the maximum lease time is 1 day by default.

Example: Set the maximum lease time of DHCP address pool1 to 3 days 12 hours and 30 minutes.

Switch(dhcp-1-config)#max-lease-time 3 12 30

1.1.23 netbios-name-server

Command: netbios-name-server <*address1*>[<*address2*>[…<*address8*>]]

no netbios-name-server

Function: Configures WINS servers' address; the "**no netbios-name-server**" command deletes the WINS server.

Parameters: <*address1*>…<*address8*> are IP addresses, in decimal format.

Default: No WINS server is configured by default.

Command Mode: DHCP Address Pool Mode

Usage Guide: This command is used to specify WINS server for the client, up to 8 WINS server addresses can be configured. The WINS server address assigned first has the highest priority. Therefore, address 1 has the highest priority, and address 2 the second, and so on.

Example: Setting the server address of DHCP pool "1" to 192.168.1.1.

Switch(dhcp-1-config)#netbios-name-server 192.168.1.1

1.1.24 netbios-node-type

Command: netbios-node-type {b-node | h-node | m-node | p-node | <*type-number*>}

no netbios-node-type

Function: Sets the node type for the specified port; the "**no netbios-node-type**" command cancels the setting.

Parameters: b-node stands for broadcasting node, **h-node** for hybrid node that broadcasts after point-to-point communication; **m-node** for hybrid node to communicate in point-to-point after broadcast; **p-node** for point-to-point node; **<*type-number*>** is the node type in Hex from 0 to FF.

Default: No client node type is specified by default.

Command Mode: DHCP Address Pool Mode

Usage Guide: If client node type is to be specified, it is recommended to set the client node type to **h-node** that broadcasts after point-to-point communication.

Example: Setting the node type for client of pool 1 to broadcasting node.

Switch(dhcp-1-config)#netbios-node-type b-node

1.1.25 network-address

Command: network-address <*network-number*> [<*mask*> | <*prefix-length*>]

no network-address

Function: Sets the scope for assignment for addresses in the pool; the "**no network-address**" command cancels the setting.

Parameters: ***<network-number>*** is the network number; ***<mask>*** is the subnet mask in the decimal format; ***<prefix-length>*** stands for mask in prefix form. For example, mask 255.255.255.0 in prefix is “24”, and mask 255.255.255.252 in prefix is “30”. Note: When using DHCP server, the pool mask should be longer or equal to that of layer 3 interface IP address in the corresponding segment.

Default: If no mask is specified, default mask will be assigned according to the address class.

Command Mode: DHCP Address Pool Mode

Usage Guide: This command sets the scope of addresses that can be used for dynamic assignment by the DHCP server; one address pool can only have one corresponding segment. This command is exclusive with the manual address binding command “hardware address” and “host”.

Example: Configuring the assignable address in pool 1 to be 10.1.128.0/24.

Switch(dhcp-1-config)#network-address 10.1.128.0 24

1.1.26 next-server

Command: next-server <*address1*>[<*address2*>[…<*address8*>]]

no next-server

Function: Sets the server address for storing the client import file; the “**no next-server**” command cancels the setting.

Parameters: ***<address1>…<address8>*** are IP addresses, in the decimal format.

Command Mode: DHCP Address Pool Mode

Usage Guide: This command configures the address for the server hosting client import file. This is usually used for diskless workstations that need to download configuration files from the server on boot up. This command is used together with “bootfile”.

Example: Setting the hosting server address as 10.1.128.4.

Switch(dhcp-1-config)#next-server 10.1.128.4

1.1.27 option

Command: option <*code*> {ascii <*string*> | hex <*hex*> | ipaddress <*ipaddress*>}

no option <*code*>

Function: Sets the network parameter specified by the option code; the “**no option <*code*>**“command cancels the setting for option.

Parameters: ***<code>*** is the code for network parameters; ***<string>*** is the ASCII string up to 255 characters; ***<hex>*** is a value in Hex that is no greater than 510 and must be of even length; ***<ipaddress>*** is the IP address in decimal format, up to 63 IP addresses can be configured.

Command Mode: DHCP Address Pool Mode

Default: None

Usage Guide: The switch provides common commands for network parameter configuration as well as various commands useful in network configuration to meet different user needs. The definition of option code is described in detail in RFC2123.

Example: Setting the WWW server address as 10.1.128.240.

Switch(dhcp-1-config)#option 72 ip 10.1.128.240

1.1.28 service dhcp

Command: service dhcp

no service dhcp

Function: Enables DHCP server; the "**no service dhcp**" command disables the DHCP service.

Parameters: None

Default: DHCP service is disabled by default.

Command mode: Global Mode

Usage Guide: Both DHCP server and DHCP relay are included in the DHCP service. When DHCP services are enabled, both DHCP server and DHCP relay are enabled. Switch can only assign IP address for the DHCP clients and enable DHCP relay when DHCP server function is enabled.

Example: Enabling DHCP server.

Switch(config)#service dhcp

1.1.29 show ip dhcp binding

Command: show ip dhcp binding [[*<ip-addr>*] [type {all | manual | dynamic}] [count]]

Function: Displays IP-MAC binding information.

Parameters: ***<ip-addr>*** is a specified IP address in decimal format; **all** stands for all binding types (manual binding and dynamic assignment); **manual** for manual binding; **dynamic** for dynamic assignment; **count** displays statistics for DHCP address binding entries.

Command mode: Admin and Configuration Mode.

Example:

Switch# show ip dhcp binding

IP address	Hardware address	Lease expiration	Type
10.1.1.233	00-00-E2-3A-26-04	Infinite	Manual
10.1.1.254	00-00-E2-3A-5C-D3	60	Automatic

Displayed information	Explanation
IP address	IP address assigned to a DHCP client
Hardware address	MAC address of a DHCP client
Lease expiration	Valid time for the DHCP client to hold the IP address
Type	Type of assignment: manual binding or dynamic assignment.

1.1.30 show ip dhcp conflict

Command: show ip dhcp conflict

Function: Displays log information for addresses that have a conflict record.

Command mode: Admin and Configuration Mode.

Example:

Switch# show ip dhcp conflict

IP Address Detection method Detection Time

10.1.1.1 Ping FRI JAN 02 00:07:01 2002

Displayed information	Explanation
IP Address	Conflicting IP address
Detection method	Method in which the conflict is detected.
Detection Time	Time when the conflict is detected.

1.1.31 show ip dhcp relay information option

Command: show ip dhcp relay information option

Function: Show the relative configuration for DHCP relay option82.

Parameters: None.

Command mode: Admin and configuration mode

Default: None.

Usage guide: None.

Example: Set the admin mode timeout value to 6 minutes.

Switch#show ip dhcp relay information option

ip dhcp server relay information option(i.e. option 82) is enabled

ip dhcp relay information option(i.e. option 82) is enabled

1.1.32 show ip dhcp server statistics

Command: show ip dhcp server statistics

Function: Displays statistics of all DHCP packets for a DHCP server.

Command mode: Admin and Configuration Mode.

Example:

```
Switch# show ip dhcp server statistics
Address pools               3
Database agents             0
Automatic bindings          2
Manual bindings             0
Conflict bindings           0
Expired bindings            0
Malformed message           0

Message                     Received
BOOTREQUEST                 3814
DHCPDISCOVER                1899
DHCPREQUEST                 6
DHCPDECLINE                 0
DHCPRELEASE                 1
DHCPINFORM                  1

Message                     Send
BOOTREPLY                   1911
DHCPOFFER                   6
DHCPACK                     6
DHCPNAK                     0
DHCPRELAY                   1907
DHCPFORWARD                 0
Switch#
```

Displayed information	Explanation
Address pools	Number of DHCP address pools configured.
Database agents	Number of database agents.
Automatic bindings	Number of addresses assigned automatically
Manual bindings	Number of addresses bound manually
Conflict bindings	Number of conflicting addresses
Expired bindings	Number of addresses whose leases are expired
Malformed message	Number of error messages.

Message Received	Statistics for DHCP packets received
BOOTREQUEST	Total packets received
DHCPDISCOVER	Number of DHCPDISCOVER packets
DHCPREQUEST	Number of DHCPREQUEST packets
DHCPDECLINE	Number of DHCPDECLINE packets
DHCPRELEASE	Number of DHCPRELEASE packets
DHCPINFORM	Number of DHCPINFORM packets
Message Send	Statistics for DHCP packets sent
BOOTREPLY	Total packets sent
DHCPOFFER	Number of DHCPOFFER packets
DHCPACK	Number of DHCPACK packets
DHCPNAK	Number of DHCPNAK packets
DHCPRELAY	Number of DHCPRELAY packets
DHCPFORWARD	Number of DHCPFORWARD packets

1.2 Commands for DHCP Relay Configuration

1.2.1 ip dhcp broadcast suppress

Command: ip dhcp broadcast suppress

no ip dhcp broadcast suppress

Function: Enable DHCP broadcast suppress function, the **no** command disables the function.

Parameter: None.

Default: Disable.

Command Mode: Global mode

Usage Guide: Suppress the forwarding about DHCP broadcast packets, namely, drop or copy DHCP broadcast packets to CPU.

Example: Enable DHCP broadcast suppress function.

Switch(config)#ip dhcp broadcast suppress

1.2.2 ip dhcp relay share-vlan <vlanid> sub-vlan <vlanlist>

This command is not supported by the switch.

1.2.3 ip forward-protocol udp bootps

Command: ip forward-protocol udp bootps

no ip forward-protocol udp bootps

Function: Sets DHCP relay to forward UPD broadcast packets on the port; the "**no ip forward-protocol udp bootps**"command cancels the service.

Parameter: bootps forwarding UDP port as 67 DHCP broadcast packets.

Default: Not forward UPD broadcast packets by default.

Command Mode: Global Mode

Usage Guide: The forwarding destination address is set in the "**ip helper-address**" command and described later.

Example: Setting DHCP packets to be forwarded to 192.168.1.5.

Switch(config)#ip forward-protocol udp boots

Switch(config)#interface vlan 1

Switch(Config-if-Vlan1)#ip helper-address 192.168.1.5

1.2.4 ip helper-address

Command: ip helper-address <*ip-address*>

no ip helper-address <*ip-address*>

Function: Specifies the destination address for the DHCP relay to forward UDP packets. The "**no ip helper-address <*ip-address*>**" command cancels the setting.

Default: None.

Command Mode: Interface Configuration Mode

Usage Guide: The DHCP relay forwarding server address corresponds to the port forwarding UDP, i.e. DHCP relay forwards corresponding UDP packets only to the corresponding server instead of all UDP packets to all servers. When this command is run after "**ip forward-protocol udp <*port*>**" command, the forwarding address configured by this command receives the UDP packets from **<*port*>**. The combination of "**ip forward-protocol udp <*port*>**" command and this command should be used for configuration.

1.2.5 show ip forward-protocol

Command: show ip forward-protocol

Function: Show the configured port ID of the protocol which support the forwarding of broadcast packets, it means the port ID for forwarding DHCP packets.

Command Mode: Admin and configuration mode

Example:

Switch#show ip forward-protocol

Forward protocol(UDP port): 67(active)

1.2.6 show ip helper-address

Command: show ip helper-address

Function: Show the configuration relation for the port ID of the protocol (It can forward broadcast packets), the interface (It supports forwarding function) and the forwarded destination IP.

Command Mode: Admin and configuration mode

Example:

Switch#show ip helper-address

Forward protocol	Interface	Forward server
67(active)	Vlan1	192.168.1.1

Chapter 2 Commands for DHCPv6

2.1 clear ipv6 dhcp binding

Command: clear ipv6 dhcp binding [<*ipv6-address*>] [pd <*ipv6-prefix* | *prefix-length*>]

Function: To clear one specified DHCPv6 assigned address binding record or all the IPv6 address binding records.

Parameter: ***<ipv6-address>*** is the specified IPv6 address with binding record; ***<ipv6-prefix| prefix-length>*** is the specified IPv6 prefix with binding record; To clear all IPv6 address binding record if there is no specified record.

Command Mode: Admin Configuration Mode.

Usage Guide: DHCPv6 IPv6 address binding information can be displayed through the command show ipv6 dhcp binding. If DHCPv6 client does not use the DHCPv6 allocated IPv6 address but when the life time of the IPv6 address does not end, the DHCPv6 server will not remove its bind for this address. In this situation, the address binding information can be removed manually through this command; and if no parameter is appended, this command will remove all the address binding information, then all addresses and prefix will be assigned again in the DHCPv6 address pool.

Example: To delete all binding record of IPv6 address and prefix.

Switch#clear ipv6 dhcp binding

Relative Command: show ipv6 dhcp binding

2.2 clear ipv6 dhcp conflict

Command: clear ipv6 dhcp conflict [<*address*>]

Function: Clear the address with the conflict record in address conflict log.

Parameter: ***<address>*** is the specified address with the conflict record, no specified address will clear all conflict records.

Command Mode: Admin Mode

Usage Guide: With **show ipv6 dhcp conflict** command, the user can check the conflict in which IP addresses. With this command, the user can clears the conflict record of an address. If no specified address will clear the conflict record of all addresses in log. After the conflict records are cleared in log, these addresses can be used by DHCPv6 server again.

Example: When administrator checks the conflict logs, administrator discovers that

address 2001::1 with the conflict record is not used, so its record will be cleared from address conflict files.

Switch#clear ipv6 dhcp conflict 2001::1

2.3 clear ipv6 dhcp statistics

Command: clear ipv6 dhcp statistics

Function: Clear the statistic records of DHCPv6 packets, the statistic counter of DHCPv6 packets is cleared.

Parameter: None.

Command mode: Admin Mode

Usage Guide: With **show ipv6 dhcp statistics** command, the user can check the statistic information of the counter for DHCPv6 packets, all statistic information is an accumulative value. With this command will clear the counter to check the debugging conveniently.

Example: Clear the counter of DHCPv6 packets.

Switch#clear ipv6 dhcp statistics

Relative Command: show ipv6 dhcp statistics

2.4 debug ipv6 dhcp client packet

Command: debug ipv6 dhcp client {event | packet}

no debug ipv6 dhcp client {event | packet}

Function: To enable the debugging messages for protocol packets of DHCPv6 prefix delegation client, the no form of this command will disable the debugging information.

Default: Disabled.

Command Mode: Admin Mode.

Example:

Switch# debug ipv6 dhcp client packet

2.5 debug ipv6 dhcp detail

Command: debug ipv6 dhcp detail

no debug ipv6 dhcp detail

Function: To display the debug information of all kinds of packets received or sent by DHCPv6, the no form of this command disabled this function.

Default: Disabled.

Command Mode: Admin Mode.

Example:

Switch# debug ipv6 dhcp detail

2.6 debug ipv6 dhcp relay packet

Command: debug ipv6 dhcp relay packet

no debug ipv6 dhcp relay packet

Function: To enable the debugging information for protocol packets of DHCPv6 relay, the no form of this command will disable the debugging.

Default: Disabled.

Command Mode: Admin Mode.

Example:

Switch# debug ipv6 dhcp relay packet

2.7 debug ipv6 dhcp server

Command: debug ipv6 dhcp server { event | packet }

no debug ipv6 dhcp server { event | packet }

Function: To enable the debugging information of DHCPv6 server, the no form of this command will disable the debugging.

Parameter: event is to enable debugging messages for DHCPv6 server events, such as address allocation; packet is for debugging messages of protocol packets of DHCPv6 server.

Default: Disabled.

Command Mode: Admin Mode.

Example:

Switch#debug ipv6 dhcp server packet

2.8 dns-server

Command: dns-server *<ipv6-address>*

no dns-server *<ipv6-address>*

Function: To configure the IPv6 address of the DNS server for DHCPv6 client; the no form of this command will remove the DNS configuration.

Parameter: *<ipv6-address>* is the IPv6 address of DNS Server.

Default: No configured address pool of DNS Server by default.

Command Mode: DHCPv6 Address Pool Configuration Mode.

Usage Guide: For each address pool, at most three DNS server can be configured, and the addresses of the DNS server must be valid IPv6 addresses.

Example: To configure the DNS Server address of DHCPv6 client as 2001:da8::1.

Switch(dhcp-1-config)#dns-server 2001:da8::1

2.9 domain-name

Command: domain-name *<domain-name>*

no domain-name *<domain-name>*

Function: To configure domain name of DHCPv6 client; the no form of this command will delete the domain name.

Parameter: *<domain-name>* is the domain name, less than 32 characters.

Command Mode: DHCPv6 Address Pool Configuration Mode.

Default: The domain name parameter of address pool is not configured by default.

Usage Guide: At most 3 domain names can be configured for each address pool.

Example: To set the domain name of DHCPv6 client as test.com.cn

Switch(dhcp-1-config)#domain-name test.com.cn

2.10 excluded-address

Command: excluded-address *<ipv6-address>*

no excluded-address *<ipv6-address>*

Function: To configure the specified IPv6 address to be excluded from the address pool, the excluded address will not be allocated to any hosts; the **no** form of this command will remove the configuration.

Parameter: *<ipv6-address>* is the IPv6 address to be excluded from being allocated to hosts in the address pool.

Default: Disabled

Command Mode: DHCPv6 address pool configuration mode.

Usage Guide: This command is used to preserve the specified address from DHCPv6 address allocation.

Example: To configure to exclude 2001:da8:123::1 from DHCPv6 address allocation.

Switch(config)#excluded-address 2001:da8:123::1

2.11 ipv6 address

Command: ipv6 address *<prefix-name> <ipv6-prefix/prefix-length>*

no ipv6 address *<prefix-name> <ipv6-prefix/prefix-length>*

Function: To configure the specified interface to use prefix delegation for address allocation. The **no** form of this command will disable the using of prefix delegation for address allocation.

Parameters: *<prefix-name>* is a string with its length no more than 32, designating or manual configuring the name of the address prefix defined in the prefix pool. ***<ipv6-prefix/prefix-length>*** is latter part of the IPv6 address excluding the address prefix, as well as its length.

Command Mode: Interface Configuration Mode.

Default: No global address is configured for interfaces by default.

Usage Guide: The IPv6 address of an interface falls into two parts: ***<prefix-name>*** and ***<ipv6-prefix>/<prefix-length>***. If routing advertisement has been enabled, the first 64 bits of the addresses will be advertised. The address generated by ***<prefix-name>*** and ***<ipv6-prefix/prefix-length>*** combination will be removed, and the advertising of the prefix will be disabled. Only one ***<ipv6-prefix/prefix-length>*** can be configured for one prefix name.

Example: If the prefix name my-prefix designates 2001:da8:221::/48, then the following command will add the address 2001:da8:221:2008::2008 to interface VLAN1.

Switch(Config-if-Vlan1)# ipv6 address my-prefix 0:0:0:2008::2008/64

2.12 ipv6 dhcp client pd

Command: ipv6 dhcp client pd *<prefix-name>* [rapid-commit]

no ipv6 dhcp client pd

Function: To configure DHCPv6 prefix delegation client for the specified interface. The no form of this command will disable the DHCPv6 prefix delegation client and remove the allocated address prefix.

Parameters: *<prefix-name>* is the string with its length no more than 32, which designates the name of the address prefix. If rapid-commit optional is specified and the prefix delegation server enables the rapid-commit function, then the prefix delegation server will reply the prefix delegation client with the REPLY message directly. And the prefix delegation request will be accomplished by exchanging messages once.

Command Mode: Interface Configuration Mode.

Default: DHCPv6 prefix delegation client is not enabled by default.

Usage Guide: This command is used to configure the prefix delegation client on the specified interface, an interface with prefix delegation client enabled will send SOLICIT packets to try to get address prefix from the server. If the prefix is retrieved correctly, the address prefix in the global address pool can be used by the **ipv6 address** command to generate a valid IPv6 address. This command is exclusive with **ipv6 dhcp server** and **ipv6 dhcp relay destination**. If the prefix delegation client is disabled for an interface, then the address prefix which is get from this interface through prefix delegation client, will be removed from the global address pool. Also the interface address which is generated by the prefix delegation client will be removed, and routing advertisement with the prefix will be disabled. If any general prefix has been configured by the **ipv6 general-prefix** command, the same prefix learnt from prefix delegation will be disagreed.

Example:

Switch(Config-if-Vlan1)#ipv6 dhcp client pd ClientA rapid-commit

2.13 ipv6 dhcp client pd hint

Command: ipv6 dhcp client pd hint *<prefix|prefix-length>*

no ipv6 dhcp client pd hint *<prefix|prefix-length>*

Function: Designate the prefix demanded by the client and its length. The **no** operation of this command will delete that prefix and its length from the specified interface.

Parameters: *<prefix|prefix-length>* means the prefix demanded by the client and its length.

Command Mode: Interface Configure Mode.

Default Settings: There is no such configuration in the system by default.

Usage Guide: The system designates a prefix and its length on the interface for a client. If client prefix-proxy demanding function is enabled on the interface and hint function is enabled on the switch, the user will have prior claim to the prefix it demands and the prefix length when the server allocates them. Only one hint prefix is allowed in the system.

Examples:

Switch(vlan-1-config)#ipv6 dhcp client pd hint 2001::/48

2.14 ipv6 dhcp pool

Command: ipv6 dhcp pool *<poolname>*

no ipv6 dhcp pool *<poolname>*

Function: To configure the address pool for DHCPv6, and enter the DHCPv6 address pool configuration mode. In this mode, information such as the address prefix to be

allocated, the DNS server addresses, and domain names, can be configured for the DHCPv6 client. The **no** form of this command will remove the configuration of the address pool.

Parameter: < *poolname*> is the address pool name of DHCPv6 with its length no more than 32.

Default: Any DHCPv6 address pool are not configured by default.

Command Mode: Global Mode.

Usage Guide: This command should be launched in global configuration mode, and falls in DHCPv6 address pool configuration mode if launched successfully. To remove a configured address pool, interface bindings related to the address pool, as well as the related address bindings will be removed.

Example: To define an address pool, named 1.

Switch(config)#ipv6 dhcp pool 1

2.15 ipv6 dhcp relay destination

Command: ipv6 dhcp relay destination {[<*ipv6-address*>] [interface { <*interface-name*> | vlan <*1-4096*> }] }

no ipv6 dhcp relay destination { [<*ipv6-address*>] [interface { <*interface-name*> | vlan <*1-4096*> }] }

Function: To configure the destination to which the DHCPv6 relay forwards the DHCPv6 requests from the clients, the destination should be the address of an external DHCPv6 relay or the DHCPv6 server. The **no** form of this command will remove the configuration.

Parameters: *<ipv6-address>* is the address of the destination to which the DHCPv6 relay forwards; ***<interface-name>*** or VLAN is the interface name or VLAN id which is used for forwarding of DHCPv6 requests, ***<interface-name>*** should be a lay three VLAN name, and the VLAN id is limited between 1 and 4096. If ***<ipv6-addess>*** is a global unicast address, the **interface** parameter should not be configured; If ***<ipv6-address>*** is an local address, the **interface** parameter is required be configured; The destination address for the DHCPv6 server will be the multicast address of **ALL_DHCP_Servers (FF05::1:3)**, if the interface parameter is configured only.

Command Mode: Interface Configuration Mode.

Default: By default, destination address for DHCPv6 relay is not configured.

Usage Guide: This command is used to configure the DHCPv6 relay for the specified interface, the address should be the address of another DHCPv6 relay or the address DHCPv6 server. At most three relay addresses can be configured for an interface. To be mentioned, the DHCPv6 relay stops working only if all the relay destination address configurations have been removed. This command is mutually exclusive to "**ipv6 dhcp**

server" and "**ipv6 dhcp client pd**" commands.

Example:

Switch(Config-if-Vlan1)#ipv6 dhcp relay destination 2001:da8::1

2.16 ipv6 dhcp server

Command: ipv6 dhcp server <*poolname*> [preference <*value*>] [rapid-commit] [allow-hint]

no ipv6 dhcp server <*poolname*>

Function: This command configures the address pool which will be allocated by the DHCPv6 server through the specified interface. The **no** form of this command will remove the address pool configuration.

Parameters: <*poolname*> is a string with its length less than 32, which designates the name of the address pool which is associated with the specified interface. If the **rapid-commit** option has been specified, the DHCPv6 server send a REPLY packet to the client immediately after receiving the SOLICIT packet. If the **preference** option has been specified, **<*value*>** will be the priority of the DHCPv6 server, with its value allowed between 0 and 255, and with 0 by default, the bigger the preference value is, the higher the priority of the DHCPv6 server. If the **allow-hint** option has been specified, the client expected value of parameters will be appended in its request packets.

Command Mode: Interface Configuration Mode.

Default: DHCPv6 address pool based on port is not configured by default.

Usage Guide: This command configure the DHCPv6 address pool which is applied by the DHCPv6 server for the specified interface, as well as optional parameters. One VLAN can bind many DHCPv6 address pools and assign the address for DHCPv6 request packet from direct-link and relay delegation.

Example:

Switch(Config-if-Vlan1)#ipv6 dhcp server PoolA preference 80 rapid-commit allow-hint

2.17 ipv6 general-prefix

Command: ipv6 general-prefix <*prefix-name*> <*ipv6-prefix/prefix-length*>

no ipv6 general-prefix <*prefix-name*>

Function: To define an IPv6 general prefix. The **no** form of this command will delete the configuration.

Parameter: <*prefix-name*> is a character string less than 32 characters, to use as IPv6 general prefix name. **<*ipv6-prefix/prefix-length*>** is defined as IPv6 general prefix.

Command Mode: Global Mode.

Default: IPv6 general prefix is not configured by default.

Usage Guide: If IPv6 general prefix is configured, the interface will use the configured prefix for IPv6 address generating. Commonly, the general prefix is used for enterprise IPv6 prefix, and when entering an IPv6 address, users can simply add the address suffix of to the name of the general prefix. The configured address prefix will be reserved in the general address prefix pool. At most 8 general prefix can be configured at the same time. When trying to remove a configured general prefix name, the operation will fail if any interfaces used the configured prefix. Only one general prefix for a prefix name. The general prefix can not use the same prefix definition with prefixes learnt from prefix delegation.

Example: To set the prefix of 2001:da8:221::/48 to general prefix my-prefix.

Switch(config)# ipv6 general-prefix my-prefix 2001:da8:221::/48

2.18 ipv6 local pool

Command: ipv6 local pool *<poolname> <prefix/prefix-length> <assigned-length>*

no ipv6 local pool *<poolname>*

Function: To configure the address pool for prefix delegation. The **no** form of this command will remove the IPv6 prefix delegation configuration.

Parameters: *<poolname>* is the name for the IPv6 address pool of the prefix delegation, the length name string should be less than 32. ***<prefix/prefix-length>*** is the address prefix and its length of the prefix delegation. ***<assigned-length>*** is the length of the prefix in the address pool which can be retrieved by the client, the assigned prefix length should be no less than the value of ***<prefix-length>***

Command Mode: Global Mode.

Default: No IPv6 prefix delegation address pool is configured by default.

Usage Guide: This command should be used with the "**prefix delegation pool**" command to allocate address prefixes to the clients. If IPv6 prefix delegation is removed, the associated "**prefix delegation**" command will be in-effective either.

2.19 lifetime

Command: lifetime {*<valid-time>* | infinity} {*<preferred-time>* | infinity}

no lifetime

Function: To configure the life time for the addresses or the address prefixes allocated by DHCPv6. The **no** form of this command will restore the default setting.

Parameters: <*valid-time*> and <*preferred-time*> are the valid life time and preferred life time respectively for the allocated IPv6 addresses in the local address pool. Its value is allowed to be between 1 and 31536000 in seconds, and **<*preferred-time*>** should never be bigger than **<*valid-time*>**. The **infinity** parameter designates the maximum life time.

Command Mode: DHCPv6 Address Pool Configuration Mode.

Default: The default valid life time and preferred life time are 2592000 seconds (30 days) and 604800 seconds (7 days) respectively.

Example: To configure the valid life time as 1000 seconds, and the preferred life time as 600 seconds.

Switch(config)#lifetime 1000 600

2.20 network-address

Command: network-address <*ipv6-pool-start-address*> {<*ipv6-pool-end-address*> | <*prefix-length*>} [eui-64]

no network-address

Function: To configure the DHCPv6 address pool; the **no** form of this command will remove the address pool configuration.

Parameters: <*ipv6-pool-start-adderss*> is the start of the address pool; **<*ipv6-pool-end-address*>** is the end of the address pool; **<*prefix-length*>** is the length of the address prefix, which is allowed to be between 3 and 128, and 64 by default, the size of the pool will be determined by **<*prefix-length*>** if it has been specified. **<*ipv6-pool-end-address*>** and **<*prefix-length*>** alternative options to determine the size of the IPv6 address pool. If **<*prefix-length*>** is 64 and the **eui-64** option has been configured, the DHCPv6 server will allocate IPv6 addresses according to the EUI-64 standard, or the DHCPv6 server will be allocating addresses sequentially.

Default: No address pool is configured by default.

Command Mode: DHCPv6 Address Pool Configuration Mode.

Usage Guide: This command configures the address pool for the DHCPv6 server to allocate addresses, only one address range can be configured for each address pool. To be noticed, if the DHCPv6 server has been enabled, and the length of the IPv6 address prefix has been configured, the length of the prefix in the address pool should be no less than the length of the prefix of the IPv6 address of the respective layer three interfaces in the switch. If **<*ipv6-pool-end-address*>** is bigger than **<*ipv6-pool-start-address*>**, this command returns at once.

Example: To configure the address range for address pool as 2001:da8:123::100-2001:da8:123::200.

Switch(dhcp-1-config)#network-address 2001:da8:123::100 2001:da8:123::200

Relative Command: excluded-address

2.21 prefix-delegation

Command: prefix-delegation <*ipv6-prefix/prefix-length*> <*client-DUID*> [iaid <*iaid*>] [lifetime {<*valid-time*> | infinity} {<*preferred-time*> | infinity}]

no prefix-delegation <*ipv6-prefix/prefix-length*> <*client-DUID*> [iaid <*iaid*>]

Function: To configure dedicated prefix delegation for the specified user. The **no** form of this command will remove the dedicated prefix delegation.

Parameters: <*ipv6-prefix/prefix-length*> is the length of the prefix to be allocated to the client. **<*client-DUID*>** is the DUID of the client. DUID with the type of DUID-LLT and DUID-LL are supported, the DUID of DUID-LLT type should be of 14 characters. **<*iaid*>** is the value to be appended in the IA_PD field of the clients' requests. **<*valid-time*>** and **<*preferred-time*>** are the valid life time and the preferred life time of the IPv6 address allocated to the clients respectively, in seconds, and its value is allowed between 1 and 31536000. However, **<*preferred-time*>** should never be bigger than **<*valid-time*>**. If not configured, the default **<*valid-time*>** will be 2592000, while **<*preferred-time*>** will be 604800. The **infinity** parameter means the life time is infinity.

Command Mode: DHCPv6 Address Pool Configuration Mode.

Default: Disabled.

Usage Guide: This command configures the specified IPv6 address prefix to bind with the specified client. If no IAID is configured, any IA of any clients will be able get this address prefix. At most eight static binding address prefix can be configured for each address pool. For prefix delegation, static binding is of higher priority than the prefix address pool.

Example: The following command will allocate 2001:da8::/48 to the client with DUID as 000100060000005000BBFAA2408, and IAID as 12.

Switch(dhcp-1-config)#prefix-delegation 2001:da8::/48 000100060000005000BBFAA2408 iaid 12

2.22 prefix-delegation pool

Command: prefix-delegation pool <*poolname*> [lifetime {<*valid-time*> | infinity} {<*preferred-time*> | infinity}]

no prefix-delegation pool <*poolname*>

Function: To configure prefix delegation name used by DHCPv6 address pool. The **no** form of this command deletes the configuration.

Parameters: ***<poolname>*** is the name of the address prefix pool, the length name string should be less than 32. ***<valid-time>*** and ***<preferred-time>*** are the valid life time and the preferred life time of the IPv6 address allocated to the clients respectively, in seconds, and its value is allowed between 1 and 31536000. However, ***<preferred-time>*** should never be bigger than ***<valid-time>***. If not configured, the default ***<valid-time>*** will be 2592000, while ***<preferred-time>*** will be 604800. The **infinity** parameter means the life time is infinity.

Command Mode: DHCPv6 address pool configuration mode.

Default: The prefix delegation name used by DHCPv6 address pool is not configured.

Usage Guide: This command configures the name of the address prefix pool for address allocation. If configured, the addresses in the prefix address pool will be allocated to the clients. This command can be used in association with the **ipv6 local pool** command. For one address pool, only one prefix delegation pool can be bound. When trying to remove the prefix name configuration, the prefix delegation service of the server will be unavailable, if both the address pool is not associated with the prefix delegation pool and no static prefix delegation binding is enabled.

Example:

Switch(dhcp-1-config)#prefix-delegation pool abc

2.23 service dhcpv6

Command: service dhcpv6

no service dhcpv6

Function: To enable DHCPv6 server function; the no form of this command disables the configuration.

Parameter: None.

Default: Disabled.

Command Mode: Global Mode.

Usage Guide: The DHCPv6 services include DHCPv6 server function, DHCPv6 relay function, DHCPv6 prefix delegation function. All of the above services are configured on ports. Only when DHCPv6 server function is enabled, the IP address assignment of DHCPv6 client, DHCPv6 relay and DHCPv6 prefix delegation functions enabled can be configured on ports.

Example: To enable DHCPv6 server.

Switch(config)#service dhcpv6

2.24 show ipv6 dhcp

Command: show ipv6 dhcp

Function: To show the enable switch and DUID of DHCPv6 service.

Command Mode: Admin and Configuration Mode.

Usage Guide: To show the enable switch and DUID of DHCPv6 service, server identifier options only use DUID of DUID-LLT type.

Example:

Switch#show ipv6 dhcp

DHCPv6 is enabled

LLT DUID is <00:01:00:01:43:b7:1b:81:00:03:0f:01:5f:9d>

LL DUID is <00:03:00:01:00:03:0f:01:5f:9d>

2.25 show ipv6 dhcp binding

Command: show ipv6 dhcp binding [<*ipv6-address*>| pd <*ipv6-prefix*|*prefix-length*>|count]

Function: To show all the address and prefix binding information of DHCPv6.

Parameter: <*ipv6-address*> is the specified IPv6 address; **count** show the number of DHCPv6 address bindings.

Command Mode: Admin and Configuration Mode.

Usage Guide: To show all the address and prefix binding information of DHCPv6, include type, DUID, IAID, prefix, valid time and so on.

Example:

Switch#show ipv6 dhcp binding

Client: iatype IANA, iaid 0x0e001d92

DUID: 00:01:00:01:0f:55:82:4f:00:19:e0:3f:d1:83

IANA leased address: 2001:da8::10

Preferred lifetime 604800 seconds, valid lifetime 2592000 seconds

Lease obtained at %Jan 01 01:34:44 1970

Lease expires at %Jan 31 01:34:44 1970 (2592000 seconds left)

The number of DHCPv6 bindings is 1

2.26 show ipv6 dhcp conflict

Command: show ipv6 dhcp conflict

Function: Show the log for the address that have a conflict record.

Command Mode: Admin and Configuration Mode.

Example:

Switch# show ipv6 dhcp conflict

2.27 show ipv6 dhcp interface

Command: show ipv6 dhcp interface [<*interface-name*>]

Function: To show the information for DHCPv6 interface.

Parameter: ***<interface-name>*** is the name and number of interface, if the***<interface-name>*** parameter is not provided, then all the DHCPv6 interface information will be shown.

Command Mode: Admin and Configuration Mode.

Usage Guide: To show the information for DHCPv6 interface, include Port Mode (Prefix delegation client、DHCPv6 server、DHCPv6 relay) , and the relative conformation information under all kinds of mode.

Example:

Switch#show ipv6 dhcp interface vlan10

Vlan10 is in server mode

Using pool: poolv6

Preference value: 20

Rapid-Commit is disabled

2.28 show ipv6 dhcp pool

Command: show ipv6 dhcp pool [<*poolname*>]

Function: To show the DHCPv6 address pool information.

Parameter: ***<poolname>*** is the DHCPv6 address pool name which configured already, and the length less than 32 characters. If the ***<poolname>*** parameter is not provided, then all the DHCPv6 address pool information will be shown.

Command Mode: Admin and Configuration Mode.

Usage Guide: To display the configuration and dynamic assignment information for DHCPv6 address pool, include the name of DHCPv6 address pool, the prefix of DHCPv6 address pool, excluded address, DNS server configuration, relative prefix information and so on. To display assigned address binding number of address pool that is used as address assignment server. To display assigned prefix number of address pool that is used as prefix delegation server.

Example:

Switch#show ipv6 dhcp pool poolv6

2.29 show ipv6 dhcp statistics

Command: show ipv6 dhcp statistics

Function: To show the statistic of all kinds of DHCPv6 packets by DHCPv6 server.

Command Mode: Admin and Configuration Mode.

Example:

Switch#show ipv6 dhcp server statistics

Address pools	1
Active bindings	0
Expiried bindings	0
Malformed message	0

Message	Recieved
DHCP6SOLICIT	0
DHCP6ADVERTISE	0
DHCP6REQUEST	0
DHCP6REPLY	0
DHCP6RENEW	0
DHCP6REBIND	0
DHCP6RELEASE	0
DHCP6DECLINE	0
DHCP6CONFIRM	0
DHCP6RECONFIGURE	0
DHCP6INFORMREQ	0
DHCP6RELAYFORW	0
DHCP6RELAYREPLY	0

Message	Send
DHCP6SOLICIT	0
DHCP6ADVERTISE	0
DHCP6REQUEST	0
DHCP6REPLY	0
DHCP6RENEW	0
DHCP6REBIND	0
DHCP6RELEASE	0

DHCP6DECLINE 0
DHCP6CONFIRM 0
DHCP6RECONFIGURE 0
DHCP6INFORMREQ 0
DHCP6RELAYFORW 0
DHCP6RELAYREPLY 0

Show information	Explanation
Address pools	To configure the number of DHCPv6 address pools;
Active bindings	The number of auto assign addresses;
Expiried bindings	The number of expiried bindings;
Malformed message	The number of malformed messages;
Message Recieved	The statistic of received DHCPv6 packets.
DHCP6SOLICIT	The number of DHCPv6 SOLICIT packets.
DHCP6ADVERTISE	The number of DHCPv6 ADVERTISE packets.
DHCPv6REQUEST	The number of DHCPv6 REQUEST packets.
DHCP6REPLY	The number of DHCPv6 REPLY packets.
DHCP6RENEW	The number of DHCPv6 RENEW packets.
DHCP6REBIND	The number of DHCPv6 REBIND packets.
DHCP6RELEASE	The number of DHCPv6 RELEASE packets.
DHCP6DECLINE	The number of DHCPv6 DECLINE packets.
DHCP6CONFIRM	The number of DHCPv6 CONFIRM packets.
DHCP6RECONFIGURE	The number of DHCPv6 RECONFIGURE packets.
DHCP6INFORMREQ	The number of DHCPv6 INFORMREQ packets.
DHCP6RELAYFORW	The number of DHCPv6 RELAYFORW packets.
DHCP6RELAYREPLY	The number of DHCPv6 RELAYREPLY packets.
Message Send	The statistic of sending DHCPv6 packets
DHCP6SOLICIT	The number of DHCPv6 SOLICIT packets.
DHCP6ADVERTISE	The number of DHCPv6 ADVERTISE packets.
DHCPv6REQUEST	The number of DHCPv6 REQUEST packets.
DHCP6REPLY	The number of DHCPv6 REPLY packets.
DHCP6RENEW	The number of DHCPv6 RENEW packets.
DHCP6REBIND	The number of DHCPv6 REBIND packets.
DHCP6RELEASE	The number of DHCPv6 RELEASE packets.
DHCP6DECLINE	The number of DHCPv6 DECLINE packets.
DHCP6CONFIRM	The number of DHCPv6 CONFIRM packets.
DHCP6RECONFIGURE	The number of DHCPv6 RECONFIGURE packets.

DHCP6INFORMREQ	The number of DHCPv6 INFORMREQ packets.
DHCP6RELAYFORW	The number of DHCPv6 RELAYFORW packets.

2.30 show ipv6 general-prefix

Command: show ipv6 general-prefix

Function: To show the IPv6 general prefix pool information.

Command Mode: Admin and Configuration Mode.

Usage Guide: To show the IPv6 general prefix pool information, include the prefix number in general prefix pool, the name of every prefix, the interface of prefix obtained, and the prefix value.

Example:

Switch#show ipv6 general-prefix

2.31 show ipv6 local pool

Command: show ipv6 local pool

Function: To show the statistic information of DHCPv6 prefix pool.

Command Mode: Admin and Configuration Mode.

Usage Guide: To show the statistic information of DHCPv6 prefix pool, include the name of prefix pool, the prefix and prefix length as well as assigned prefix length, the number of assigned prefix and information in DHCPv6 address pool.

Example:

Switch#show ipv6 local pool

Pool	Prefix	Free	In use
a	2010::1/48	65536	0

Chapter 3 Commands for DHCP option 60 and option 43

3.1 option 43 ascii LINE

Command: option 43 ascii LINE

no option 43

Function: Configure option 43 character string with ascii format in ip dhcp pool mode. The no command deletes the configured option 43.

Parameter: LINE: The configured option 43 character string with ascii format, its length range between 1 and 255.

Default: No option 43 character string is configured.

Command Mode: ip dhcp pool mode

Usage Guide: None.

Example: Configure option 43 with ascii format to be "AP 1000".

switch(config)#ip dhcp pool a

switch (dhcp-a-config)#option 43 ascii AP 1000

3.2 option 43 hex WORD

Command: option 43 hex WORD

no option 43

Function: Configure option 43 character string with hex format in ip dhcp pool mode. The **no** command deletes the configured option 43.

Parameter: WORD: The configured option 43 character string with hex format, such as a1241b.

Default: No option 43 is configured.

Command Mode: ip dhcp pool mode

Usage Guide: When using hex method to configure option 43, the string needs to be written according to TLV (Type-Length-Value) format. For example, issue ip address of 10.1.1.1 through option 43, then the hex string here should be 01040A010101; Type=0x01, it means IP address; Length=0x04, it means the length of IP address is 4 Bytes; Value=0x0A010101, it means the hexadecimal format of 10.1.1.1.

Example: Configure option 43 with hex format to be "01040a010101".

switch(config)#ip dhcp pool a

switch (dhcp-a-config)#option 43 hex 01040a010101

3.3 option 43 ip A.B.C.D

Command: option 43 ip A.B.C.D

no option 43

Function: Configure option 43 character string with IP format in ip dhcp pool mode. The no command deletes the configured option 43.

Parameter: A.B.C.D: The configured option 43 with IP format, such as 192.168.1.1.

Default: No option 43 is configured.

Command Mode: ip dhcp pool mode

Usage Guide: Using this command to configure option 43, such as "192.168.1.1", then option 43 filled in packets is "C0A80101".

Example: Configure option 43 with IP format to be "192.168.1.1".

switch(config)#ip dhcp pool a

switch (dhcp-a-config)#option 43 ip 192.168.1.1

3.4 option 60 ascii LINE

Command: option 60 ascii LINE

no option 60

Function: Configure option 60 character string with ascii format in ip dhcp pool mode. The **no** command deletes the configured option 60.

Parameter: LINE: The configured option 60 character string with ascii format, its length range between 1 and 255.

Default: No option 60 character string is configured.

Command Mode: ip dhcp pool mode

Usage Guide: The option 60 string parameter of DCWL-7942-W and DCWL-7942-W(H) series AP is udhcp 1.12.1, the option 60 string parameter of other series AP of DCWL -7900 is udhcp 1.18.2.

Example: Configure option 60 with ascii format to be "AP 1000".

switch(config)#ip dhcp pool a

switch (dhcp-a-config)#option 60 ascii AP 1000

3.5 option 60 hex WORD

Command: option 60 hex WORD

no option 60

Function: Configure option 60 character string with hex format in ip dhcp pool mode. The no command deletes the configured option 60.

Parameter: WORD: The configured option 60 character string with hex format, such as a1241b.

Default: No option 60 is configured.

Command Mode: ip dhcp pool mode

Usage Guide: None.

Example: Configure option 60 with hex format to be "41502031303030".

switch(config)#ip dhcp pool a

switch(dhcp-a-config)#option 60 hex 41502031303030

3.6 option 60 ip A.B.C.D

Command: option 60 ip A.B.C.D

no option 60

Function: Configure option 60 character string with IP format in ip dhcp pool mode. The **no** command deletes the configured option 60.

Parameter: A.B.C.D: The configured option 60 with IP format, such as 192.168.1.1.

Default: No option 60 is configured.

Command Mode: ip dhcp pool mode

Usage Guide: Using this command to configure option 60, such as "192.168.1.1", option 60 of packets matched with the configured option 60 is "C0A80101".

Example: Configure option 60 with IP format to be "192.168.1.1".

switch(config)#ip dhcp pool a

switch (dhcp-a-config)#option 60 ip 192.168.1.1

Chapter 4 Commands for DHCP Option 82

4.1 debug ip dhcp relay packet

Command: debug ip dhcp relay packet

Function: This command is used to display the information of data packets processing in DHCP Relay Agent, including the “add” and “peel” action of option 82.

Parameters: None

Command Mode: Admin Mode.

User Guide: Use this command during the operation to display the procedure of data packets processing of the server and to display the corresponding option82 operation information. Identified option 82 information of the request message and the option 82 information returned by the reply message.

Example: Display the information of data packets processing in DHCP Relay Agent.

Switch(config)# debug ip dhcp relay packet

4.2 ip dhcp relay information option

Command: ip dhcp relay information option

no ip dhcp relay information option

Function: Set this command to enable the option82 function of the switch Relay Agent. The “**no ip dhcp relay information option**” command is used to disable the option82 function of the switch Relay Agent.

Parameters: None.

Default Settings: The system disables the option82 function by default.

Command Mode: Global configuration mode

Usage Guide: Only the DHCP Relay Agents configuring with this command can add option82 to the DHCP request message, and let the server to process it. Before enabling this function, users should make sure that the DHCP service is enabled and the Relay Agent will transmit the udp broadcast messages whose destination port is 67.

Example: Enable the option82 function of the Relay Agent.

Switch(config)#service dhcp

Switch(config)# ip forward-protocol udp bootps

Switch(config)# ip dhcp relay information option

4.3 ip dhcp relay information option delimiter

Command: ip dhcp relay information option delimiter [colon | dot | slash | space]
no ip dhcp relay information option delimiter

Function: Set the delimiter of each parameter for suboption of option82 in global mode, **no** command restores the delimiter as slash.

Parameters: None.

Default Settings: slash ("/").

Command Mode: Global mode

Usage Guide: Divide the parameters with the configured delimiters after users have defined them which are used to create suboption (remot-de, circuit-id) of option82 in global mode.

Example: Set the parameter delimiters as dot (".") for suboption of option82.

Switch(config)#ip dhcp relay information option delimiter dot

4.4 ip dhcp relay information option remote-id

Command: ip dhcp relay information option remote-id {standard | *<remote-id>*}
no ip dhcp relay information option remote-id

Function: Set the suboption2 (remote ID option) content of option 82 added by DHCP request packets (They are received by the interface). The **no** command sets the additive suboption2 (remote ID option) format of option 82 as standard.

Parameters: standard means the default VLAN MAC format. ***<remote-id>*** means the remote-id content of option 82 specified by users, its length cannot exceed 64 characters.

Command Mode: Global Mode

Default: Use standard format to set remote-id of option 82.

Usage Guide: The additive option 82 information needs to associate with third-party DHCP server, it is used to specify the remote-id content by users when the standard remote-id format cannot satisfy server's request.

Example: Set the suboption remote-id of DHCP option82 as street-1-1.

Switch(config)#ip dhcp relay information option remote-id street-1-1

4.5 ip dhcp relay information option remote-id format

Command: ip dhcp relay information option remote-id format {default | vs-hp}

Function: Set remote-id format of Relay Agent option82.

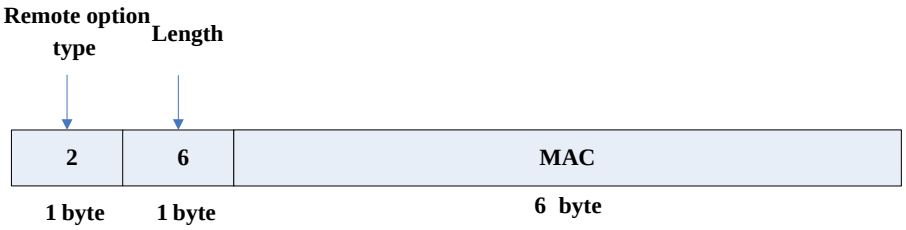
Parameters: default means that remote-id is the VLAN MAC address with hexadecimal

format, vs-hp means that remote-id is compatible with the remote-id format of HP manufacturer.

Default: default.

Command Mode: Global mode

Usage Guide: The default remote-id format defined as below:



MAC means VLAN MAC address.

The compatible remote-id format with HP manufacturer defined as below:

IP means the primary IP address of layer 3 interface where DHCP packets from.

Example: Set remote-id of Relay Agent option82 as the compatible format with HP manufacturer.

Switch(config)#ip dhcp relay information option remote-id format vs-hp

4.6 ip dhcp relay information option self-defined remote-id

Command: ip dhcp relay information option self-defined remote-id {hostname | mac | string WORD}

no ip dhcp relay information option self-defined remote-id

Function: Set creation method for option82, users can define the parameters of remote-id suboption by themselves.

Parameters: WORD the defined character string of remote-id by themselves, the maximum length is 64.

Command Mode: Global Mode

Default: Using standard method.

Usage Guide: After configure this command, if users do not configure remote-id on interface, it will create remote-id suboption for option82 according to self-defined method. For mac, use the format such as 00-02-d1-2e-3a-0d if it is filled to packets with ascii

format, but hex format occupies 6 bytes. Each option will be filled to packets according to the configured order of the commands and divide them with delimiter (delimiter is **ip dhcp relay information option delimiter** configuration).

Example: Set self-defined method and character string of remote-id suboption are hostname and abc respectively for option82.

Switch(config)#ip dhcp relay information option self-defined remote-id hostname string abc

4.7 ip dhcp relay information option self-defined remote-id format

Command: ip dhcp relay information option self-defined remote-id format [ascii | hex]

Function: Set self-defined format of remote-id for relay option82.

Parameters: None.

Command Mode: Global Mode

Default: ascii.

Usage Guide: self-defined format use ip dhcp relay information option type self-defined remote-id to create remote-id format.

Example: Set self-defined method of remote-id as hex for relay option82.

Switch(config)# ip dhcp relay information option self-defined remote-id format hex

4.8 ip dhcp relay information option self-defined subscriber-id

Command: ip dhcp relay information option self-defined subscriber-id {vlan | port | id (switch-id (mac | hostname)| remote-mac)| string WORD }

no ip dhcp relay information option self-defined subscriber-id

Function: Set creation method for option82, users can define the parameters of circute-id suboption by themselves.

Parameters: WORD the defined character string of circuit-id by themselves, the maximum length is 64.

Command Mode: Global Mode

Default: Using standard method.

Usage Guide: After configure this command, if users do not configure circuit-id on interface, it will create circuit-id suboption for option82 according to self-defined method.

Self-defined format of circuit-id: if self-defined format is ascii, the filled format of vlan such as “Vlan2”, the format of port such as “Ethernet1/0/1”, the format of mac and remote-mac such as “00-02-d1-2e-3a-0d”. If self-defined format is hex, the filled format of vlan occupies 2 bytes, port occupies 4 bytes, a byte means slot (for chassis switch, it means slot ID, for box switch, it is 1), a byte means Module (the default is 0), two bytes means port ID beginning from 1, mac and remote-mac occupy 6 bytes. Each option will be filled to packets according to the configured order of the commands and divide them with delimiter (delimiter is **ip dhcp relay information option delimiter** configuration).

Example: Set self-defined method of circuit-id suboption as port, mac for option82.

Switch(config)# ip dhcp relay information option self-defined subscriber-id port id switch-id mac

4.9 ip dhcp relay information option self-defined subscriber-id format

Command: ip dhcp relay information option self-defined subscriber-id format [ascii | hex]

Function: Set self-defined format of circuit-id for relay option82.

Parameters: None.

Command Mode: Global Mode

Default: ascii.

Usage Guide: self-defined format use ip dhcp relay information option type self-defined subscriber-id to create circuit-id format.

Example: Set self-defined format of circuit-id as hex for relay option82.

Switch(config)# ip dhcp relay information option self-defined subscriber-id format hex

4.10 ip dhcp relay information option subscriber-id

Command: ip dhcp relay information option subscriber-id {standard | <*circuit-id*>}

no ip dhcp relay information option subscriber-id

Function: This command is used to set the format of option82 sub-option1(Circuit ID option) added to the DHCP request messages from interface, **standard** means the standard vlan name and physical port name format, like”Vlan2+Ethernet1/0/12”,***<circuit-id>*** is the circuit-id contents of option82 specified by users, which is a string no longer than 64 characters. The” **no ip dhcp relay information option subscriber-id**” command will set the format of added option82 sub-option1 (Circuit ID option) as standard format.

Parameters: None

Command Mode: Interface configuration mode.

Default Settings: The system uses the standard format to set the circuit-id of option 82 by default.

User Guide: Because the option 82 information added for the switch should cooperate with the third party DHCP server, if the standard circuit-id format of the switch cannot satisfy the server's request, this method will be provided for users to specify the contents of circuit-id according to the situation of the server.

Example: Set the sub-option circuit-id of DHCP option82 as foobar.

Switch(config-if-vlan1)#ip dhcp relay information option subscriber-id foobar

4.11 ip dhcp relay information option subscriber-id format

Command: ip dhcp relay information option subscriber-id format {hex | acsii | vs-hp}

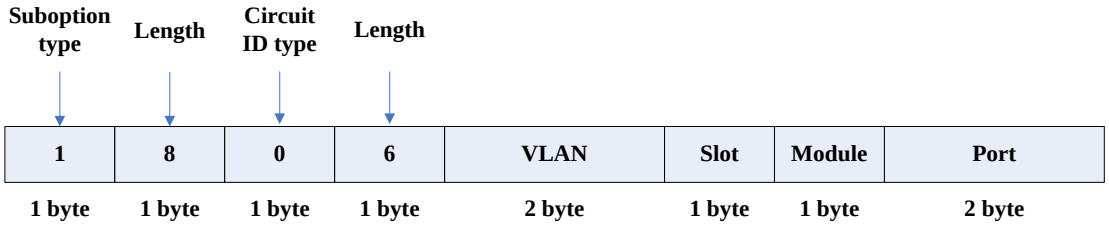
Function: Set subscriber-id format of Relay Agent option82.

Parameters: hex means that subscriber-id is VLAN and port information with hexadecimal format, acsii means that subscriber-id is VLAN and port information with ACSII format. vs-hp means that subscriber-id is compatible with the format of HP manufacturer.

Command Mode: Global mode

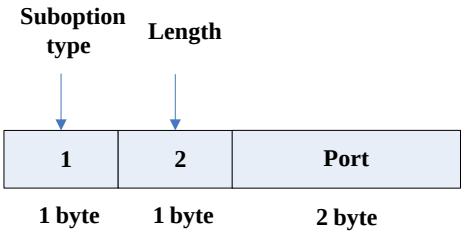
Default: ascii.

User Guide: VLAN and port information with ASCII format, such as "Vlan1+Ethernet1/0/11", VLAN and port information with hexadecimal format defined as below:



VLAN field fills in VLAN ID. For chassis switch, Slot means slot number, for box switch, Slot is 1; default Module is 0; Port means port number which begins from 1.

The compatible subscriber-id format with HP manufacturer defined as below:



Port means port number which begins from 1.

Example: Set subscriber-id format of Relay Agent option82 as hexadecimal format.

Switch(config)#ip dhcp relay information option subscriber-id format hex

4.12 ip dhcp relay information policy

Command: ip dhcp relay information policy {drop | keep | replace}

no ip dhcp relay information policy

Function: This command is used to set the retransmitting policy of the system for the received DHCP request message which contains option82. The drop mode means that if the message has option82, then the system will drop it without processing; keep mode means that the system will keep the original option82 segment in the message, and forward it to the server to process; replace mode means that the system will replace the option 82 segment in the existing message with its own option 82, and forward the message to the server to process. The **"no ip dhcp relay information policy**" will set the retransmitting policy of the option 82 DCHP message as "replace".

Parameters: None

Command Mode: Interface configuration mode.

Default Settings: The system uses replace mode to replace the option 82 segment in the existing message with its own option 82.

User Guide: Since the DHCP client messages might go through several DHCP Relay Agents when passed to the DHCP server, the latter Relay Agents on the path should set policies to decide how to process the option82 added by Relay Agents before them. The selection of option 82 retransmitting policies should take the configuration policy of the DHCP server into account.

Example: Set the retransmitting policy of DHCP messages option 82 as keep.

Switch(Config-if-Vlan1)# ip dhcp relay information policy keep

4.13 ip dhcp server relay information enable

Command: ip dhcp server relay information enable

no ip dhcp server relay information enable

Function: This command is used to enable the switch DHCP server to identify option82. The "**no ip dhcp server relay information enable**" command will make the server ignore the option 82.

Parameters: None

Command Mode: Global configuration mode

Default Setting: The system disable the option82 identifying function by default.

User Guide: If the users want the switch DHCP server to identify option82 and return option 82 information in the reply message, this command needs to be set, or, the switch DHCP server will ignore the option82.

Example: Set the DHCP server to support option82

Switch(Config-if-Vlan1)# ip dhcp server relay information enable

4.14 show ip dhcp relay information option

Command: show ip dhcp relay information option

Function: This command will display the state information of the DHCP option 82 in the system, including option82 enabling switch, the interface retransmitting policy, the circuit ID mode and the switch DHCP server option82 enabling switch.

Parameters: None.

Command Mode: Admin and Global Configuration Mode.

User Guide: Use this command to check the state information of Relay Agent option82 during operation.

Example:

Switch#show ip dhcp relay information option

ip dhcp server relay information option(i.e. option 82) is disabled

ip dhcp relay information option(i.e. option 82) is enabled

Vlan2:

ip dhcp relay information policy keep

ip dhcp relay information option subscriber-id standard

Vlan3:

ip dhcp relay information policy replace

ip dhcp relay information option subscriber-id foobar

Chapter 5 Commands for DHCP Snooping

5.1 debug ip dhcp snooping binding

Command: debug ip dhcp snooping binding

no debug ip dhcp snooping binding

Function: This command is use to enable the DHCP SNOOPING debug switch to debug the state of binding data of DHCP SNOOPING.

Command Mode: Admin mode

Usage Guide: This command is mainly used to debug the state of DHCP SNOOPING task when it adds ARP list entries, dot1x users and trusted user list entries according to binding data.

5.2 debug ip dhcp snooping event

Command: debug ip dhcp snooping event

no debug ip dhcp snooping event

Function: This command is use to enable the DHCP SNOOPING debug switch to debug the state of DHCP SNOOPING task.

Command Mode: Admin mode.

Usage Guide: This command is mainly used to debug the state of DHCP SNOOPING task and available of outputting the state of checking binding data and executing port action and so on.

5.3 debug ip dhcp snooping packet

Command: debug ip dhcp snooping packet

no debug ip dhcp snooping packet

Function: This command is used to enable the DHCP SNOOPING debug switch to debug the message-processing procedure of DHCP SNOOPING.

Command Mode: Admin Mode.

Usage Guide: The debug information that the DHCP SNOOPING is processing messages, including every step in the message-processing procedure: adding alarm information, adding binding information, transmitting DHCP messages, adding/peeling

option 82 and etc.

5.4 debug ip dhcp snooping packet interface

Command: debug ip dhcp snooping packet interface {[ethernet] <*InterfaceName*>}

no debug ip dhcp snooping packet {[ethernet] <*InterfaceName*>}

Function: This command is used to enable the DHCP SNOOPING debug switch to debug the information that DHCP SNOOPING is receiving a packet.

Parameters: <*InterfaceName*>: Interface name.

Command Mode: Admin Mode.

Usage Guide: The information that DHCP Snooping is receiving messages from a specific port.

5.5 debug ip dhcp snooping update

Command: debug ip dhcp snooping update

no debug ip dhcp snooping update

Function: This command is use to enable the DHCP snooping debug switch to debug the communication information between DHCP snooping and helper server.

Command Mode: Admin Mode.

Usage Guide: Debug the information of communication messages received and sent by DHCP snooping and helper server.

5.6 enable trustview key

Command: enable trustview key {0 | 7} <*password*>

no enable trustview key

Function: To configure DES encrypted key for private packets, this command is also the switch for the private packets encrypt and hash function enabled or not.

Parameter: <*password*> is character string length less than 16, which use as encrypted key. 0 for un-encrypted text for the password, while 7 for encrypted.

Command Mode: Global Mode.

Default: Disabled.

Usage Guide: The switch communicates with the TrustView management system through private protocols. By default these packets are not encrypted. In order to prevent spoofing, it can be configured to encrypt these packets. And at the same time, the same password should be configured on TrustView server.

Example: Enable encrypt or hash function of private message.

Switch(config)# enable trustview key 0 digitalchina

5.7 ip dhcp snooping

Command: ip dhcp snooping enable

no ip dhcp snooping enable

Function: Enable the DHCP Snooping function.

Parameters: None.

Command Mode: Globe mode.

Default: DHCP Snooping is disabled by default.

Usage Guide: When this function is enabled, it will monitor all the DHCP Server packets of non-trusted ports.

Example: Enable the DHCP Snooping function.

switch(config)#ip dhcp snooping enable

5.8 ip dhcp snooping action

Command: ip dhcp snooping action {shutdown | blackhole} [recovery <*second*>]

no ip dhcp snooping action

Function: Set or delete the automatic defense action of a port.

Parameters:shutdown: When the port detects a fake DHCP Server, it will be shutdown.

blackhole: When the port detects a fake DHCP Server, the vid and source MAC of the fake packet will be used to block the traffic from this MAC.

recovery: Users can set to recover after the automatic defense action being executed.(no shut ports or delete correponding blackhole）.

second: Users can set how long after the execution of defense action to recover. The unit is second, and valid range is 10-3600.

Command Mode: Port mode

Default: No default defense action.

Usage Guide: Only when DHCP Snooping is globally enabled, can this command be set. Trusted port will not detect fake DHCP Server, so, will never trigger the corresponding defense action. When a port turns into a trusted port from a non-trusted port, the original defense action of the port will be automatically deleted.

Example: Set the DHCP Snooping defense action of port ethernet1/0/1 as setting blackhole, and the recovery time is 30 seconds.

switch(config)#interface ethernet 1/0/1

switch(Config-Ethernet1/0/1)#ip dhcp snooping action blackhole recovery 30

5.9 ip dhcp snooping action MaxNum

Command: ip dhcp snooping action {<*maxNum*>|default}

Function: Set the number of defense action that can be simultaneously took effect.

Parameters: <*maxNum*>: the number of defense action on each port, the range of which is 1-200, and the value of which is 10 by default.

default: recover to the default value.

Command Mode: Globe mode

Default: The default value is 10.

Usage Guide: Set the max number of defense actions to avoid the resource exhaustion of the switch caused by attacks. If the number of alarm information is larger than the set value, then the earliest defense action will be recovered forcibly in order to send new defense actions.

Example: Set the number of port defense actions as 100.

switch(config)#ip dhcp snooping action 100

5.10 ip dhcp snooping binding

Command: ip dhcp snooping binding enable

no ip dhcp snooping binding enable

Function: Enable the DHCP Snooping binding funciton

Parameters: None.

Command Mode: Globe mode

Default Settings: DHCP Snooping binding is disabled by default.

Usage Guide: When the function is enabled, it will record the binding information allocated by DHCP Server of all trusted ports. Only after the DHCP SNOOPING function is enabled, the binding function can be enabled.

Example: Enable the DHCP Snooping binding funciton.

switch(config)#ip dhcp snooping binding enable

Relative Command: ip dhcp snooping enable

5.11 ip dhcp snooping binding arp

Command: ip dhcp snooping binding arp

no ip dhcp snooping binding arp

Function: Enable the DHCP Snooping binding ARP funciton.

Parameters: None

Command Mode: Globe mode

Default: DHCP Snooping binding ARP funciton is disabled by default.

Usage Guide: When this function is enbaled, DHCP SNOOPING will add binding ARP list entries according to binding information. Only after the binding function is enabled, can the binding ARP function be enabled. Binding ARP list entries are static entries without configuration of reservation, and will be added to the NEIGHBOUR list directly. The priority of binding ARP list entries is lower than the static ARP list entries set by administrator, so can be overwritten by static ARP list entries; but, when static ARP list entries are deleted, the binding ARP list entries can not be recovered untill the DHCP SNOOPING recapture the biding inforamtion. Adding binding ARP list entries is used to prevent these list entried from being attacked by ARP cheating. At the same time, these static list entries need no reauthenticaiton, which can prenvent the switch from the failing to reauthenticate ARP when it is being attacked by ARP scanning.

Only after the DHCP SNOOPING binding function is enabled, the binding ARP function can be set.

Example: Enable the DHCP Snooping binding ARP funciton.

switch(config)#ip dhcp snooping binding arp

Relative Command: ip dhcp snooping binding enable

5.12 ip dhcp snooping binding dot1x

Command: ip dhcp snooping binding dot1x

no ip dhcp snooping binding dot1x

Function: Enable the DHCP Snooping binding DOT1X funciton.

Parameters: None

Command Mode: Port mode

Default: By default, the binding DOT1X funciton is disabled on all ports.

Usage Guide: When this function is enabled, DHCP SNOOPING will notify the DOT1X module about the captured bindng information as a DOT1X controlled user. This command is mutually exclusive to”ip dhcp snooping binding user-contro“command.

Only after the DHCP SNOOPING binding function is enabled, the binding dot1x function can be set.

Example: Enable the binding DOT1X funciton on port ethernet1/0/1.

switch(config)#interface ethernet 1/0/1

switch(Config-Ethernet 1/0/1)# ip dhcp snooping binding dot1x

Relative Command: ip dhcp snooping binding enable

ip dhcp snooping binding user-control

5.13 ip dhcp snooping binding user

Command: ip dhcp snooping binding user <*mac*> address <*ipaddress*> vlan **<*vid*> interface [Ethernet] <*ifname*>**

no ip dhcp snooping binding user <*mac*> interface [Ethernet] <*ifname*>

Function: Configure the information of static binding users.

Parameters:

<*mac*>: The MAC address of the static binding user, whic is the only index of the binding user.

<*ipaddress*>: The IP address of the static binding user.

<vid>: The VLAN ID which the static binding user belongs to.

<*ifname*>: The access interface of static binding user.

Command Mode: Globe mode

Default: DHCP Snooping has no static binding list entry by default.

Usage Guide: The static binding users is deal in the same way as the dynamic binding users captured by DHCP SNOOPING; the follwoing actions are all allowed: notifying DOT1X to be a controlled user of DOT1X, adding a trusted user list entry directly, adding a bingding ARP list entry. The static binding uses will never be aged, and have a priority higher than dynamic binding users. Only after the DHCP SNOOPING binding function is enabled, the static binding users can be enabled.

Example: Configure static binding users.

switch(config)#ip dhcp snooping binding user 00-03-0f-12-34-56 address 192.168.1.16 interface Ethernet 1/0/16

Relative Command: ip dhcp snooping binding enable

5.14 ip dhcp snooping binding user-control

Command: ip dhcp snooping binding user-control

no ip dhcp snooping binding user-control

Function: Enable the binding user funtion.

Parameters: None.

Command Mode: Port Mode.

Default: By default, the binding user funciton is disabled on all ports.

Usage Guide: When this function is enabled, DHCP SNOOPING will treat the captured binding information as trusted users allowed to access all resources. This command is mutually exclusive to "**ip dhcp snooping binding dot1x**" command.

Only after DHCP SNOOPING binding function is enabled, the binding user function can be set. This command is not limited by "ip dhcp snooping" based on VLAN, but it is only limited by the global "**ip dhcp snooping enable**" command.

Example: Enable the binding USER funciton on port ethernet1/0/1.

switch(config)#interface ethernet 1/0/1

switch(Config-Ethernet 1/0/1)# ip dhcp snooping binding user-control

Relative Command: ip dhcp snooping binding enable

ip dhcp snooping binding dot1x

5.15 ip dhcp snooping binding user-control max-user

Command: ip dhcp snooping binding user-control max-user <*number*>

no ip dhcp snooping binding user-control max-user

Function: Set the max number of users allowed to access the port when enabling DHCP Snooping binding user funciton; the **no** operation of this command will restore default value.

Parameters: <*number*> the max number of users allowed to access the port, from 0 to 1024.

Command Mode: Port Configuration Mode.

Default: The max number of users allowed by each port to access is 1024.

Usage Guide: This command defines the max number of trust users distributed according to binding information, with **ip dhcp snooping binding user-contrl** enabled on the port. By default, the number is 1024. Considering the limited hardware resources of the switch, the actual number of trust users distributed depends on the resource amount. If a bigger max number of users is set using this command, DHCP Snooping will distribute the binding informaiton of untrust users to hardware to be trust users as long as there is enough available resources. Otherwise, DHCP Snooping will change the distributed binging informaiton accordint to the new smaller max user number. When the number of distributed bingding informaiton entries reaches the max limit, no new DHCP will be able

to become trust user or to access other network resouces via the switch.

Examples: Enable DHCP Snooping binding user funtion on Port ethernet1/0/1, setting the max number of user allowed to access by Port Ethernet1/0/1 as 5.

Switch(Config-If-Ethernet1/0/1)# ip dhcp snooping binding user-control max-user 5

Related Command: ip dhcp snooping binding user-control

5.16 ip dhcp snooping information enable

Command: ip dhcp snooping information enable

no ip dhcp snooping information enable

Function: This command will enable option 82 function of DHCP Snooping on the switch, the **no** operation of this command will disable that function.

Parameters: None.

Default : Option 82 function is disabled in DHCP Snooping by default.

Command Mode: Global Configuration Mode.

Usage Guide: Only by implementing this command, can DHCP Snooping add standard option 82 to DHCP request messages and forward the message. The format of option1 in option 82 (Circuit ID option) is standard vlan name plus physical port name, like vlan1+ethernet1/0/12. That of option2 in option 82 (remote ID option) is CPU MAC of the switch, like 00030f023301. If a DHCP request message with option 82 options is received, DHCP Snooping will replace those options in the message with its own. If a DHCP reply message with option 82 options is received, DHCP Snooping will dump those options in the message and forward it.

Examples: Enable option 82 function of DHCP Snooping on the switch.

Switch(config)#ip dhcp snooping enable

Switch(config)# ip dhcp snooping binding enable

Switch(config)# ip dhcp snooping information enable

5.17 ip dhcp snooping information option allow-untrusted (replace|)

Command：ip dhcp snooping information option allow-untrusted (replace|)

no ip dhcp snooping information option allow-untrusted (replace|)

Function: This command is used to set that allow untrusted ports of DHCP snooping to receive DHCP packets with option82 option. When the "replace" is setting, the potion82 option is allowed to replace. When disabling this command, all untrusted ports will drop DHCP packets with option82 option.

Parameter: None.

Command Mode: Global Mode

Default: Drop DHCP packets with option82 option received by untrusted ports.

Usage Guide: Usually the switch with DHCP snooping function connects the terminal user directly, so close allow-untrusted by default to avoid option82 option added by user privately. Please set uplink port as trust port when enabling the uplink of DHCP snooping function.

Example: Enable the function that receives DHCP packets with option82.

Switch(config)#ip dhcp snooping information option allow-untrusted

5.18 ip dhcp snooping information option delimiter

Command: ip dhcp snooping information option delimiter [colon | dot | slash | space]

no ip dhcp snooping information option delimiter

Function: Set the delimiter of each parameter for suboption of option82 in global mode, **no** command restores the delimiter as slash.

Parameters: None.

Default: slash (“/”).

Command Mode: Global mode

Usage Guide: Divide parameters with the configured delimiters after users have defined them which are used to create suboption (remote-id, circuit-id) of option82 in global mode.

Example: Set the parameter delimiters as dot (“.”) for suboption of option82.

Switch(config)# ip dhcp snooping information option delimiter dot

5.19 ip dhcp snooping information option remote-id

Command: ip dhcp snooping information **option remote-id {standard | *<remote-id>*}**

no ip dhcp snooping information option remote-id

Function: Set the suboption2 (remote ID option) content of option 82 added by DHCP request packets (they are received by the port). The **no** command sets the additive suboption2 (remote ID option) format of option 82 as standard.

Parameters: standard means the default VLAN MAC format. ***<remote-id>*** means the remote-id content of option 82 specified by users, its length can not exceed 64 characters.

Command Mode: Global Mode

Default: Use standard format to set remote-id.

Usage Guide: The additive option 82 needs to associate with third-party DHCP server, it

is used to specify the remote-id content by users when the standard remote-id format can not satisfy server's request.

Example: Set the suboption remote-id of DHCP option82 as street-1-1.

Switch(config)#ip dhcp snooping information option remote-id street-1-1

5.20 ip dhcp snooping information option self-defined remote-id

Command: ip dhcp snooping information option self-defined remote-id {hostname | mac | string WORD}

no ip dhcp snooping information option self-defined remote-id

Function: Set creation method for option82, users can define the parameters of **remote-id** suboption by themselves.

Parameters: WORD the defined character string of remote-id by themselves, the maximum length is 64.

Command Mode: Global Mode

Default: Using standard method.

Usage Guide: After configure this command, if users do not configure ip dhcp snooping information option remote-id globally, it will create remote-id suboption for option82 according to self-defined method. For mac, use the format such as 00-02-d1-2e-3a-0d if it is filled to packets with ascii format, but hex format occpies 6 bytes. Each option will be filled to packets according to the configured order of the commands and divide them with delimiter (delimiter is **ip dhcp snooping information option delimiter** configuration).

Example: Set self-defined method and character string of remote-id suboption are mac and abc respectively for option82.

Switch(config)# ip dhcp snooping information option self-defined remote-id mac string abc

5.21 ip dhcp snooping information option self-defined remote-id format

Command: ip dhcp snooping information option self-defined remote-id format [ascii | hex]

Function: Set self-defined format of remote-id for snooping option82.

Parameters: None.

Command Mode: Global Mode

Default: ascii.

Usage Guide: self-defined format use ip dhcp snooping information option type self-defined remote-id to create remote-id format.

Example: Set self-defined format of remote-id as hex for snooping option82.

Switch(config)# ip dhcp snooping information option self-defined remote-id format hex

5.22 ip dhcp snooping information option self-defined subscriber-id

Command: ip dhcp snooping information option self-defined subscriber-id {vlan | port | id (switch-id (mac | hostname)| remote-mac) | string WORD}

no ip dhcp snooping information option type self-defined subscriber-id

Function: Set creation method for option82, users can define the parameters of circute-id suboption by themselves.

Parameters: WORD the defined character string of circuit-id by themselves, the maximum length is 64.

Command Mode: Global Mode

Default: Using standard method.

Usage Guide: After configure this command, if users do not configure circuit-id on port, it will create circuit-id suboption for option82 according to self-defined method. Self-defined format of circuit-id: if self-defined subscriber-id format is ascii, the filled format of vlan such as “Vlan2”, the format of port such as “Ethernet1/0/1”, the format of mac and remote-mac such as “00-02-d1-2e-3a-0d”. If self-defined format is hex, the filled format of vlan occupies 2 bytes, port occupies 4 bytes, a byte means slot (for chassis switch, it means slot ID, for box switch, it is 1), a byte means Module (the default is 0), two bytes means port ID beginning from 1, mac and remote-mac occupy 6 bytes. Each option will be filled to packets according to the configured order of the commands and divide them with delimiter (delimiter is **ip dhcp snooping information option delimiter** configuration).

Example: Set self-defined method of circuit-id suboption as vlan, port, mac and remote-mac for option82.

Switch(config)#ip dhcp snooping information option self-defined subscriber-id vlan port id remote-mac

5.23 ip dhcp snooping information option self-defined subscriber-id format

Command: ip dhcp snooping information option self-defined subscriber-id format

[ascii | hex]

Function: Set self-defined format of circuit-id for snooping option82.

Parameters: None.

Command Mode: Global Mode

Default: ascii.

Usage Guide: self-defined format uses ip dhcp snooping information option type self-defined subscriber-id to create circuit-id format.

Example: Set self-defined format of circuit-id as hex for snooping option82.

Switch(config)#ip dhcp snooping information option self-defined subscriber-id format hex

5.24 ip dhcp snooping information option subscriber-id

Command: ip dhcp snooping information option subscriber-id {standard | <*circuit-id*>}

no ip dhcp snooping information option subscriber-id

Function: Set the suboption1 (circuit ID option) content of option 82 added by DHCP request packets (they are received by the port). The **no** command sets the additive suboption1 (circuit ID option) format of option 82 as standard.

Parameters: standard means the standard format of VLAN name and physical port name, such as Vlan2+Ethernet1/0/12. ***<circuit-id>*** means the circuit-id content of option 82 specified by users, its length can not exceed 64 characters.

Command Mode: Port Mode

Default: Use standard format to set circuit-id.

Usage Guide: The additive option 82 needs to associate with third-party DHCP server, it is used to specify the circuit-id content by user when the standard circuit-id format can not satisfy server's request.

Example: Set the suboption circuit-id of DHCP option82 as P2.

Switch(config)#ip dhcp snooping information option subscriber-id P2

5.25 ip dhcp snooping information option subscriber-id format

Command: ip dhcp snooping information option subscriber-id format {hex | acsii | vs-hp}

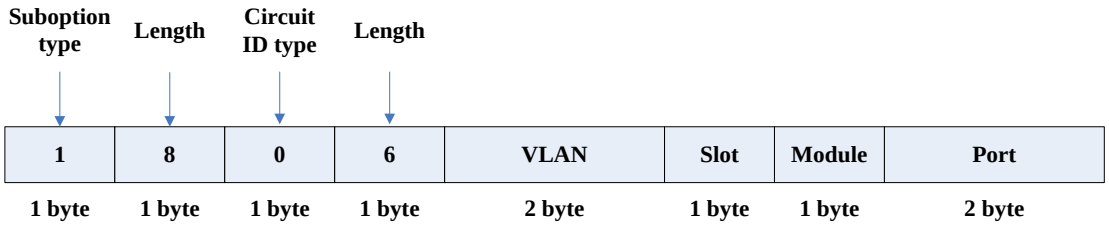
Function: This command is used to set subscriber-id format of DHCP snooping option82.

Parameters: hex means that subscriber-id is VLAN and port information with hexadecimal format, acsii means that subscriber-id is VLAN and port information with ACSII format. vs-hp means that subscriber-id is compatible with the format of HP manufacturer.

Command Mode: Global mode

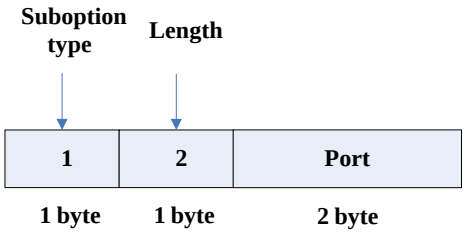
Default: **ascii.**

User Guide: VLAN and port information with ASCII format, such as Vlan1+Ethernet1/0/11, VLAN and port information with hexadecimal format defined as below:



VLAN field fill in VLAN ID. For chassis switch, Slot means slot number, for box switch, Slot is 1; default Module is 0; Port means port number which begins from 1.

The compatible subscriber-id format with HP manufacturer defined as below:



Port means port number which begins from 1.

Example: Set subscriber-id format of DHCP snooping option82 as hexadecimal format.

Switch(config)#ip dhcp snooping information option subscriber-id format hex

5.26 ip dhcp snooping trust

Command: ip dhcp snooping trust

no ip dhcp snooping trust

Function: Set or delete the DHCP Snooping trust attributes of a port.

Parameters: None

Command Mode: Port mode

Default: By default, all ports are non-trusted ports

Usage Guide: Only when DHCP Snooping is globally enabled, can this command be set. When a port turns into a trusted port from a non-trusted port, the original defense action of the port will be automatically deleted; all the security history records will be cleared

(except the information in system log).

Example: Set port ethernet1/0/1 as a DHCP Snooping trusted port

switch(config)#interface ethernet 1/0/1

switch(Config- Ethernet 1/0/1)#ip dhcp snooping trust

5.27 ip user helper-address

Command: ip user *helper-address* <svr_addr> [*port* <udp_port>] source <*src*_addr> [secondary]

no ip user helper-address [secondary]

Function: Set the address and port of HELPER SERVER.

Parameters:

<svr_addr>: The IP address of HELPER SERVER IP in dotted-decimal notation.

udp_port: The UDP port of HELPER SERVER, the range of which is1—65535, and its default value is 9119.

src_addr: The local management IP address of the switch, in dotted-decimal notation.

sencondary: Whether it is a secondary SERVER address.

Command Mode: Global mode

Default: There is no HELPER SERVER address by default.

Usage Guide: DHCP SNOOPING will send the monitored binding information to HELPER SERVER to save it. If the switch starts abnormally, it can recover the binding data from HELPER SERVER. The HELPER SERVER function usually is integrated into DCBI packet. The DHCP SNOOPING and HELPER SERVER use the UDP protocol to communicate, and guarantee the arrival of retransmitted data. HELPER SERVER configuration can also be used to sent DOT1X user data from the server, the detail of usage is described in the chapter of dot1x configuration.

Two HELPER SERVER addresses are allowed, DHCP SNOOPING will try to connect to PRIMARY SERVER in the first place. Only when the PRIMARY SERVER is unreachable, will the switch c HELPER SERVER connects to SECONDARY SERVER.

Please pay attention: source address is the effective management IP address of the switch, if the management IP address of the switch changes, this configuration should be updated in time.

Example: Set the local management IP address as 100.1.1.1, primary HELPER SERVER address as 100.1.1.100 and the port as default value.

switch(config)#interface vlan 1

switch(Config- If-Vlan1)#ip address 100.1.1.1 255.255.255.0

switch(Config-if-Vlan1)exit

switch(config)#ip user helper-address 100.1.1.100 source 100.1.1.1

5.28 ip user private packet version two

Command: ip user private packet version two

no ip user private packet version two

Function: The switch choose private packet version two to communicate with trustview.

Parameter: None.

Command Mode: Global Mode.

Default: The switch choose private packet version one to communicate with DCBI.

Usage Guide: If the DCBI access control system is applied, the switch should be configured to use private protocol of version one to communicate with the DCBI server. However, if TrustView is applied, version two should be applied.

Example: To configure the switch choose private packet version two to communicate with inter security management background system.

switch(config)#ip user private packet version two

5.29 show ip dhcp snooping

Command: show ip dhcp snooping [interface [ethernet] <*interfaceName*>]

Function: Display the current cofiguration information of dhcp snooping or display the records of defense actions of a specific port.

Parameters: <*interfaceName*>: The name of the specific port.

Command Mode: Admin and Global Configuration Mode.

Default: None.

Usage Guide: If there is no specific port, then display the current cofiguration information of dhcp snooping, otherwise, display the records of defense actions of the specific port.

Example:

switch#show ip dhcp snooping
DHCP Snooping is enabled

DHCP Snooping binding arp: disabled
DHCP Snooping maxnum of action info:10
DHCP Snooping limit rate: 100(pps), switch ID: 0003.0F12.3456
DHCP Snooping droped packets: 0, discarded packets: 0
DHCP Snooping alarm count: 0, binding count: 0,
expired binding: 0, request binding: 0

```
interface          trust     action     recovery     alarm num   bind num
---------------- --------- --------- ---------- --------- ----------
Ethernet1/0/1      trust     none       0second      0           0
Ethernet1/0/2      untrust   none       0second      0           0
Ethernet1/0/3      untrust   none       0second      0           0
Ethernet1/0/4      untrust   none       0second      0           1
Ethernet1/0/5      untrust   none       0second      2           0
Ethernet1/0/6      untrust   none       0second      0           0
Ethernet1/0/7      untrust   none       0second      0           0
Ethernet1/0/8      untrust   none       0second      0           1
Ethernet1/0/9      untrust   none       0second      0           0
Ethernet1/0/10     untrust   none       0second      0           0
Ethernet1/0/11     untrust   none       0second      0           0
Ethernet1/0/12     untrust   none       0second      0           0
Ethernet1/0/13     untrust   none       0second      0           0
Ethernet1/0/14     untrust   none       0second      0           0
Ethernet1/0/15     untrust   none       0second      0           0
Ethernet1/0/16     untrust   none       0second      0           0
Ethernet1/0/17     untrust   none       0second      0           0
Ethernet1/0/18     untrust   none       0second      0           0
Ethernet1/0/19     untrust   none       0second      0           0
Ethernet1/0/20     untrust   none       0second      0           0
Ethernet1/0/21     untrust   none       0second      0           0
Ethernet1/0/22     untrust   none       0second      0           0
Ethernet1/0/23     untrust   none       0second      0           0
Ethernet1/0/24     untrust   none       0second      0           0
```

Displayed Information	Explanation
DHCP Snooping is enable	Whether the DHCP Snooping is globally enabled or disabled.
DHCP Snooping binding arp	Whether the ARP binding function is enabled.
DHCP Snooping maxnum of action info	The number limitation of port defense actions
DHCP Snooping limit rate	The rate limitation of receiving packets
switch ID	The switch ID is used to identify the switch, usually using the CPU MAC address.
DHCP Snooping droped packets	The number of dropped messages when the

	received DHCP messages exceeds the rate limit.
discarded packets	The number of discarded packets caused by the communication failure within the system. If the CPU of the switch is too busy to schedule the DHCP SNOOPING task and thus can not handle the received DHCP messages, such situation might happen.
DHCP Snooping alarm count:	The number of alarm information.
binding count	The number of binding information.
expired binding	The number of binding information which is already expired but has not been deleted. The reason why the expired information is not deleted immediately might be that the switch needs to notify the helper server about the information, but the helper server has not acknowledged it.
request binding	The number of REQUEST information
interface	The name of port
trust	The truest attributes of the port
action	The automatic defense action of the port
recovery	The automatic recovery time of the port
alarm num	The number of history records of the port automatic defense actions
bind num	The number of port-relative binding information.

switch#show ip dhcp snooping int Ethernet1/0/1
interface Ethernet1/0/1 user config:
trust attribute: untrust
action: none
binding dot1x: disabled
binding user: disabled
recovery interval:0(s)
Alarm info: 0

Binding info: 0

Expired Binding: 0

Request Binding: 0

Displayed Information	Explanation
interface	The name of port
trust attribute	The truest attributes of the port
action	The automatic defense action of the port
recovery interval	The automatic recovery time of the port
maxnum of alarm info	The max number of automatic defense actions that can be recorded by the port
binding dot1x	Whether the binding dot1x function is enabled on the port
binding user	Whether the binding user function is enabled on the port.
Alarm info	The number of alarm information.
Binding info	The number of binding information.
Expired Binding	The expired binding information
Request Binding	REQUEST information

5.30 show ip dhcp snooping binding all

Command: show ip dhcp snooping binding all

Function: Display the current global binding information of DHCP snooping.

Parameters: None.

Command Mode: Admin and Global Configuration Mode.

Default: None.

Usage Guide: This command can check the global binding information of DHCP snooping, each table entry includes the corresponding MAC address, IP address, port name, VLAN ID and the flag of the binding state. Besides, DHCP Snooping must be enabled globally, this command can be configured.

Example:

switch#show ip dhcp snooping binding all

ip dhcp snooping static binding count:1169, dynamic binding count:0

MAC IP address Interface Vlan ID Flag

00-00-00-00-11-11 192.168.40.1 Ethernet1/0/1 1 S

00-00-00-00-00-10	192.168.40.10	Ethernet1/0/2	1	D
00-00-00-00-00-11	192.168.40.11	Ethernet1/0/4	1	D
00-00-00-00-00-12	192.168.40.12	Ethernet1/0/4	1	D
00-00-00-00-00-13	192.168.40.13	Ethernet1/0/4	1	SU
00-00-00-00-00-14	192.168.40.14	Ethernet1/0/4	1	SU
00-00-00-00-00-15	192.168.40.15	Ethernet1/0/5	1	SL
00-00-00-00-00-16	192.168.40.16	Ethernet1/0/5	1	SL

The flag explanation of the binding state:

S The static binding is configured by shell command

D The dynamic binding type

U The binding is uploaded to the server

R The static binding is configured by the server

O DHCP response with the option82

L The hardware drive is announced by the binding

X Announcing dot1x module is successful

E Announcing dot1x module is failing

5.31 show trustview status

Command: show trustview status

Function: To show all kinds of private packets state information, which sending or receiving from TrustView (inter security management background system).

Parameter: None.

Command Mode: Admin and Global Configuration Mode.

Default: None.

Usage Guide: This command can be used for debugging the communication messages between the switch and the TrustView server, messages such as protocol version notification, encryption negotiation, free resource and web URL redirection, and the number of forced log-off messages, as well as the number of forced accounting update messages, can be displayed.

Example:

Switch#show trustview status

Primary TrustView Server 200.101.0.9:9119

TrustView version2 message inform successed

TrustView inform free resource successed

TrustView inform web redirect address successed

TrustView inform user binding data successed

TrustView version2 message encrypt/digest enabled

Key: 08:02:33:34:35:36:37:38

Rcvd 106 encrypted messages, in which MD5-error 0 messages, DES-error 0 messages

Sent 106 encrypted messages

Free resource is 200.101.0.9/255.255.255.255

Web redirect address for unauthencated users is <http://200.101.0.9:8080>

Rcvd 0 force log-off packets

Rcvd 19 force accounting update packets

Using version two private packet

Chapter 6 Commands for DHCPv6 Snooping

6.1 clear ipv6 dhcp snooping binding

Command: clear ipv6 dhcp snooping binding {<*MAC*> | <*ipv6 address*> | interface {ethernet <*IFNAME*> | port-channel <*IFNAME*> | <*IFNAME*>} | all}

Function: Clear DHCPv6 Snooping binding.

Parameter: MAC: Delete the binding of the specific MAC address

ipv6 address: Delete the binding of the specific IPv6 address

IFNAME: The port name

all: Delete all binding of DHCPv6 Snooping

Command Mode: Admin mode

Default: None

Usage Guide: Delete the (one port or all ports) dynamic DHCPv6 Snooping binding information.

Example: Clear all dynamic binding of DHCPv6 Snooping.

switch#clear ipv6 dhcp snooping binding all

6.2 debug ipv6 dhcp snooping binding

Command: debug ipv6 dhcp snooping binding

Function: Debug the binding information of DHCPv6 Snooping.

Parameter: None

Command Mode: Admin mode

Default: None

Usage Guide: Display the binding processing information of DHCPv6 Snooping, include: create/delete the binding.

Example: Enable the command which debug the binding information of DHCPv6 Snooping.

switch# debug ipv6 dhcp snooping binding

%Jan 16 02:25:14 2006 DHCP6SNP BINDING: Do binding info from client 00-19-e0-3f-d1-83,

interface Ethernet1/0/11, type 1, transaction-ID 3873

%Jan 16 02:25:14 2006 DHCP6SNP BINDING: Create new binding.

%Jan 16 02:25:14 2006 DHCP6SNP BINDING: Do binding info from client 00-00-00-11-22-33,
interface Ethernet1/0/2, type 2, transaction-ID 3873
%Jan 16 02:25:14 2006 DHCP6SNP BINDING: release binding :: MAC 00-19-e0-3f-d1-83 on default Ethernet1/0/11
%Jan 16 02:25:16 2006 DHCP6SNP BINDING: Do binding info from client 00-19-e0-3f-d1-83,
interface Ethernet1/0/11, type 3, transaction-ID 30305
%Jan 16 02:25:16 2006 DHCP6SNP BINDING: Create new binding.
%Jan 16 02:25:16 2006 DHCP6SNP BINDING: Do binding info from client 00-00-00-11-22-33,
interface Ethernet1/0/2, type 7, transaction-ID 30305

6.3 debug ipv6 dhcp snooping event

Command: debug ipv6 dhcp snooping event
Function: Debug the event information of DHCPv6 Snooping.
Parameter: None
Command Mode: Admin mode
Default: None
Usage Guide: Enable this command to show the processing information of the events for DHCPv6 Snooping, the event include sending/deleting the security policy events, such as: black hole MAC, port shutdown/no shutdown, and the error prompt, etc.
Example: Enable debug of events information for DHCPv6 Snooping.
switch# debug ipv6 dhcp snooping event
%Jan 16 02:25:14 2006 DHCP6SNP EVENT: add blackhole 00-19-e0-3f-d1-83 on interface Ethernet1/0/13
%Jan 16 02:35:15 2006 DHCP6SNP EVENT: delete blackhole 00-19-e0-3f-d1-83 on interface Ethernet1/0/13

6.4 debug ipv6 dhcp snooping packet

Command: debug ipv6 dhcp snooping packet
Function: Debug the packet information of DHCPv6 Snooping.
Parameter: None
Command Mode: Admin mode
Default: None

Usage Guide: The processing information of DHCPv6 Snooping packets include the type of the receiving packets, the source MAC and the destination MAC of the packets, client DUID, IA address, preferred lifetime, valid lifetime, and packets drop, etc.

Example: Enable debug of the packet information for DHCPv6 Snooping.

switch# debug ipv6 dhcp snooping packet

%Jan 16 02:18:01 2006 DHCP6SNP EVENT: Parse packet SOLICIT from fe80::219:e0ff:fe3f:d183

src MAC 00-19-e0-3f-d1-83 interface Ethernet1/0/11 vlan 1

%Jan 16 02:18:01 2006 DHCP6SNP PACKET: Receive DHCPv6 packet SOLICIT from fe80::219:e0ff:fe3f:d183

src MAC 00-19-e0-3f-d1-83, dst MAC 33-33-00-01-00-02,

interface Ethernet1/0/11 vlan 1,

transaction-ID 2469, smac host flag 0, dmac host flag 0

%Jan 16 02:18:01 2006 DHCP6SNP PACKET: Forward packet SOLICIT (protocol 0x819)

%Jan 16 02:18:01 2006 DHCP6SNP PACKET: to vlan 1 except port Ethernet1/0/11 (designPort flag 0)

%Jan 16 02:18:01 2006 DHCP6SNP PACKET: and return packet to network stack

%Jan 16 02:18:01 2006 DHCP6SNP EVENT: Parse packet ADVERTISE from fe80::200:ff:fe11:2233

src MAC 00-00-00-11-22-33 interface Ethernet1/0/2 vlan 1

%Jan 16 02:18:01 2006 DHCP6SNP PACKET: Receive DHCPv6 packet ADVERTISE from fe80::200:ff:fe11:2233

src MAC 00-00-00-11-22-33, dst MAC 00-19-e0-3f-d1-83,

interface Ethernet1/0/2 vlan 1,

transaction-ID 2469, smac host flag 1, dmac host flag 0

%Jan 16 02:18:01 2006 DHCP6SNP PACKET: Forward packet ADVERTISE (protocol 0x819)

%Jan 16 02:18:01 2006 DHCP6SNP PACKET: to exact port Ethernet1/0/11 (designPort flag 1)

%Jan 16 02:18:03 2006 DHCP6SNP EVENT: Parse packet REQUEST from fe80::219:e0ff:fe3f:d183

src MAC 00-19-e0-3f-d1-83 interface Ethernet1/0/11 vlan 1

%Jan 16 02:18:03 2006 DHCP6SNP PACKET: Receive DHCPv6 packet REQUEST from fe80::219:e0ff:fe3f:d183

src MAC 00-19-e0-3f-d1-83, dst MAC 33-33-00-01-00-02,

interface Ethernet1/0/11 vlan 1,

transaction-ID 16424, smac host flag 0, dmac host flag 0

%Jan 16 02:18:03 2006 DHCP6SNP PACKET: Forward packet REQUEST (protocol

0x819)

%Jan 16 02:18:03 2006 DHCP6SNP PACKET: to vlan 1 except port Ethernet1/0/11 (designPort flag 0)

%Jan 16 02:18:03 2006 DHCP6SNP PACKET: and return packet to network stack

%Jan 16 02:18:03 2006 DHCP6SNP EVENT: Parse packet REPLY from fe80::200:ff:fe11:2233

src MAC 00-00-00-11-22-33 interface Ethernet1/0/2 vlan 1

%Jan 16 02:18:03 2006 DHCP6SNP PACKET: Receive DHCPv6 packet REPLY from fe80::200:ff:fe11:2233

src MAC 00-00-00-11-22-33, dst MAC 00-19-e0-3f-d1-83,

interface Ethernet1/0/2 vlan 1,

transaction-ID 16424, smac host flag 1, dmac host flag 0

%Jan 16 02:18:03 2006 DHCP6SNP PACKET: Forward packet REPLY (protocol 0x819)

%Jan 16 02:18:03 2006 DHCP6SNP PACKET: to exact port Ethernet1/0/11 (designPort flag 1)

6.5 ipv6 dhcp snooping action

Command: ipv6 dhcp snooping action {shutdown | blackhole} [recovery <*second*>]

no ipv6 dhcp snooping action

Function: After the abnormity is detected by DHCPv6 Snooping, set the action and the duration on the port, the no command cancels the configuration.

Parameters: shutdown | blackhole: After DHCPv6 Snooping receives the response packet of DHCPv6 from non-trusted port, then execute the action.

second: The duration between the action execution and recovery , ranging from 1-3600, and the default action is not recovered.

Command Mode: Port mode

Default: There is no user-defined action, the default action is not recovered and has no recovery time.

Usage Guide: Set the user-defined action for non-trusted port, when the security policy is changed, clear the security policy sent to the hardware at the same time.

Example: Set the user-defined action for non-trusted port.

switch(config-if-ethernet1/0/1)# ipv6 dhcp snooping action shutdown recovery 100

6.6 ipv6 dhcp snooping action MaxNum

Command: ipv6 dhcp snooping action {<*max-num*> | default}

Function: After the abnormity is detected by DHCPv6 Snooping, set the max number of blackhole MAC on each non-trusted port.

Parameters: max-num: The max number of blackhole MAC that can be sent after DHCPv6 Snooping receives the response packet of DHCPv6 from non-trusted port, the range from 1 to 200.

Default: The limitation number is 10 by default.

Command Mode: Global mode

Default: Limit blackhole MAC as 10 by the default port.

Usage Guide: Set the max number of the blackhole MAC to avoid the resource exhaustion of the switch caused by attacks. If the number of alarm information is bigger than the setting value, then the earliest blackhole MAC will be recovered forcibly while the new blackhole MAC take effect.

Example: After the abnormity is detected by DHCPv6 Snooping, set the max number of blackhole MAC as 100 on each non-trusted port.

switch(config)# ipv6 dhcp snooping action 100

6.7 ipv6 dhcp snooping binding enable

Command: ipv6 dhcp snooping binding enable

no ipv6 dhcp snooping binding enable

Function: Enable the DHCPv6 Snooping binding funciton globally. The **no** command disables the function.

Parameters: None.

Command Mode: Globe mode

Default: DHCPv6 Snooping binding is disabled by default.

Usage Guide: When enabling the binding function of DHCPv6 Snooping to monitor the DHCPv6 packets, it allows DHCPv6 Snooping binding to be established. This command limits the dynamic binding and the static binding. After disable the global DHCPv6 Snooping function, the device stops establishing the binding according to DHCPv6 packets.

Example: Establish DHCPv6 Snooping binding according to DHCPv6 REPLY packets.

switch(config)#ipv6 dhcp snooping binding enable

6.8 ipv6 dhcp snooping binding nd

Command: ipv6 dhcp snooping binding nd

no ipv6 dhcp snooping binding nd

Function: Globally enable the function that DHCPv6 Snooping binds ND. The **no** command disables the function.

Parameters: None.

Command Mode: Globe mode

Default: Disable the function that DHCPv6 Snooping binds ND.

Usage Guide: After this function is enabled globally, send static ND while setting up DHCPv6 Snooping binding, and convert the already existent DHCPv6 Snooping binding into the static ND entry. After disable the global DHCPv6 Snooping function, the static ND entries will not be set according to DHCPv6 Snooping binding, and all the corresponding static ND entries set by DHCP Snooping binding will be deleted.

Example: Send the static ND entries according to DHCPv6 Snooping binding.

switch(config)#ipv6 dhcp snooping binding nd

6.9 ipv6 dhcp snooping binding user

Command: ipv6 dhcp snooping binding user <*MAC-address*> address <*ipv6-address*> vlan <*vid*> interface [ethernet | port-channel] <*ifname*>

no ipv6 dhcp snooping binding user <*MAC-address*>

Function: Users set the static binding entries. The no command deletes the list entry.

Parameters: MAC-address: The MAC address

vid: VLAN ID, the range from 1 to 4094

ipv6-address: The IPv6 address

ifname: The access interface of the static binding user.

Command Mode: Globe mode

Default: There is no static list entry.

Usage Guide: Add the static list entry to the binding table. For DHCPv6 Snooping binding data, MAC address and IPv6 address must ensure that have no conflict. The static binding data can cover the dynamic binding data and can not be covered by the dynamic binding data.

Port name can the name of a Port-Channel or a Ethernet port, allows the inexistent Port-Channel specified, but it must authenticate the validity of Port-Channel name and cannot configure the Ethernet port which is not existent.

In addition, check the validity of MAC and Ipv6 address. MAC must configures the unicast MAC, IPv6 address can not be link local address, loopback address, :: address and multicast address. If the port name exist,,it is still necessary to check whether this port in the vid specified VLAN .

After enable DHCPv6 Snooping and DHCPv6 Snooping binding, the static binding command is able to set.

Example: Set up the static binding of DHCPv6 Snooping.

switch(config)#ipv6 dhcp snooping binding user mac 00-03-0F-01-02-03 address 2010::10 vlan 10 interface ethernet 1/0/13

6.10 ipv6 dhcp snooping binding user-control

Command: ipv6 dhcp snooping binding user-control

no ipv6 dhcp snooping binding user-control

Function: Enable the DHCPv6 Snooping binding user-access-control funtion. The **no** command disables the function.

Parameters: None.

Command Mode: port mode

Default: Disable the DHCPv6 Snooping binding user-access-control.

Usage Guide: Only enable the global DHCPv6 Snooping function at first, it is able to enable the user-access-control function. This command can not be configured under Port-Channel mode. The no command clears all user-access-control rules of DHCPv6 Snooping on the port, but the binding can not be deleted.

Example: Enable the user-access-control funtion which is bound by DHCPv6 Snooping.

switch(config-if-ethernet1/0/1)# ipv6 dhcp snooping binding user-control

6.11 ipv6 dhcp snooping binding-limit

Command: ipv6 dhcp snooping binding-limit <*max-num*>

no ipv6 dhcp snooping binding-limit

Function: Set the max dynamic binding number which is allowed to be set on the port for DHCPv6 Snooping. The **no** command will not limit the number on the port.

Parameters: max-num: The max dynamic binding number that port allows to set, and the range from 1 to 100.

Command Mode: Port mode

Default: There is no limitation by default.

Usage Guide: When the limitation number is modified to a smaller value, the redundant dynamic binding will be deleted (delete the aged and interim binding at first). The static binding, which is created by user configuration, is not limited in number.

Example: Set the allowed max dynamic binding number as 10.

switch(config-if-ethernet1/0/1)# ipv6 dhcp snooping binding-limit 10

6.12 ip dhcp snooping trust

Command: ipv6 dhcp snooping trust

no ipv6 dhcp snooping trust

Function: Set the port to the trusted port. The **no** command sets the port to non-trusted port.

Parameters: None

Command Mode: Port mode

Default: By default, the port is non-trusted port.

Usage Guide: When a port turns into a trusted port from a non-trusted port, the original security policy of the port will be deleted that means clear all blackhole MAC or undo the shutdown of this port. At the same time, it allows the DHCPv6 responding packets of this port to be forwarded. When a port turns into a non-trusted port from a trusted port, forbid the DHCPv6 responding packets to be forwarded and drop them.

Example: Set the port as the trusted port.

switch(config-if-ethernet1/0/1)# ipv6 dhcp snooping trust

6.13 show ipv6 dhcp snooping binding

Command: show ipv6 dhcp snooping binding {*<MAC>* | *<ipv6address>* | interface [ethernet | port-channel] *<ifname>* | all}

Function: Show the binding information of DHCPv6 Snooping.

Parameter: MAC: Show the specific MAC address

ipv6 address: Show the specific IPv6 address

ifname: The port ID

all: Show all DHCPv6 Snooping binding

Command Mode: Any mode

Default: None

Usage Guide: Display the specified (one port or all ports) binding information for DHCPv6 Snooping.

Example: Disable the binding information function of DHCPv6 Snooping:

switch(config)# show ipv6 dhcp snooping binding all

DHCPv6 Snooping is enabled

DHCPv6 Snooping binding count 1, static binding 0

MAC	IPv6 address	Interface	Vlan ID	State

00-19-e0-3f-d1-83 2001::100 Ethernet1/0/13 1 DHCPv6_BOUND

6.14 show ipv6 dhcp snooping interface

Command: show ipv6 dhcp snooping interface [ethernet | port-channel] <ifname>

Function: Display the current port cofiguration of DHCPv6 Snooping.

Parameters: ifname: The port name.

Command Mode: Any Mode.

Default: None.

Usage Guide: Collect the information about the ports: the relating configuration, the detail information of binding data, detail information of the warning data.

Example: Display the current port cofiguration of DHCPv6 Snooping.

switch(config)# show ipv6 dhcp snooping interface ethernet 1/0/13

interface Ethernet1/0/13 user config:

trust attribute: untrust

action: none

binding user control: disabled

recovery interval: infinite

Alarm info: 0

Dynamic binding info: 1

DHCPv6 Snooping Binding built at MON JAN 16 02:40:29 2006

Time Stamp: 5634

Vlan: 1, Port: Ethernet1/0/13

Client MAC: 00-19-e0-3f-d1-83

Client IPv6 addr: 2001::200

Lease: 259200(s)

Flag: Dynamic

Static Binding info: 0

Chapter 7 Commands for DHCPv6 option 52

7.1 option 52 ascii LINE

Command: option 52 ascii LINE

no option 52

Function: Configure option 52 character string with ascii format in ipv6 dhcp pool mode. The **no** command deletes the configured option 52.

Parameter: LINE: The configured option 52 character string with ascii format, its length range between 1 and 255.

Default: No option 52 character string is configured.

Command Mode: ipv6 dhcp pool mode

Usage Guide: None.

Example: Configure option 52 with ascii format to be "AP 1000".

switch(config)#ipv6 dhcp pool a

switch(dhcpv6-a-config)#option 52 ascii AP 1000

7.2 option 52 hex WORD

Command: option 52 hex WORD

no option 52

Function: Configure option 52 character string with hex format in ipv6 dhcp pool mode. The **no** command deletes the configured option 52.

Parameter: WORD: The configured option 52 character string with hex format, such as a1241b.

Default: No option 52 is configured.

Command Mode: ipv6 dhcp pool mode

Usage Guide: None.

Example: Configure option 52 with hex format to be "01102001000100000000000000000000100" (it means the IPv6 address is 2001:1::100).

switch(config)#ipv6 dhcp pool a

switch(dhcpv6-a-config)#option 52 hex 01102001000100000000000000000000100

7.3 option 52 ipv6 X:X::X:X

Command: option 52 ipv6 X:X::X:X

no option 52

Function: Configure option 52 character string with IPv6 format in ipv6 dhcp pool mode. The **no** command deletes the configured option 52.

Parameter: X:X::X:X: The configured option 52 with IPv6 format, such as 2001:1::100.

Default: No option 52 is configured.

Command Mode: ipv6 dhcp pool mode

Usage Guide: Using this command to configure option 52, such as "2001:1::100", then option 52 filled in packets is the corresponding hexadecimal format of this IPv6 address.

Example: Configure option 52 with IPv6 format to be "2001:1::100".

switch(config)#ipv6 dhcp pool a

switch(dhcpv6-a-config)#option 52 ipv6 2001:1::100