Content

CHAPTER 1 DHCP CONFIGURATION 1-1

1.1 INTRODUCTION TO DHCP 1-1

1.2 DHCP SERVER CONFIGURATION...1-2

1.3 DHCP RELAY CONFIGURATION 1-5

1.4 DHCP CONFIGURATION EXAMPLES...1-6

1.5 DHCP TROUBLESHOOTING..1-9

CHAPTER 2 DHCPV6 CONFIGURATION.................................2-1

2.1 INTRODUCTION TO DHCPV6 2-1

2.2 DHCPV6 SERVER CONFIGURATION..2-2

2.3 DHCPV6 RELAY DELEGATION CONFIGURATION 2-4

2.4 DHCPV6 PREFIX DELEGATION SERVER CONFIGURATION.......................2-4

2.5 DHCPV6 PREFIX DELEGATION CLIENT CONFIGURATION 2-6

2.6 DHCPV6 CONFIGURATION EXAMPLES..2-7

2.7 DHCPV6 TROUBLESHOOTING...2-11

CHAPTER 3 DHCP OPTION 60 AND OPTION 43 3-1

3.1 INTRODUCTION TO DHCP OPTION 60 AND OPTION 43............................3-1

3.2 DHCP OPTION 60 AND OPTION 43 CONFIGURATION TASK LIST 3-1

3.3 DHCPV6 OPTION 60 AND OPTION 43 EXAMPLE 3-2

3.4 DHCP OPTION 60 AND OPTION 43 TROUBLESHOOTING 3-3

CHAPTER 4 DHCP OPTION 82 CONFIGURATION..................4-1

4.1 INTRODUCTION TO DHCP OPTION 82 4-1

4.1.1 DHCP option 82 Message Structure 4-1
4.1.2 option 82 Working Mechanism..4-2

4.2 DHCP OPTION 82 CONFIGURATION TASK LIST 4-3

4.3 DHCP OPTION 82 APPLICATION EXAMPLES 4-7

4.4 DHCP OPTION 82 TROUBLESHOOTING 4-8

CHAPTER 5 DHCP SNOOPING CONFIGURATION 5-1

5.1 INTRODUCTION TO DHCP SNOOPING..5-1

5.2 DHCP SNOOPING CONFIGURATION TASK SEQUENCE 5-2

5.3 DHCP SNOOPING TYPICAL APPLICATION...5-7

5.4 DHCP SNOOPING TROUBLESHOOTING HELP 5-8

5.4.1 Monitor and Debug Information 5-8
5.4.2 DHCP Snooping Troubleshooting Help...5-8

CHAPTER 6 DHCPV6 SNOOPING CONFIGURATION............6-1

6.1 INTRODUCTION TO DHCPV6 SNOOPING...6-1

6.1.1 Defense against Fake DHCPv6 Server...6-1
6.1.2 Defense against Fake IPv6 Address 6-1
6.1.3 Defense against the attack of DHCPv6 addresses exhaustion 6-1
6.1.4 Defense against ND cheat..6-2
6.1.5 Reply the remove requirement for port 6-2

6.2 DHCPV6 SNOOPING CONFIGURATION TASK SEQUENCE 6-2

6.3 DHCPV6 SNOOPING TYPICAL APPLICATION...6-5

6.4 DHCPV6 SNOOPING TROUBLESHOOTING 6-6

6.4.1 Monitor and Debug Information 6-6
6.4.2 DHCPv6 Snooping Troubleshooting Help...6-6

CHAPTER 7 DHCPV6 OPTION 52...7-1

7.1 INTRODUCTION TO DHCPV6 OPTION 52 7-1

7.2 DHCPV6 OPTION 52 CONFIGURATION TASK LIST 7-1

7.3 DHCPV6 OPTION 52 CONFIGURATION EXAMPLE 7-2

7.4 DHCPV6 OPTION 52 TROUBLESHOOTING 7-2

Chapter 1 DHCP Configuration

Explanation:

The layer 3 switch in this chapter represents the a general sense of router or wireless controller which is running routing protocol.

1.1 Introduction to DHCP

DHCP [RFC2131] is the acronym for Dynamic Host Configuration Protocol. It is a protocol that assigns IP address dynamically from the address pool as well as other network configuration parameters such as default gateway, DNS server, and default route and host image file position within the network. DHCP is the enhanced version of BOOTP. It is a mainstream technology that can not only provide boot information for diskless workstations, but can also release the administrators from manual recording of IP allocation and reduce user effort and cost on configuration. Another benefit of DHCP is it can partially ease the pressure on IP demands, when the user of an IP leaves the network that IP can be assigned to another user.

DHCP is a client-server protocol, the DHCP client requests the network address and configuration parameters from the DHCP server; the server provides the network address and configuration parameters for the clients; if DHCP server and clients are located in different subnets, DHCP relay is required for DHCP packets to be transferred between the DHCP client and DHCP server. The implementation of DHCP is shown below:

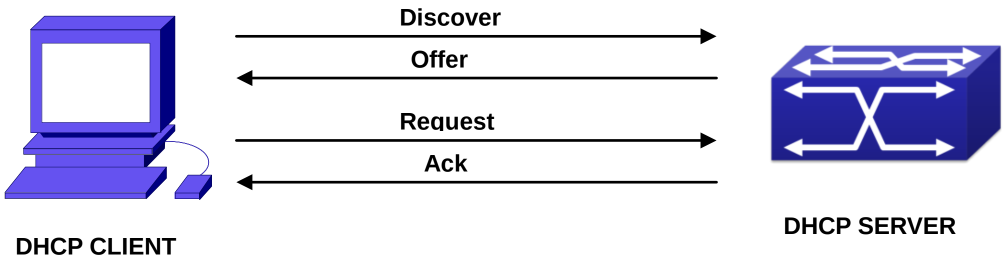


Fig 1-1 DHCP protocol interaction

Explanation:

1. DHCP client broadcasts DHCPDISCOVER packets in the local subnet.
2. On receiving the DHCPDISCOVER packet, DHCP server sends a DHCPOFFER packet along with IP address and other network parameters to the DHCP client.
3. DHCP client broadcast DHCPREQUEST packet with the information for the DHCP server it selected after selecting from the DHCPOFFER packets.

4. The DHCP server selected by the client sends a DHCPACK packet and the client gets an IP address and other network configuration parameters.

The above four steps finish a Dynamic host configuration assignment process. However, if the DHCP server and the DHCP client are not in the same network, the server will not receive the DHCP broadcast packets sent by the client, therefore no DHCP packets will be sent to the client by the server. In this case, a DHCP relay is required to forward such DHCP packets so that the DHCP packets exchange can be completed between the DHCP client and server.

Switch can act as both a DHCP server and a DHCP relay. DHCP server supports not only dynamic IP address assignment, but also manual IP address binding (i.e. specify a specific IP address to a specified MAC address or specified device ID over a long period. The differences and relations between dynamic IP address allocation and manual IP address binding are: 1) IP address obtained dynamically can be different every time; manually bound IP address will be the same all the time. 2) The lease period of IP address obtained dynamically is the same as the lease period of the address pool, and is limited; the lease of manually bound IP address is theoretically endless. 3) Dynamically allocated address cannot be bound manually. 4) Dynamic DHCP address pool can inherit the network configuration parameters of the dynamic DHCP address pool of the related segment.

1.2 DHCP Server Configuration

DHCP Sever Configuration Task List:

1. Enable/Disable DHCP service
2. Configure DHCP Address pool
    (1) Create/Delete DHCP Address pool
    (2) Configure DHCP address pool parameters
    (3) Configure manual DHCP address pool parameters
3. Enable logging for address conflicts

1. Enable/Disable DHCP service

Command	Explanation
Global Mode	
service dhcp **no service dhcp**	Enable DHCP server. The no command disables DHCP server.

2. Configure DHCP Address pool

(1) Create/Delete DHCP Address pool

Command	Explanation
Global Mode	
ip dhcp pool <*name*> **no ip dhcp pool <*name*>**	Configure DHCP Address pool. The no operation cancels the DHCP Address pool.

(2) Configure DHCP address pool parameters

Command	Explanation
DHCP Address Pool Mode	
network-address <*network-number*> [mask | prefix-length] **no network-address**	Configure the address scope that can be allocated to the address pool. The no operation of this command cancels the allocation address pool.
default-router [<*address1*>[<*address2*>[…<*address 8*>]]] **no default-router**	Configure default gateway for DHCP clients. The no operation cancels the default gateway.
dns-server [<*address1*>[<*address2*>[…<*address 8*>]]] **no dns-server**	Configure DNS server for DHCP clients. The no command deletes DNS server configuration.
domain-name <*domain*> **no domain-name**	Configure Domain name for DHCP clients; the "**no domain-name**" command deletes the domain name.
netbios-name-server [<*address1*>[<*address2*>[…<*address 8*>]]] **no netbios-name-server**	Configure the address for WINS server. The no operation cancels the address for server.
netbios-node-type {b-node|h-node|m-node|p-node|<*type -number*>} **no netbios-node-type**	Configure node type for DHCP clients. The no operation cancels the node type for DHCP clients.
bootfile <*filename*> **no bootfile**	Configure the file to be imported for DHCP clients on boot up. The no command cancels this operation.

next-server [<*address1*>[<*address2*>[…<*address 8*>]]] **no next-server [<*address1*>[<*address2*>[…<*address 8*>]]]**	Configure the address of the server hosting file for importing. The no command deletes the address of the server hosting file for importing.
option <*code*> {ascii <*string*> | hex <*hex*> | ipaddress <*ipaddress*>} **no option <*code*>**	Configure the network parameter specified by the option code. The no command deletes the network parameter specified by the option code.
lease { days [hours][minutes] | infinite } **no lease**	Configure the lease period allocated to addresses in the address pool. The no command deletes the lease period allocated to addresses in the address pool.
max-lease-time {[<*days*>] [<*hours*>] [<*minutes*>] | infinite} **no max-lease-time**	Set the maximum lease time for the addresses in the address pool; the no command restores the default setting.
Global Mode	
ip dhcp excluded-address <*low-address*> [<*high-address*>] **no ip dhcp excluded-address <*low-address*> [<*high-address*>]**	Exclude the addresses in the address pool that are not for dynamic allocation.

(3) Configure manual DHCP address pool parameters

Command	Explanation
DHCP Address Pool Mode	
hardware-address <*hardware-address*> [{Ethernet | IEEE802|<*type-number*>}] **no hardware-address**	Specify/delete the hardware address when assigning address manually.
host <*address*> [<*mask*> | <*prefix-length*>] **no host**	Specify/delete the IP address to be assigned to the specified client when binding address manually.
client-identifier <*unique-identifier*> **no client-identifier**	Specify/delete the unique ID of the user when binding address manually.

3. Enable logging for address conflicts

Command	Explanation
Global Mode	

ip dhcp conflict logging **no ip dhcp conflict logging**	Enable/disable logging for DHCP address to detect address conflicts.
Admin Mode	
clear ip dhcp conflict <*address* | all >	Delete a single address conflict record or all conflict records.

1.3 DHCP Relay Configuration

When the DHCP client and server are in different segments, DHCP relay is required to transfer DHCP packets. Adding a DHCP relay makes it unnecessary to configure a DHCP server for each segment, one DHCP server can provide the network configuration parameter for clients from multiple segments, which is not only cost-effective but also management-effective.

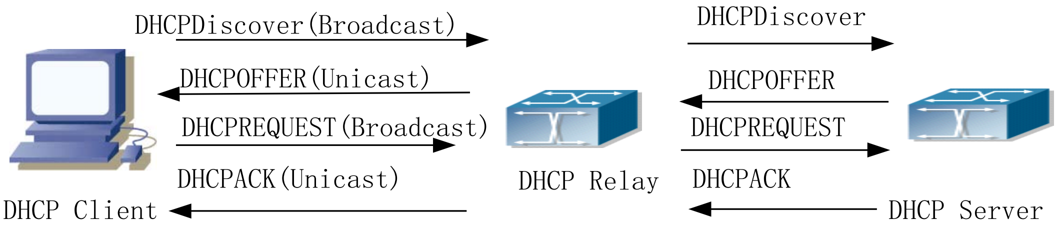


Fig 1-2 DHCP relay

As shown in the above figure, the DHCP client and the DHCP server are in different networks, the DHCP client performs the four DHCP steps as usual yet DHCP relay is added to the process.

1. The client broadcasts a DHCPDISCOVER packet, and DHCP relay inserts its own IP address to the relay agent field in the DHCPDISCOVER packet on receiving the packet, and forwards the packet to the specified DHCP server (for DHCP frame format, please refer to RFC2131).
2. On the receiving the DHCPDISCOVER packets forwarded by DHCP relay, the DHCP server sends the DHCPOFFER packet via DHCP relay to the DHCP client.
3. DHCP client chooses a DHCP server and broadcasts a DHCPREQUEST packet, DHCP relay forwards the packet to the DHCP server after processing.
4. On receiving DHCPREQUEST, the DHCP server responds with a DHCPACK packet via DHCP relay to the DHCP client.

DHCP Relay Configuration Task List:

1. Enable DHCP relay.
2. Configure DHCP relay to forward DHCP broadcast packet.

1. Enable DHCP relay.

Command	Explanation
Global Mode	
service dhcp **no service dhcp**	DHCP server and DHCP relay is enabled as the DHCP service is enabled.

2. Configure DHCP relay to forward DHCP broadcast packet.

Command	Explanation
Global Mode	
ip forward-protocol udp bootps **no ip forward-protocol udp bootps**	The UDP port 67 is used for DHCP broadcast packet forwarding.
Interface Configuration Mode	
ip helper-address <*ipaddress*> **no ip helper-address <*ipaddress*>**	Set the destination IP address for DHCP relay forwarding; the "**no ip helper-address <*ipaddress*>**"command cancels the setting.

1.4 DHCP Configuration Examples

Scenario 1:

Too save configuration efforts of network administrators and users, a company is using switch as a DHCP server. The Admin VLAN IP address is 10.16.1.2/16. The local area network for the company is divided into network A and B according to the office locations. The network configurations for location A and B are shown below.

PoolA(network 10.16.1.0)		PoolB(network 10.16.2.0)	
Device	IP address	Device	IP address
Default gateway	10.16.1.200 10.16.1.201	Default gateway	10.16.1.200 10.16.1.201
DNS server	10.16.1.202	DNS server	10.16.1.202
WINS server	10.16.1.209	WWW server	10.16.1.209
WINS node type	H-node		
Lease	3 days	Lease	1day

In location A, a machine with MAC address 00-03-22-23-dc-ab is assigned with a fixed IP address of 10.16.1.210 and named as "management".

```
Switch(config)#service dhcp
Switch(config)#interface vlan 1
Switch(Config-Vlan-1)#ip address 10.16.1.2 255.255.0.0
Switch(Config-Vlan-1)#exit
Switch(config)#ip dhcp pool A
Switch(dhcp-A-config)#network 10.16.1.0 24
Switch(dhcp-A-config)#lease 3
Switch(dhcp-A-config)#default-route 10.16.1.200 10.16.1.201
Switch(dhcp-A-config)#dns-server 10.16.1.202
Switch(dhcp-A-config)#netbios-name-server 10.16.1.209
Switch(dhcp-A-config)#netbios-node-type H-node
Switch(dhcp-A-config)#exit
Switch(config)#ip dhcp excluded-address 10.16.1.200 10.16.1.201
Switch(config)#ip dhcp pool B
Switch(dhcp-B-config)#network 10.16.2.0 24
Switch(dhcp-B-config)#lease 1
Switch(dhcp-B-config)#default-route 10.16.2.200 10.16.2.201
Switch(dhcp-B-config)#dns-server 10.16.2.202
Switch(dhcp-B-config)#option 72 ip 10.16.2.209
Switch(dhcp-config)#exit
Switch(config)#ip dhcp excluded-address 10.16.2.200 10.16.2.201
Switch(config)#ip dhcp pool A1
Switch(dhcp-A1-config)#host 10.16.1.210
Switch(dhcp-A1-config)#hardware-address 00-03-22-23-dc-ab
Switch(dhcp-A1-config)#exit
```

Usage Guide: When a DHCP/BOOTP client is connected to a VLAN1 port of the switch, the client can only get its address from 10.16.1.0/24 instead of 10.16.2.0/24. This is because the broadcast packet from the client will be requesting the IP address in the same segment of the VLAN interface after VLAN interface forwarding, and the VLAN interface IP address is 10.16.1.2/24, therefore the IP address assigned to the client will belong to 10.16.1.0/24.

If the DHCP/BOOTP client wants to have an address in 10.16.2.0/24, the gateway forwarding broadcast packets of the client must belong to 10.16.2.0/24. The connectivity between the client gateway and the switch must be ensured for the client to get an IP address from the 10.16.2.0/24 address pool.

Scenario 2:

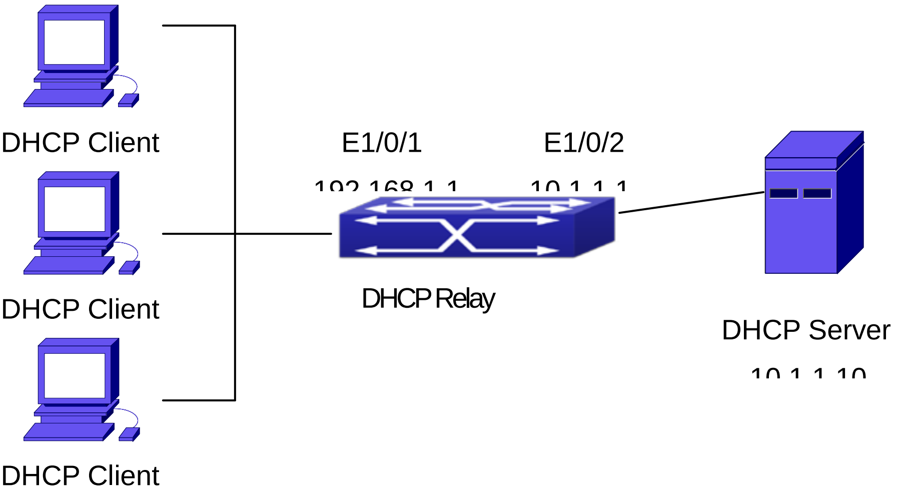


Fig 1-3 DHCP Relay Configuration

As shown in the above figure, route switch is configured as a DHCP relay. The DHCP server address is 10.1.1.10, the configuration steps is as follows:

```
Switch(config)#service dhcp
Switch(config)#interface vlan 1
Switch(Config-if-Vlan1)#ip address 192.168.1.1 255.255.255.0
Switch(Config-if-Vlan1)#exit
Switch(config)#vlan 2
Switch(Config-Vlan-2)#exit
Switch(config)#interface Ethernet 1/0/2
Switch(Config-Erthernet1/0/2)#switchport access vlan 2
Switch(Config-Erthernet1/0/2)#exit
Switch(config)#interface vlan 2
Switch(Config-if-Vlan2)#ip address 10.1.1.1 255.255.255.0
Switch(Config-if-Vlan2)#exit
Switch(config)#ip forward-protocol udp bootps
Switch(config)#interface vlan 1
Switch(Config-if-Vlan1)#ip help-address 10.1.1.10
Switch(Config-if-Vlan1)#exit
```

Note: It is recommended to use the combination of command **ip forward-protocol udp** ***<port>*** and **ip helper-address** ***<ipaddress>***. **ip help-address** can only be configured for ports on layer 3 and cannot be configured on layer 2 ports directly.

1.5 DHCP Troubleshooting

If the DHCP clients cannot obtain IP addresses and other network parameters, the following procedures can be followed when DHCP client hardware and cables have been verified ok.

☞ Verify the DHCP server is running, start the related DHCP server if not running. If the DHCP clients and servers are not in the same physical network, verify the router responsible for DHCP packet forwarding has DHCP relay function. If DHCP relay is not available for the intermediate router, it is recommended to replace the router or upgrade its software to one that has a DHCP relay function.

☞ In such case, DHCP server should be examined for an address pool that is in the same segment of the switch VLAN, such a pool should be added if not present, and (This does not indicate switch cannot assign IP address for different segments, see solution 2 for details.)

☞ In DHCP service, pools for dynamic IP allocation and manual binding are conflicting, i.e., if command “**network-address**” and “**host**” are run for a pool, only one of them will take effect; furthermore, in manual binding, only one IP-MAC binding can be configured in one pool. If multiple bindings are required, multiple manual pools can be created and IP-MAC bindings set for each pool. New configuration in the same pool overwrites the previous configuration.

Chapter 2 DHCPv6 Configuration

2.1 Introduction to DHCPv6

DHCPv6 [RFC3315] is the IPv6 version for Dynamic Host Configuration Protocol (DHCP). It is a protocol that assigns IPv6 address as well as other network configuration parameters such as DNS address, and domain name to DHCPv6 client, DHCPv6 is a conditional auto address configuration protocol relative to IPv6. In the conditional address configuration process, DHCPv6 server assigns a complete IPv6 address to client, and provides DNS address, domain name and other configuration information, maybe the DHCPv6 packet can transmit through relay delegation, at last the binding of IPv6 address and client can be recorded by DHCPv6 server, all that can enhance the management of network; DHCPv6 server can also provide non state DHCPv6 service, that is only assigns DNS address and domain name and other configuration information but not assigns IPv6 address, it can solve the bug of IPv6 auto address configuration in non state; DHCPv6 can provide extend function of DHCPv6 prefix delegation, upstream route can assign address prefix to downstream route automatically, that achieve the IPv6 address auto assignment in levels of network environment, and resolved the problem of ISP and IPv6 network dispose.

There are three entities in the DHCPv6 protocol – the client, the relay and the server. The DHCPv6 protocol is based on the UDP protocol. The DHCPv6 client sends request messages to the DHCP server or DHCP relay with the destination port as 547, and the DHCPv6 server and relay send replying messages with the destination port as 546. The DHCPv6 client sends solicit or request messages with the multicast address – ff02::1:2 for DHCP relay and server.

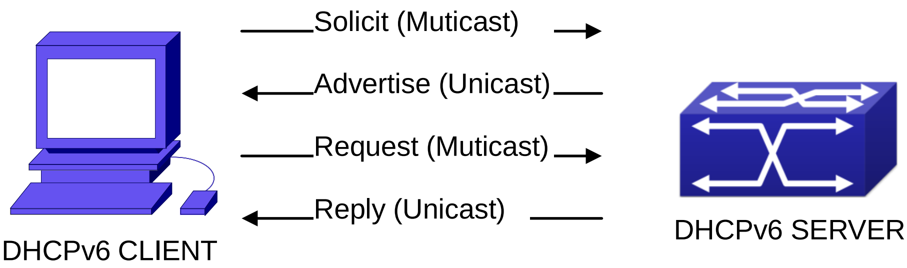


Fig 2-1 DHCPv6 negotiation

When a DHCPv6 client tries to request an IPv6 address and other configurations from the DHCPv6 server, the client has to find the location of the DHCP server, and then request configurations from the DHCP server.

1. In the time of located server, the DHCP client tries to find a DHCPv6 server by broadcasting a SOLICIT packet to all the DHCP delay delegation and server with broadcast address as FF02::1:2.
2. Any DHCP server which receives the request, will reply the client with an ADVERTISE message, which includes the identity of the server –DUID, and its priority.
3. It is possible that the client receives multiple ADVERTISE messages. The client should select one and reply it with a REQUEST message to request the address which is advertised in the ADVERTISE message.
4. The selected DHCPv6 server then confirms the client about the IPv6 address and any other configuration with the REPLY message.

The above four steps finish a Dynamic host configuration assignment process. However, if the DHCPv6 server and the DHCPv6 client are not in the same network, the server will not receive the DHCPv6 broadcast packets sent by the client, therefore no DHCPv6 packets will be sent to the client by the server. In this case, a DHCPv6 relay is required to forward such DHCPv6 packets so that the DHCPv6 packets exchange can be completed between the DHCPv6 client and server.

At the time this manual is written, DHCPv6 server, relay and prefix delegation client have been implemented on the switch. When the DHCPv6 relay receives any messages from the DHCPv6 client, it will encapsulate the request in a Relay-forward packet and deliver it to the next DHCPv6 relay or the DHCPv6 server. The DHCPv6 messages coming from the server will be encapsulated as relay reply packets to the DHCPv6 relay. The relay then removes the encapsulation and delivers it the DHCPv6 client or the next DHCPv6 relay in the network.

For DHCPv6 prefix delegation where DHCPv6 server is configured on the PE router and DHCPv6 client it configured on the CPE router, the CPE router is able to send address prefix allocation request to the PE router and get a pre-configured address prefix, but not set the address prefix manually. The protocol negotiation between the client and the prefix delegation client is quite similar to that when getting a DHCPv6 address. Then the CPE router divides the allocated prefix – whose length should be less than 64 characters, into 64 subnets. The divided address prefix will be advertised through routing advertisement messages (RA) to the host directly connected to the client.

2.2 DHCPv6 Server Configuration

DHCPv6 server configuration task list as below:

1. To enable/disable DHCPv6 service
2. To configure DHCPv6 address pool
    （1） To achieve/delete DHCPv6 address pool
    （2） To configure parameter of DHCPv6 address pool
3. To enable DHCPv6 server function on port

1. To enable/disable DHCPv6 service

Command	Explanation
Global Mode	
service dhcpv6 **no service dhcpv6**	To enable DHCPv6 service.

2. To configure DHCPv6 address pool

（1）To achieve/delete DHCPv6 address pool

Command	Explanation
Global Mode	
ipv6 dhcp pool <*poolname*> **no ipv6 dhcp pool <*poolname*>**	To configure DHCPv6 address pool.

（2）To configure parameter of DHCPv6 address pool

Command	Explanation
DHCPv6 address pool Configuration Mode	
network-address <*ipv6-pool-start-address*> {<*ipv6-pool-end-address*> | <*prefix-length*>} [eui-64] **no network-address**	To configure the range of IPv6 address assignable of address pool.
dns-server <*ipv6-address*> **no dns-server <*ipv6-address*>**	To configure DNS server address for DHCPv6 client.
domain-name <*domain-name*> **no domain-name <*domain-name*>**	To configure DHCPv6 client domain name.
excluded-address <*ipv6-address*> **no excluded-address <*ipv6-address*>**	To exclude IPv6 address which isn’t used for dynamic assignment in address pool.
lifetime {<*valid-time*> | infinity} {<*preferred-time*> | infinity} **no lifetime**	To configure valid time or preferred time of DHCPv6 address pool.

3. To enable DHCPv6 server function on port.

Command	Explanation
Interface Configuration Mode	
ipv6 dhcp server <*poolname*> [preference <*value*>] [rapid-commit] [allow-hint] **no ipv6 dhcp server <*poolname*>**	To enable DHCPv6 server function on specified port, and binding the used DHCPv6 address pool.

2.3 DHCPv6 Relay Delegation Configuration

DHCPv6 relay delegation configuration task list as below:

1. To enable/disable DHCPv6 service
2. To configure DHCPv6 relay delegation on port

1. To enable DHCPv6 service

Command	Explanation
Global Mode	
service dhcpv6 **no service dhcpv6**	To enableDHCPv6 service.

2. To configure DHCPv6 relay delegation on port

Command	Explanation
Interface Configuration Mode	

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*>}]}
	To specify the destination address of DHCPv6 relay transmit; The no form of this command delete the configuration.

2.4 DHCPv6 Prefix Delegation Server Configuration

DHCPv6 prefix delegation server configuration task list as below:

1. To enable/delete DHCPv6 service
2. To configure prefix delegation pool
3. To configure DHCPv6 address pool

（1） To achieve/delete DHCPv6 address pool
（2） To configure prefix delegation pool used by DHCPv6 address pool
（3） To configure static prefix delegation binding
（4） To configure other parameters of DHCPv6 address pool

4. To enable DHCPv6 prefix delegation server function on port

1. To enable/delete DHCPv6 service

Command	Explanation
Global Mode	
service dhcpv6 **no service dhcpv6**	To enable DHCPv6 service.

2. To configure prefix delegation pool

Command	Explanation
Global Mode	
ipv6 local pool <*poolname*> <*prefix*|*prefix-length*> <*assigned-length*> **no ipv6 local pool <*poolname*>**	To configure prefix delegation pool.

3. To configure DHCPv6 address pool

（1）To achieve/delete DHCPv6 address pool

Command	Explanation
Global Mode	
ipv6 dhcp pool <*poolname*> **no ipv6 dhcp pool <*poolname*>**	To configure DHCPv6 address pool.

（2）To configure prefix delegation pool used by DHCPv6 address pool

Command	Explanation
DHCPv6 address pool Configuration Mode	
prefix-delegation pool <*poolname*> [lifetime {<*valid-time*> | *infinity*} {<*preferred-time*> | infinity}] **no prefix-delegation pool <*poolname*>**	To specify prefix delegation pool used by DHCPv6 address pool, and assign usable prefix to client.

（3） To configure static prefix delegation binding

Command	Explanation

DHCPv6 address pool Configuration Mode	
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*>]**	To specify IPv6 prefix and any prefix required static binding by client.

（4） To configure other parameter of DHCPv6 address pool

Command	Explanation
DHCPv6 address pool Configuration Mode	
dns-server <*ipv6-address*> **no dns-server <*ipv6-address*>**	To configure DNS server address for DHCPv6 client.
domain-name <*domain-name*> **no domain-name <*domain-name*>**	To configure domain name for DHCPv6 client.

4. To enable DHCPv6 prefix delegation server function on port

Command	Explanation
Interface Configuration Mode	
ipv6 dhcp server <*poolname*> [preference <*value*>] [rapid-commit] [allow-hint] **no ipv6 dhcp server <*poolname*>**	To enable DHCPv6 server function on specified port, and binding used DHCPv6 address pool.

2.5 DHCPv6 Prefix Delegation Client Configuration

DHCPv6 prefix delegation client configuration task list as below:

1. To enable/disable DHCPv6 service
2. To enable DHCPv6 prefix delegation client function on port

1. To enable/disable DHCPv6 service

Command	Explanation
Global Mode	

service dhcpv6 **no service dhcpv6**	To enable DHCPv6 service.

2. To enable DHCPv6 prefix delegation client function on port

Command	Explanation
Interface Configuration Mode	
ipv6 dhcp client pd <*prefix-name*> [rapid-commit] **no ipv6 dhcp client pd**	To enable client prefix delegation request function on specified port, and the prefix obtained associate with universal prefix configured.

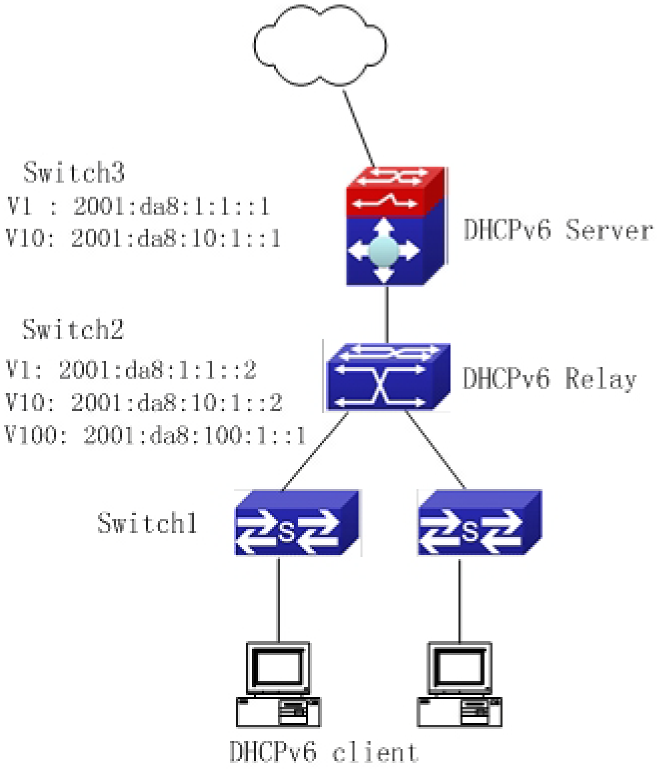
2.6 DHCPv6 Configuration Examples

Example1:

When deploying IPv6 networking, the switch can be configured as DHCPv6 server in order to manage the allocation of IPv6 addresses. Both the state and the stateless DHCPv6 are supported.

Topology:

The access layer use Switch1 switch to connect users of dormitory buildings; Switch2 is configured as DHCPv6 relay delegation in primary aggregation layer ; Switch3 is configured as DHCPv6 server in secondary aggregation layer, and connected with backbone network or higher aggregation layers; The Windows Vista which be provided with DHCPv6 client must load on PC.



Usage guide:

Switch3 configuration：

```
Switch3>enable
Switch3#config
Switch3(config)#service dhcpv6
Switch3(config)#ipv6 dhcp pool EastDormPool
Switch3(dhcpv6-EastDormPool-config)#network-address 2001:da8:100:1::1 2001:da8:100:1::100
Switch3(dhcpv6-EastDormPool-config)#excluded-address 2001:da8:100:1::1
Switch3(dhcpv6-EastDormPool-config)#dns-server 2001:da8::20
Switch3(dhcpv6-EastDormPool-config)#dns-server 2001:da8::21
Switch3(dhcpv6-EastDormPool-config)#domain-name dhcpv6.com
Switch3(dhcpv6-EastDormPool-config)#lifetime 1000 600
Switch3(dhcpv6-EastDormPool-config)#exit
Switch3(config)#interface vlan 1
Switch3(Config-if-Vlan1)#ipv6 address 2001:da8:1:1::1/64
Switch3(Config-if-Vlan1)#exit
Switch3(config)#interface vlan 10
Switch3(Config-if-Vlan10)#ipv6 address 2001:da8:10:1::1/64
Switch3(Config-if-Vlan10)#ipv6 dhcp server EastDormPool preference 80
Switch3(Config-if-Vlan10)#exit
Switch3(config)#
```

Switch2 configuration：

```
Switch2>enable
Switch2#config
Switch2(config)#service dhcpv6
Switch2(config)#interface vlan 1
Switch2(Config-if-Vlan1)#ipv6 address 2001:da8:1:1::2/64
Switch2(Config-if-Vlan1)#exit
Switch2(config)#interface vlan 10
Switch2(Config-if-Vlan10)#ipv6 address 2001:da8:10:1::2/64
Switch2(Config-if-Vlan10)#exit
Switch2(config)#interface vlan 100
Switch2(Config-if-Vlan100)#ipv6 address 2001:da8:100:1::1/64
Switch2(Config-if-Vlan100)#no ipv6 nd suppress-ra
Switch2(Config-if-Vlan100)#ipv6 nd managed-config-flag
Switch2(Config-if-Vlan100)#ipv6 nd other-config-flag
Switch2(Config-if-Vlan100)#ipv6 dhcp relay destination 2001:da8:10:1::1
Switch2(Config-if-Vlan100)#exit
Switch2(config)#
```

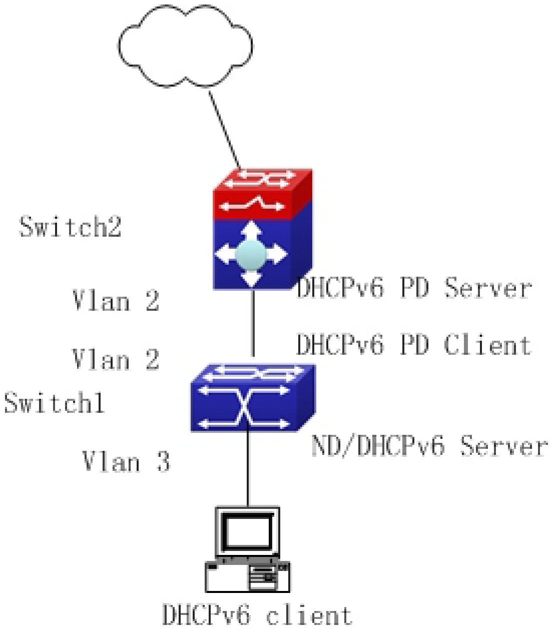
Example2:

When the network operator is deploying IPv6 networks, network automatically configuration can be achieved through the prefix delegation allocation of IPv6 addresses, in stead of configuring manually for each switch:

1. To configure the switching or routing device which is connected to the client switch as DHCPv6 prefix delegation server, that is to setup a local database for the relationship between the allocated prefix and the DUID of the client switch.
2. To configure the switch as the prefix delegation client, and make the client switch to get IPv6 address prefix from the prefix delegation server, through a process which is much like the process of DHCPv6 address allocation.
3. The edge devices which receive the address prefix, send routing advertisement - RA messages, to the client hosts about the address prefix through the interface which is connected to the hosts, then the hosts get an valid IPv6 address through stateless auto configuration, while at the same time, the stateless DHCPv6 server will be configured for the interface, in order to provide the DHCPv6 client with information such as DNS, and domain name, etc.

Network Topology:

The edge switch is a Switch1 switch. The interface connected to the trunk switch which is Switch2, is configured as the prefix delegation client. The interfaces connected to hosts, are configured as stateless DHCPv6 servers to provide the hosts with stateless information such as DNS and domain names, also routing advertisement of stateless address allocation is enabled for the host interfaces; On Switch2, the prefix delegation server is configured, and routing advertisement of state address allocation is enabled; On the host side, DHCPv6 client capable operating system such Windows Vista should be installed.



Usage guide:

Switch2 configuration

```
Switch2>enable
Switch2#config
Switch2(config)#interface vlan 2
Switch2(Config-if-Vlan2)#ipv6 address 2001:da8:1100::1/64
Switch2(Config-if-Vlan2)#exit
Switch2(config)#service dhcpv6
Switch2(config)#ipv6 local pool client-prefix-pool 2001:da8:1800::/40 48
Switch2(config)#ipv6 dhcp pool dhcp-pool
Switch2(dhcpv6-dhcp-pool-config)#prefix-delegation pool client-prefix-pool 1800 600
Switch2(dhcpv6-dhcp-pool-config)#exit
Switch2(config)#interface vlan 2
Switch2(Config-if-Vlan2)#ipv6 dhcp server dhcp-pool
Switch2(Config-if-Vlan2)#exit
```

Switch1 configuration

```
Switch1>enable
```

```
Switch1#config
Switch1(config)#service dhcpv6
Switch1(config)#interface vlan 2
Switch1(Config-if-Vlan2)#ipv6 dhcp client pd prefix-from-provider
Switch1(Config-if-Vlan2)#exit
Switch1(config)#interface vlan 3
Switch1(Config-if-Vlan3)#ipv6 address prefix-from-provider 0:0:0:1::1/64
Switch1(Config-if-Vlan3)#exit
Switch1(config)#ipv6 dhcp pool foo
Switch1(dhcpv6-foo-config)#dns-server 2001:4::1
Switch1(dhcpv6-foo-config)#domain-name www.ipv6.org
Switch1(dhcpv6-foo-config)#exit
Switch1(config)#interface vlan 3
Switch1(Config-if-Vlan3)#ipv6 dhcp server foo
Switch1(Config-if-Vlan3)#ipv6 nd other-config-flag
Switch1(Config-if-Vlan3)#no ipv6 nd suppress-ra
Switch1(Config-if-Vlan3)#exit
```

2.7 DHCPv6 Troubleshooting

If the DHCPv6 clients cannot obtain IPv6 addresses and other network parameters, the following procedures can be followed when DHCPv6 client hardware and cables have been verified ok:

- ☞ Verify the DHCPv6 server is running, start the related DHCP v6 server function if not running;
- ☞ If the DHCPv6 clients and servers are not in the same physical network, verify the router responsible for DHCPv6 packet forwarding has DHCPv6 relay function. If DHCPv6 relay is not available for the intermediate router, it is recommended to replace the router or upgrade its software to one that has a DHCPv6 relay function;
- ☞ Sometimes hosts are connected to the DHCPv6 enabled switches, but can not get IPv6 addresses. In this situation, it should be checked first whether the ports which the hosts are connected to, are connected with the port which the DHCPv6 server is connected to. If connected directly, it should be checked then whether the IPv6 address pool of the VLAN which the port belongs to, is in the same subnet with the address pool configure in the DHCPv6 server; If not connected directly, and any layer three DHCPv6 relay is configured between the hosts and the DHCPv6 server, it should be checked first whether an valid IPv6 address has been configured for the

switch interface which the hosts are connected to. If not configured, configure an valid IPv6 address. If configured, it should be checked whether the configured IPv6 address is in the same subnet with the DHCPv6 server. If not, please add it to the address pool.

Chapter 3 DHCP option 60 and option 43

3.1 Introduction to DHCP option 60 and option 43

DHCP server analyzes DHCP packets from DHCP client. If packets with option 60, it will decide whether option 43 is returned to DHCP client according to option 60 of packets and configuration of option 60 and option 43 in DHCP server address pool.

Configure the corresponding option 60 and option 43 in DHCP server address pool:

1. Address pool configured option 60 and option 43 at the same time. The received DHCP packet with option 60 from DHCP client, if it matches with option 60 of DHCP server address pool, DHCP client will receive the option 43 configured in the address pool, or else do not return option 43 to DHCP client.
2. Address pool only configured option 43, it will match with any option 60. If the received DHCP packet with option 60 from DHCP client, DHCP client will receive the option 43 configured in the address pool.
3. Address pool only configured option 60, it will not return option 43 to DHCP client.

3.2 DHCP option 60 and option 43 Configuration Task List

1. Basic DHCP option 60 and option 43 configuration

Command	Explanation
Address pool configuration mode	
option 60 ascii LINE	Configure option 60 character string with ascii format in ip dhcp pool mode.
option 43 ascii LINE	Configure option 43 character string with ascii format in ip dhcp pool mode.
option 60 hex WORD	Configure option 60 character string with hex format in ip dhcp pool mode.
option 43 hex WORD	Configure option 43 character string with hex format in ip dhcp pool mode.

option 60 ip A.B.C.D	Configure option 60 character string with IP format in ip dhcp pool mode.
option 43 ip A.B.C.D	Configure option 43 character string with IP format in ip dhcp pool mode.
no option 60	Delete the configured option 60 in the address pool mode.
no option 43	Delete the configured option 43 in the address pool mode.

3.3 DHCPv6 option 60 and option 43 Example

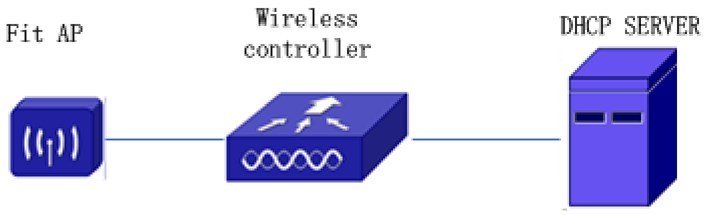


Fig 3-1 Typical DHCP option 60 and option 43 topology

Fit AP obtains IP address and option 43 attribute by DHCP server to send unicast discovery request for wireless controller. DHCP server configures option 60 matched with the option 60 of fit ap to return option 43 attribute to FTP AP. The wireless controller addresses of DHCP option 43 are 192.168.10.5 and 192.168.10.6.

Configuration procedure:

```
# Configure DHCP server
switch (config)#ip dhcp pool a
switch (dhcp-a-config)#option 60 ascii AP1000
switch (dhcp-a-config)#option 43 hex 0104C0A80A050104C0A80A06
```

DCWL-7900 series AP can get the domain information of the wireless controller through option 43 property, after FIT AP is resolved ddomain name through DNS server, FIT AP sends the unicast discovery request to the wireless controller. If the first digit of option 43 fileds is 01, it means that the wireless controlling address is the type of IP address; if it is 02, it means that the wireless controlling address is the type of domain name, and the second digit is the length of the corresponding IP address or domain name. The wireless controller domain names of DHCP option 43 are www.test.com and 123.com.

Configuration procedure:

```
# Configure DHCP server
switch(config)#ipdhcp pool a
switch(dhcp-a-config)#option 60 asciiudhcp 1.18.2
switch(dhcp-a-config)#option 43 hex 020C7777772E746573742E636F6D02073132332E636F6D
```

3.4 DHCP option 60 and option 43 Troubleshooting

If problems occur when configuring DHCP option 60 and option 43, please check whether the problem is caused by the following reasons:

- Check whether service dhcp function is enabled
- If the address pool configured option 60, check whether it matches with the option 60 of the packets

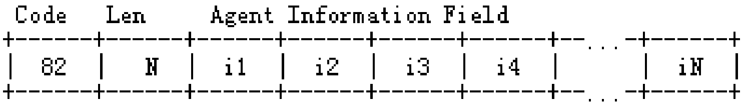
Chapter 4 DHCP option 82 Configuration

4.1 Introduction to DHCP option 82

DHCP option 82 is the Relay Agent Information Option, its option code is 82. DHCP option 82 is aimed at strengthening the security of DHCP servers and improving the IP address configuration policy. The Relay Agent adds option 82 (including the client’s physical access port, the access device ID and other information), to the DHCP request message from the client then forwards the message to DHCP server. When the DHCP server which supports the option 82 function receives the message, it will allocate an IP address and other configuration information for the client according to preconfigured policies and the option 82 information in the message. At the same time, DHCP server can identify all the possible DHCP attack messages according to the information in option 82 and defend against them. DHCP Relay Agent will peel the option 82 from the reply messages it receives, and forward the reply message to the specified port of the network access device, according to the physical port information in the option. The application of DHCP option 82 is transparent for the client.

4.1.1 DHCP option 82 Message Structure

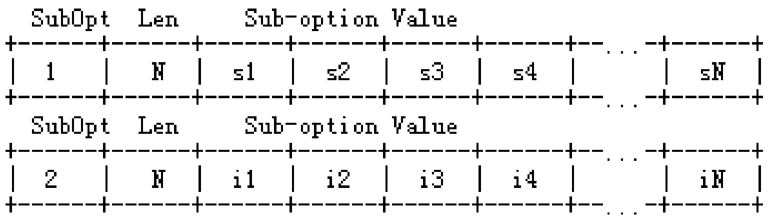
A DHCP message can have several option segments; option 82 is one of them. It has to be placed after other options but before option 255. The following is its format:



```
 Code   Len     Agent Information Field
+------+------+------+------+------+------+--...-+------+
|  82  |   N  |  i1  |  i2  |  i3  |  i4  |      |  iN  |
+------+------+------+------+------+------+--...-+------+
```

Code: represents the sequence number of the relay agent information option, the option 82 is called so because RFC3046 is defined as 82.
Len: the number of bytes in Agent Information Field, not including the two bytes in Code segment and Len segment.

Option 82 can have several sub-options, and need at least one sub-option. RFC3046 defines the following two sub-options, whose formats are showed as follows:

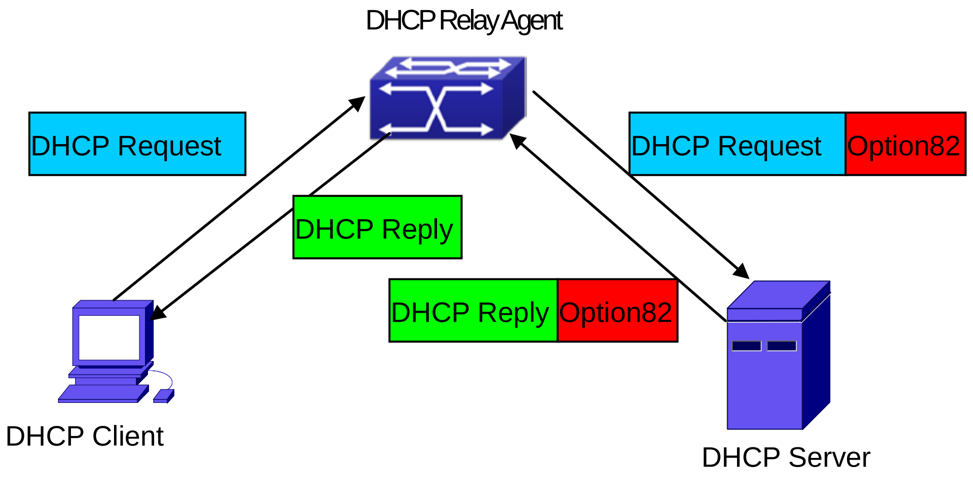


```
  SubOpt  Len     Sub-option Value
+------+------+------+------+------+------+--...-+------+
|  1   |  N   |  s1  |  s2  |  s3  |  s4  |      |  sN  |
+------+------+------+------+------+------+--...-+------+
  SubOpt  Len     Sub-option Value
+------+------+------+------+------+------+--...-+------+
|  2   |  N   |  i1  |  i2  |  i3  |  i4  |      |  iN  |
+------+------+------+------+------+------+--...-+------+
```

SubOpt: the sequence number of sub-option, the sequence number of Circuit ID sub-option is 1, the sequence number of Remote ID sub-option is 2.

Len: the number of bytes in Sub-option Value, not including the two bytes in SubOpt segment and Len segment.

4.1.2 option 82 Working Mechanism



DHCP option 82 flow chart

If the DHCP Relay Agent supports option 82, the DHCP client should go through the following four steps to get its IP address from the DHCP server: discover, offer, select and acknowledge. The DHCP protocol follows the procedure below:

1）DHCP client sends a request broadcast message while initializing. This request message does not have option 82.

2）DHCP Relay Agent will add the option 82 to the end of the request message it receives, then relay and forward the message to the DHCP server. By default, the sub-option 1 of option 82 (Circuit ID) is the interface information of the switch connected to the DHCP client (VLAN name and physical port name), but the users can configure the Circuit ID as they wish. The sub-option 2 of option 82(Remote ID) is the MAC address of the DHCP relay device.

3）After receiving the DHCP request message, the DHCP server will allocate IP address and other information for the client according to the information and preconfigured policy in the option segment of the message. Then it will forward the reply message with DHCP configuration information and option 82 information to DHCP Relay Agent.

4）DHCP Relay Agent will peel the option 82 information from the replay message sent by DHCP server, and then forward the message with DHCP configuration information to the DHCP client.

4.2 DHCP option 82 Configuration Task List

1. Enabling the DHCP option 82 of the Relay Agent
2. Configure the DHCP option 82 attributes of the interface
3. Enable the DHCP option 82 of server
4. Configure DHCP option 82 default format of Relay Agent
5. Configure delimiter
6. Configure creation method of option82
7. Diagnose and maintain DHCP option 82

1. Enabling the DHCP option 82 of the Relay Agent.

Command	Explanation
Global mode	
ip dhcp relay information option **no ip dhcp relay information option**	Set this command to enable the option 82 function of the switch Relay Agent. The “no ip dhcp relay information option” is used to disable the option 82 function of the switch Relay Agent.

2. Configure the DHCP option 82 attributes of the interface

Command	Explanation
Interface configuration mode	

ip dhcp relay information policy {drop | keep | replace} **no ip dhcp relay information policy**	This command is used to set the retransmitting policy of the system for the received DHCP request message which contains option 82. 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 option 82 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".
ip dhcp relay information option subscriber-id {standard | <*circuit-id*>} **no ip dhcp relay information option subscriber-id**	This command is used to set the format of option 82 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 option 82 specified by users, which is a string no longer than 64characters. The" **no ip dhcp relay information option subscriber-id**" command will set the format of added option 82 sub-option1 (Circuit ID option) as standard format.
Global Mode	

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

3. Enable the DHCP option 82 of server.

Command	Explanation
Global mode	
ip dhcp server relay information enable **no ip dhcp server relay information enable**	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.

4. Configure DHCP option 82 default format of Relay Agent

Command	Explanation
Global mode	
ip dhcp relay information option subscriber-id format {hex | acsii | vs-hp}	Set subscriber-id format of Relay Agent option82.
ip dhcp relay information option remote-id format {default | vs-hp}	Set remote-id format of Relay Agent option82.

5. Configure delimiter

Command	Explanation
Global mode	
ip dhcp relay information option delimiter [colon | dot | slash | space] **no ip dhcp relay information option delimiter**	Set the delimiter of each parameter for suboption of option82 in global mode, no command restores the delimiter as slash.

6. Configure creation method of option82

Command	Explanation
Global mode	

ip dhcp relay information option self-defined remote-id {hostname | mac | string WORD} **no ip dhcp relay information option self-defined remote-id**	Set creation method for option82, users can define the parameters of remote-id suboption by themselves
ip dhcp relay information option self-defined remote-id format [ascii | hex]	Set self-defined format of remote-id for relay option82.
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**	Set creation method for option82, users can define the parameters of circute-id suboption by themselves
ip dhcp relay information option self-defined subscriber-id format [ascii | hex]	Set self-defined format of circuit-id for relay option82.

7. Diagnose and maintain DHCP option 82

Command	Explanation
Admin mode	
show ip dhcp relay information option	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 DHCP server option82 enabling switch.
debug ip dhcp relay packet	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.

4.3 DHCP option 82 Application Examples

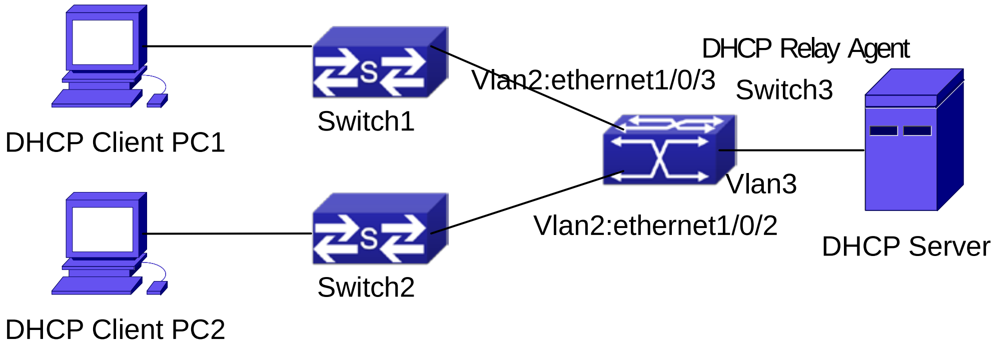


Fig 4-1 A DHCP option 82 typical application example

In the above example, layer 2 switches Switch1 and Switch2 are both connected to layer 3 switch Switch3, Switch 3 will transmit the request message from DHCP client to DHCP serer as DHCP Relay Agent. It will also transmit the reply message from the server to DHCP client to finish the DHCP protocol procedure. If the DHCP option 82 is disabled, DHCP server cannot distinguish that whether the DHCP client is from the network connected to Switch1 or Switch2. So, all the PC terminals connected to Switch1 and Switch2 will get addresses from the public address pool of the DHCP server. After the DHCP option 82 function is enabled, since the Switch3 appends the port information of accessing Switch3 to the request message from the client, the server can tell that whether the client is from the network of Swich1 or Swich2, and thus can allocate separate address spaces for the two networks, to simplify the management of networks.

The following is the configuration of Switch3(MAC address is 00:03:0f:02:33:01):

```
Switch3(Config)#service dhcp
Switch3(Config)#ip dhcp relay information option
Switch3(Config)#ip forward-protocol udp bootps
Switch3(Config)#interface vlan 3
Switch3(Config-if-vlan3)#ip address 192.168.10.222 255.255.255.0
Switch3(Config-if-vlan2)#ip address 192.168.102.2 255.255.255.0
Switch3(Config-if-vlan2)#ip helper 192.168.10.88
```

Linux ISC DHCP Server supports option 82, its configuration file /etc/dhcpd.con is

```
ddns-update-style interim;
ignore client-updates;

class "Switch3Vlan2Class1" {
match if option agent.circuit-id = "Vlan2+Ethernet1/0/2" and option
agent.remote-id=00:03:0f:02:33:01;
}

class "Switch3Vlan2Class2" {
match if option agent.circuit-id = "Vlan2+Ethernet1/0/3" and option agent.remote-id=00:03:0f:02:33:01;
}

subnet 192.168.102.0 netmask 255.255.255.0 {
option routers 192.168.102.2;
option subnet-mask 255.255.255.0;
option domain-name "example.com.cn";
option domain-name-servers 192.168.10.3;
authoritative;

pool {
range 192.168.102.21 192.168.102.50;
default-lease-time 86400; #24 Hours
max-lease-time 172800; #48 Hours
allow members of "Switch3Vlan2Class1";
}
pool {
range 192.168.102.51 192.168.102.80;
default-lease-time 43200; #12 Hours
max-lease-time 86400; #24 Hours
allow members of "Switch3Vlan2Class2";
}
}
```

Now, the DHCP server will allocate addresses for the network nodes from Switch1 which are relayed by Switch3 within the range of 192.168.102.21 ~ 192.168.102.50, and allocate addresses for the network nodes from Switch1 within the range of 192.168.102.51～192.168.102.80.

4.4 DHCP option 82 Troubleshooting

☞ DHCP option 82 is implemented as a sub-function module of DHCP Relay Agent. Before using it, users should make sure that the DHCP Relay Agent is configured correctly.

- ☞ DHCP option 82 needs the DHCP Relay Agent and the DHCP server cooperate to finish the task of allocating IP addresses. The DHCP server should set allocating policy correctly depending on the network topology of the DHCP Relay Agent, or, even the Relay Agent can operate normally, the allocation of addresses will fail. When there is more than one kind of Relay Agent, please pay attention to the retransmitting policy of the interface DHCP request messages.
- ☞ To implement the option 82 function of DHCP Relay Agent, the "debug dhcp relay packet" command can be used during the operating procedure, including adding the contents of option 82, the retransmitting policy adopted, the option 82 contents of the server peeled by the Relay Agent and etc., such information can help users to do troubleshooting.
- ☞ To implement the option 82 function of DHCP server, the "debug ip dhcp server packet" command can be used during the operating procedure to display the procedure of data packets processing of the server, including displaying the identified option 82 information of the request message and the option 82 information returned by the reply message.

Chapter 5 DHCP Snooping Configuration

5.1 Introduction to DHCP Snooping

DHCP Snooping means that the switch monitors the IP-getting process of DHCP CLIENT via DHCP protocol. It prevents DHCP attacks and illegal DHCP SERVER by setting trust ports and untrust ports. And the DHCP messages from trust ports can be forwarded without being verified. In typical settings, trust ports are used to connect DHCP SERVER or DHCP RELAY Proxy, and untrust ports are used to connect DHCP CLINET. The switch will forward the DCHP request messages from untrust ports, but not DHCP reply ones. If any DHCP reply messages is received from a untrust port, besides giving an alarm, the switch will also implement designated actions on the port according to settings, such as “shutdown”, or distributing a “blackhole”. If DHCP Snooping binding is enabled, the switch will save binding information (including its MAC address, IP address, IP lease, VLAN number and port number) of each DHCP CLINET on untrust ports in DHCP snooping binding table With such information, DHCP Snooping can combine modules like dot1x and ARP, or implement user-access-control independently.

Defense against Fake DHCP Server: once the switch intercepts the DHCP Server reply packets（including DHCPOFFER, DHCPACK, and DHCPNAK）, it will alarm and respond according to the situation（shutdown the port or send Black hole）。

Defense against DHCP over load attacks: To avoid too many DHCP messages attacking CPU, users should limit the DHCP speed of receiving packets on trusted and non-trusted ports.

Record the binding data of DHCP: DHCP SNOOPING will record the binding data allocated by DHCP SERVER while forwarding DHCP messages, it can also upload the binding data to the specified server to backup it. The binding data is mainly used to configure the dynamic users of dot1x user based ports. Please refer to the chapter called“dot1x configuration” to find more about the usage of dot1x use-based mode.

Add binding ARP: DHCP SNOOPING can add static binding ARP according to the binding data after capturing binding data, thus to avoid ARP cheating.

Add trusted users: DHCP SNOOPING can add trusted user list entries according to the parameters in binding data after capturing binding data; thus these users can access all resources without DOT1X authentication.

Automatic Recovery: A while after the switch shut down the port or send blockhole, it should automatically recover the communication of the port or source MAC and send information to Log Server via syslog.

LOG Function: When the switch discovers abnormal received packets or automatically recovers, it should send syslog information to Log Server.

The Encryption of Private Messages: The communication between the switch and the inner network security management system TrustView uses private messages. And the users can encrypt those messages of version 2.

Add authentication option82 Function: It is used **with dot1x** dhcpoption82 authentication mode. Different option 82 will be added in DHCP messages according to user's authentication status.

5.2 DHCP Snooping Configuration Task Sequence

1. Enable DHCP Snooping
2. Enable DHCP Snooping binding function
3. Enable DHCP Snooping binding ARP function
4. Enable DHCP Snooping option82 function
5. Set the private packet version
6. Set DES encrypted key for private packets
7. Set helper server address
8. Set trusted ports
9. Enable DHCP Snooping binding DOT1X function
10. Enable DHCP Snooping binding USER function
11. Adding static list entries function
12. Set defense actions
13. Enable the debug switch
14. Configure DHCP Snooping option 82 attributes

1. Enable DHCP Snooping

Command	Explanation
Globe mode	
ip dhcp snooping enable **no ip dhcp snooping enable**	Enable or disable the DHCP snooping function.

2. Enable DHCP Snooping binding

Command	Explanation
Globe mode	
ip dhcp snooping binding enable **no ip dhcp snooping binding enable**	Enable or disable the DHCP snooping binding function.

3. Enable DHCP Snooping binding ARP function

Command	Explanation
Globe mode	
ip dhcp snooping binding arp **no ip dhcp snooping binding arp**	Enable or disable the dhcp snooping binding ARP function.

4. Enable DHCP Snooping option82 function

Command	Explanation
Globe mode	
ip dhcp snooping information enable **no ip dhcp snooping information enable**	Enable/disable DHCP Snooping option 82 function.

5. Set the private packet version

Command	Explanation
Globe mode	
ip user private packet version two **no ip user private packet version two**	To configure/delete the private packet version.

6. Set DES encrypted key for private packets

Command	Explanation
Globe mode	
enable trustview key 0/7 <*password*> **no enable trustview key**	To configure/delete DES encrypted key for private packets.

7. Set helper server address

Command	Explanation
Globe mode	

ip user helper-address A.B.C.D [port <udpport>] source <ipAddr> (secondary|) **no ip user helper-address (secondary|)**	Set or delete helper server address.

8. Set trusted ports

Command	Explanation
Port mode	
ip dhcp snooping trust **no ip dhcp snooping trust**	Set or delete the DHCP snooping trust attributes of ports.

9. Enable DHCP SNOOPING binding DOT1X function

Command	Explanation
Port mode	
ip dhcp snooping binding dot1x **no ip dhcp snooping binding dot1x**	Enable or disable the DHCP snooping binding dot1x function.

10. Enable or disable the DHCP SNOOPING binding USER function

Command	Explanation
Port mode	
ip dhcp snooping binding user-control **no ip dhcp snooping binding user-control**	Enable or disable the DHCP snooping binding user function.

11. Add static binding information

Command	Explanation
Globe mode	

ip dhcp snooping binding user <*mac*> address <*ipAddr*> vlan **<*vid*> interface (ethernet|) <*ifname*>** **no ip dhcp snooping binding user <*mac*> interface (ethernet|) <*ifname*>**	Add/delete DHCP snooping static binding list entries.

12. Set defense actions

Command	Explanation
Port mode	
ip dhcp snooping action {shutdown|blackhole} [recovery <*second*>] **no ip dhcp snooping action**	Set or delete the DHCP snooping automatic defense actions of ports.

13. Enable the debug switch

Command	Explanation
Admin mode	
debug ip dhcp snooping packet **debug ip dhcp snooping event** **debug ip dhcp snooping update** **debug ip dhcp snooping binding**	Please refer to the chapter on system troubleshooting.

14. Configure DHCP Snooping option 82 attributes

Command	Explanation
Globe mode	
ip dhcp snooping information option subscriber-id format {hex | acsii | vs-hp}	This command is used to set subscriber-id format of DHCP snooping option82.
ip dhcp snooping information option remote-id {standard | <*remote-id*>} **no ip dhcp snooping information option remote-id**	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.

ip dhcp snooping information option delimiter [colon | dot | slash | space] **no ip dhcp snooping information option delimiter**	Set the delimiter of each parameter for suboption of option82 in global mode, no command restores the delimiter as slash.
ip dhcp snooping information option self-defined remote-id {hostname | mac | string WORD} **no ip dhcp snooping information option self-defined remote-id**	Set creation method for option82, users can define the parameters of remote-id suboption by themselves.
ip dhcp snooping information option self-defined remote-id format [ascii | hex]	Set self-defined format of remote-id for snooping option82.
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**	Set creation method for option82, users can define the parameters of circute-id suboption by themselves.
ip dhcp snooping information option self-defined subscriber-id format [ascii | hex]	Set self-defined format of circuit-id for snooping option82.
Port mode	
ip dhcp snooping information option subscriber-id {standard | <*circuit-id*>} **no ip dhcp snooping information option subscriber-id**	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.

Command	Explanation
Globe mode	

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

5.3 DHCP Snooping Typical Application

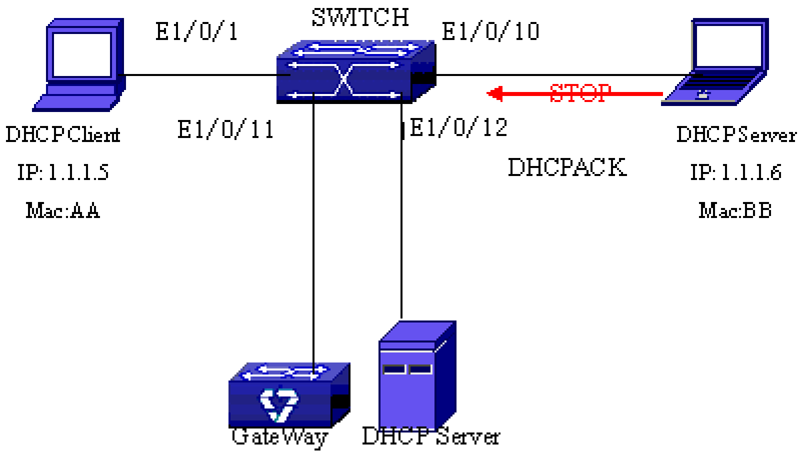


Fig 5-1 Sketch Map of TRUNK

As showed in the above chart, Mac-AA device is the normal user, connected to the non-trusted port 1/0/1 of the switch. It operates via DHCP Client, IP 1.1.1.5; DHCP Server and GateWay are connected to the trusted ports 1/0/11 and 1/0/12 of the switch; the malicious user Mac-BB is connected to the non-trusted port 1/0/10, trying to fake a DHCP Server（by sending DHCPACK）. Setting DHCP Snooping on the switch will effectively detect and block this kind of network attack.

Configuration sequence is:

```
switch#
switch#config
switch(config)#ip dhcp snooping enable
switch(config)#interface ethernet 1/0/11
switch(Config-Ethernet1/0/11)#ip dhcp snooping trust
switch(Config-Ethernet1/0/11)#exit
switch(config)#interface ethernet 1/0/12
switch(Config-Ethernet1/0/12)#ip dhcp snooping trust
switch(Config-Ethernet1/0/12)#exit
switch(config)#interface ethernet 1/0/1-10
switch(Config-Port-Range)#ip dhcp snooping action shutdown
switch(Config-Port-Range)#
```

5.4 DHCP Snooping Troubleshooting Help

5.4.1 Monitor and Debug Information

The “debug ip dhcp snooping” command can be used to monitor the debug information.

5.4.2 DHCP Snooping Troubleshooting Help

If there is any problem happens when using DHCP Snooping function, please check if the problem is caused by the following reasons:

☞ Check that whether the global DHCP Snooping is enabled;

☞ If the port does not react to invalid DHCP Server packets, please check that whether the port is set as a non-trusted port of DHCP Snooping.

Chapter 6 DHCPv6 Snooping Configuration

6.1 Introduction to DHCPv6 Snooping

DHCPv6 Snooping monitors the interaction flow of the packets between DHCPv6 client and server, so as to create the binding table of the user, and implement all kinds of security policies based on the binding table. DHCPv6 Snooping has the following functions:

6.1.1 Defense against Fake DHCPv6 Server

DHCPv6 Snooping can set the port of connecting DHCPv6 server as the trust port, other ports as the un-trusted ports by default, so as to avoid the user to configure DHCPv6 server privately in network. DHCPv6 Snooping does not forward DHCPv6 response packets which are received by the un-trusted ports, and according to the source MAC of the received DHCPv6 response packets to implement the security policy. For example, this MAC is set as a blackhole MAC within a period, or this port is directly shutdown within a period.

6.1.2 Defense against Fake IPv6 Address

DHCPv6 Snooping function can send the control list entries based the binding on the port. The port denies all IPv6 traffic by default, it only allows to forward IPv6 packets of which the IPv6 addresses and the MAC addresses are bound by this port as the source. In this way, it can effectively prevent the malicious user fake or privately set IPv6 address to access the network.

6.1.3 Defense against the attack of DHCPv6 addresses exhaustion

DHCPv6 Snooping can limit the binding number of the port. The port of which the binding number exceeds the threshold, does not forward and drop the after DHCPv6 application packets. In this way, it can effectively prevent the attack of DHCPv6 addresses exhaustion.

6.1.4 Defense against ND cheat

The IPv6 address obtained by DHCPv6 protocol can be trustier in IPv6 network, so DHCPv6 Snooping can convert the binding list entries to static one, and effectively prevent the attack of ND cheat to a gateway device. The function of binding ND for DHCPv6 Snooping needs to be enabled on the device of layer 3 gateway.

6.1.5 Reply the remove requirement for port

Through capturing the ports of DHCPv6 packets, DHCPv6 Snooping judges the port connected to the DHCPv6 user. After DHCPv6 Snooping binding is created, if DHCPv6 Snooping receives CONFIRM/REQUEST packets and response packets of DHCPv6 client from other ports, it needs to use DAD NS/NA to detect whether the binding of the original port is still usable, if it is still usable (that means to receive the response of DAD NA), then do not create new binding on new port, contrarily (that means the response of DAD NA is not received in set time), create the binding on new port and deletes the binding on the original port.

6.2 DHCPv6 Snooping Configuration Task Sequence

1. Enable DHCPv6 Snooping binding function
2. Enable DHCPv6 Snooping binding ND function
3. Delete dynamic binding information for DHCPv6 Snooping
4. Set the binding limitation number for the ports
5. Configure static binding list entries
6. Set trust ports
7. Set defense actions
8. Set the max number for Blackhole MAC
9. Enable user access control function
10. Enable the debug
11. Show the configuration status

1. Enable DHCPv6 Snooping binding function

Command	Explanation
Global mode	

ipv6 dhcp snooping binding enable **no ipv6 dhcp snooping binding enable**	Enable or disable DHCPv6 Snooping binding function.

2. Enable DHCPv6 Snooping binding ND function

Command	explanation
Global mode	
ipv6 dhcp snooping binding nd **no ipv6 dhcp snooping binding nd**	Enable or disable DHCPv6 Snooping binding ND function.

3. Delete dynamic binding information for DHCPv6 Snooping

Command	Explanation
Admin mode	
clear ipv6 dhcp snooping binding {<*MAC*> | <*ipv6address*> | interface {ethernet <*IFNAME*> | port-channel <*IFNAME*> | <*IFNAME*>} | all}	Delete the dynamic binding information for DHCPv6 Snooping.

4. Set the binding limitation number for the ports

Command	Explanation
Port mode	
ipv6 dhcp snooping binding-limit <*max-num*> **no ipv6 dhcp snooping binding-limit**	Set or delete the max number of DHCPv6 Snooping dynamic binding which is allowed to set up on the port.

5. Configure static binding list entries

Command	explanation
Global mode	

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*>**	Configure or delete the configured static binding list entries.

6. Set trust ports

Command	Explanation
Port mode	
ipv6 dhcp snooping trust **no ipv6 dhcp snooping trust**	Set or delete DHCPv6 Snooping trust attribute for the ports.

7. Set defense actions

Command	Explanation
Port mode	
ipv6 dhcp snooping action {shutdown | blackhole} [recovery <*second*>] **no ipv6 dhcp snooping action**	Set or delete the automatic defense actions of DHCPv6 Snooping for the ports.

8. Set the max number of Blackhole MAC

Command	Explanation
Global mode	
ipv6 dhcp snooping action {<*max-num*> | default}	Set the max number of blackhole MAC which can be sent by each un-trusted port.

9. Enable user access control function

Command	Explanation
Port mode	
ipv6 dhcp snooping binding user-control **no ipv6 dhcp snooping binding user-control**	Enable or disable the user access control function is bound by DHCPv6 Snooping.

10. Enable the debug switch

Command	Explanation
Admin mode	
debug ipv6 dhcp snooping packet **debug ipv6 dhcp snooping event** **debug ipv6 dhcp snooping binding**	Enable the debug of DHCP Snooping.

11. Show the configuration status

Command	Explanation
Admin mode	
show ipv6 dhcp snooping interface [ethernet | port-channel] <ifname> **show ipv6 dhcp snooping binding {<MAC> | <ipv6address> | interface [ethernet | port-channel] <ifname> | all}**	Show DHCP Snooping and binding information.

6.3 DHCPv6 Snooping Typical Application

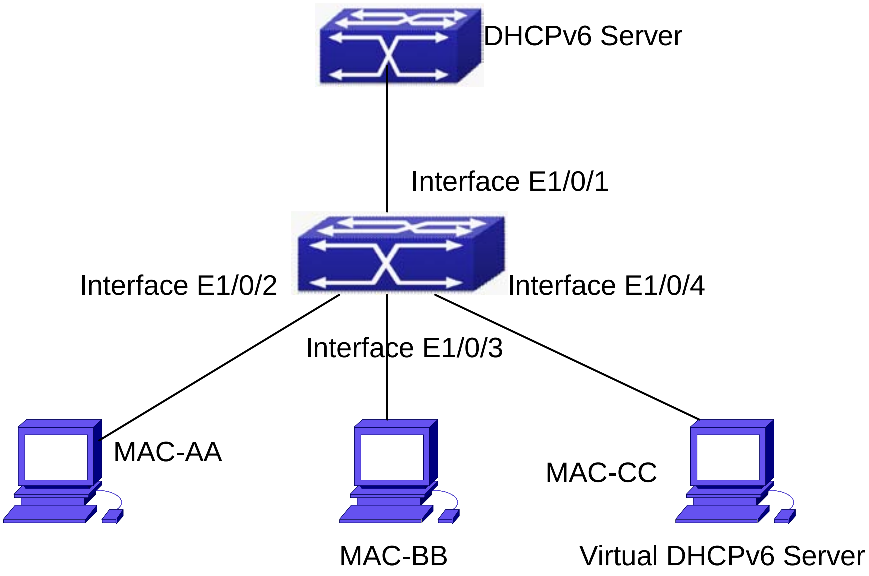


Fig 4-1 Sketch Map of preventing lawless DHCPv6 Server

As showed in the above chart, MAC-AA and MAC-BB devices are normal users, they are connected to the non-trusted ports 1/0/2 and 1/0/3 of the switch, and obtain IP 2010::3 and IP 2010::4 through DHCPv6 Client; DHCPv6 Server are connected to the trust port 1/0/1 of the switch; the malicious user Mac-CC is connected to the non-trusted port1/0/4, it tries to fake DHCPv6 Server. Setting DHCPv6 Snooping on the switch will effectively detect and prevent this kind of network attack.

Configuration sequence is:

```
switch#
switch#config
switch(config)#ipv6 dhcp snooping enable
switch(config)#ipv6 dhcp snooping binding enable
switch(config)#interface ethernet 1/0/1
switch(Config-Ethernet 1/0/1)#ipv6 dhcp snooping trust
switch(Config-Ethernet1/0/1)#exit
switch(config)#interface ethernet 1/0/4-10
switch(Config-Port-Range)#ipv6 dhcp snooping action shutdown
switch(Config-Port-Range)#
```

6.4 DHCPv6 Snooping Troubleshooting

6.4.1 Monitor and Debug Information

The “debug ipv6 dhcp snooping” command can be used to monitor the debug information.

6.4.2 DHCPv6 Snooping Troubleshooting Help

If there is any problem happens when using DHCPv6 Snooping function, please check whether the problem is caused by the following reasons:

- Check whether the DHCPv6 Snooping is enabled globally
- If DHCP client does not obtain IP when configuring DHCPv6 Snooping, please check whether the port connected by DHCPv6 server/relay is set as a trust port
- DHCPv6 Snooping is mutually exclusive to the following functions:
  - IPv6 flow redirect
  - IPv6 control multicast/ policy multicast IPv6 ACL
  - Configure QoS for IPv6 ACL

Chapter 7 DHCPv6 option 52

7.1 Introduction to DHCPv6 option 52

DHCPv6 Option52 is CAPWAP_AC_v6 option, it is used for DHCPv6 server issuing ipv6 wireless address list of wireless controller for AP. AP as DHCPv6 client fills in 52 (0x34) in option 6 (this option shows the DHCPv6 option which is requested by DHCPv6 client) of DHCPv6 Solicit packet, it means AP requests the content of option 52 (get the IPv6 address list of wireless controller through DHCPv6 server). After DHCPv6 server received Solicit packet from AP, it will analyze the option6 in it. If option6 appoints the option52 requested by client, the option52 message will be brought in the replied Advertise packet.

7.2 DHCPv6 option 52 Configuration Task List

1. Basic DHCPv6 option 52 configuration

Command	Explanation
Address pool configuration mode	
option 52 ascii LINE	Configure option 52 character string with ascii format in ipv6 dhcp pool mode.
option 52 hex WORD	Configure option 52 character string with hex format in ipv6 dhcp pool mode.
option52 ipv6 X:X::X:X	Configure option 52 character string with IPv6 format in ipv6 dhcp pool mode.
no option 52	Delete the configured option 52 in the address pool mode.

7.3 DHCPv6 option 52 Configuration Example

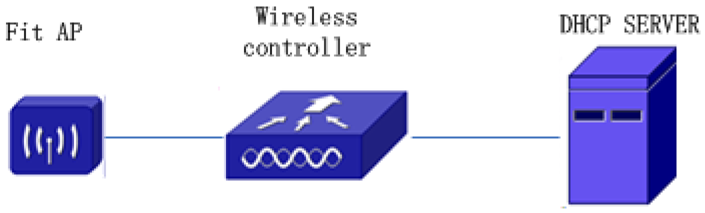


Fig 7-1 Typical DHCPv6 option52 topology

Fit AP obtains IPv6 address and option 52 attribute by DHCPv6 server to send unicast discovery request for wireless controller. DHCPv6 SERVER returns the option 52 property to FIT AP.

Configuration procedure:

# Configure DHCPv6 server

```
Switch (config)#ipv6 dhcp pool a
switch (dhcpv6-a-config)#option 52 ipv6 2001:1::100
```

7.4 DHCPv6 option 52 Troubleshooting

If problems occur when configuring DHCPv6 option 52, please check whether the problem is caused by the following reasons:

- Check whether service dhcp function is enabled.
- Check whether the string format of Option 52 is written correctly.