FSOS

DHCP Configuration

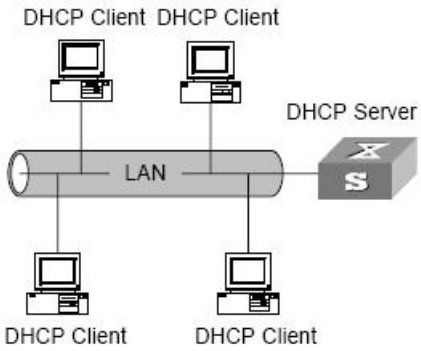
Contents

1. DHCP Configuration

1.1 DHCP Overview

With networks getting larger in size and more complicated in structure, lack of available IP addresses becomes the common situation the network administrators have to face, and network configuration becomes a tough task for the network administrators. With the emerging of wireless networks and the using of laptops, the position change of hosts and frequent change of IP addresses also require new technology. Dynamic host configuration protocol (DHCP) is developed in this background.

DHCP adopts a client/server model, where DHCP clients send requests to DHCP servers for configuration parameters; and the DHCP servers return the corresponding configuration information such as IP addresses to configure IP addresses dynamically. A typical DHCP application includes one DHCP server and multiple clients (such as PCs and laptops), as shown in Picture 1-1.



Picture 1-1. Typical DHCP application

1.2 DHCP IP Address Assignment

1.2.1 IP Address Assignment Policy

Currently, DHCP provides the following three IP address assignment policies to meet the requirements of different clients:

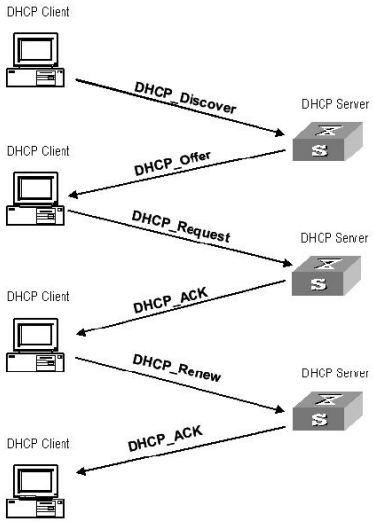
Manual assignment. The administrator statically binds IP addresses to few clients with special uses (such as WWW server). Then the DHCP server assigns these fixed IP addresses to the clients.

Automatic assignment. The DHCP server assigns IP addresses to DHCP clients. The IP addresses will be occupied by the DHCP clients permanently.

Dynamic assignment. The DHCP server assigns IP addresses to DHCP clients for predetermined period of time. In this case, a DHCP client must apply for an IP address at the expiration of the period. This policy applies to most clients.

1.2.2 Obtaining IP Addresses Dynamically

Interaction between a DHCP client and a DHCP server is as shown in Picture 1-2.



Picture 1-2. Interaction between a DHCP client and a DHCP server

There are three different modes for DHCP client to obtain IP address in different stage:

(1) Initial login for DHCP client

There are four stages for the initial login of DHCP client:

- Discover. In this phase, the DHCP client tries to find a DHCP server by broadcasting a DHCP-DISCOVER packet.

- Offer. In this phase, the DHCP server offers an IP address. Each DHCP server that receives the DHCP-DISCOVER packet chooses an unassigned IP address from the address pool based on the IP address assignment policy and then broadcasts a DHCP-OFFER packet to the DHCP client.

- Select: In this phase, the DHCP client selects an IP address. If more than one DHCP server sends DHCP-OFFER packets to the DHCP client, the DHCP client only accepts the DHCP-OFFER packet that first arrives, and then broadcasts a DHCP-REQUEST packet containing the assigned IP address carried in the DHCP-OFFER packet.

- Acknowledge: Upon receiving the DHCP-REQUEST packet, the DHCP server returns a DHCP-ACK packet to the DHCP client to confirm the assignment of the IP address to the client. When the client receives the DHCP-ACK packet, it broadcasts an ARP packet with the assigned IP address as the destination address to detect the assigned IP address, and uses the IP address only if it does not receive any response within a specified period.

The IP addresses offered by other DHCP servers (if any) are not used by the DHCP client and are still available to other clients.

(2) The next login for DHCP client

When DHCP client relogin, there are two types of situation:

➢ The last-assigned IP address is not occupied. Broadcast a DHCP-REQUEST packet containing the assigned IP address, the DHCP server returns a DHCP-ACK packet to the DHCP client to confirm the assignment of the IP address to the client.

➢ The last-assigned IP address is occupied. Broadcast a DHCP-REQUEST packet containing the assigned IP address, the DHCP server returns a DHCP-NAK packet to refuse the assignment of the IP address to the client. The client will re-send DHCP_Discover packet to request a new IP address.

(3) Updating IP Address Lease

After a DHCP server dynamically assigns an IP address to a DHCP client, the IP address keeps valid only within a specified lease time and will be reclaimed by the DHCP server when the lease expires. If the DHCP client wants to use the IP address for a longer time, it must update the IP lease.

By default, a DHCP client updates its IP address lease automatically by unicasting a DHCP-REQUEST packet to the DHCP server when half of the lease time elapses. The DHCP server responds with a DHCP-ACK packet to notify the DHCP client of a new IP lease if the server can assign the same IP address to the client. Otherwise, the DHCP server responds with a DHCP-NAK packet to notify the DHCP client that the IP address will be reclaimed when the lease time expires.

If the DHCP client fails to update its IP address lease when half of the lease time elapses, it will update its IP address lease by broadcasting a DHCP-REQUEST packet to the DHCP server again when seven-eighths of the lease time elapses. The DHCP server performs the same operations as those described in the previous section.

1.2.3 DHCP Packet Format

DHCP has eight types of packets. They have the same format, but the values of some fields in the packets are different. The DHCP packet format is based on that of the BOOTP packets. The following table describes the packet format (the number in the brackets indicates the field length, in bytes):

<table>
<tr><td>op(1)</td><td>htype(1)</td><td>hlen(1)</td><td>hops(1)</td></tr>
<tr><td colspan="4">Xid(4)</td></tr>
<tr><td colspan="2">secs(2)</td><td colspan="2">flags(2)</td></tr>
<tr><td colspan="4">ciaddr(4)</td></tr>
<tr><td colspan="4">yiaddr(4)</td></tr>
<tr><td colspan="4">siaddr(4)</td></tr>
<tr><td colspan="4">chaddr(16)</td></tr>
<tr><td colspan="4">sname(64)</td></tr>
<tr><td colspan="4">file(128)</td></tr>
<tr><td colspan="4">option(variable)</td></tr>
</table>

Picture 1-3. DHCP packet format

The field meanings are illustrated as follows:

op: Operation types of DHCP packets: 1 for request packets and 2 for response packets.

htype, hlen: Hardware address type and length of the DHCP client.

hops: Number of DHCP relays which a DHCP packet passes. For each DHCP relay that the DHCP request packet passes, the field value increases by 1.

xid: Random number that the client selects when it initiates a request. The number is used to identify an address-requesting process.

secs: Elapsed time after the DHCP client initiates a DHCP request.

flags: The first bit is the broadcast response flag bit. It is used to identify that the DHCP response packet is sent in the unicast or broadcast mode. Other bits are reserved.

ciaddr: IP address of a DHCP client.

yiaddr: IP address that the DHCP server assigns to a client.

siaddr: IP address of the DHCP server.

giaddr: IP address of the first DHCP relay that the DHCP client passes after it sent the request packet.

chaddr: Hardware address of the DHCP client.

sname: Name of the DHCP server.

file: Name of the start configuration file that the DHCP server specifies for the DHCP client.

option: Optional variable-length fields, including packet type, valid lease time, IP address of a DNS server, and IP address of the WINS server.

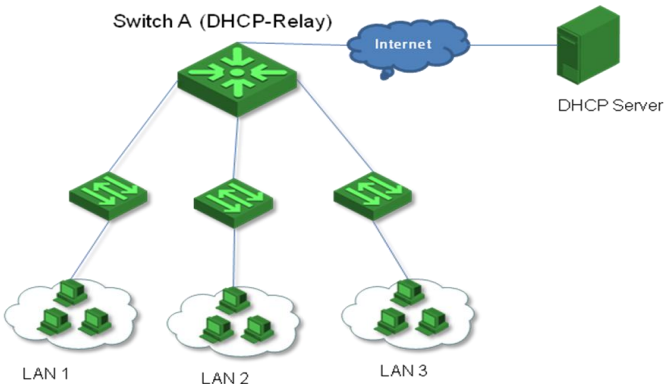
1.3 DHCP Relay

1.3.1 Usage of DHCP Relay

Since the packets are broadcasted in the process of obtaining IP addresses, DHCP is only applicable to the situation that DHCP clients and DHCP servers are in the same network segment, that is, you need to deploy at least one DHCP server for each network segment, which is far from economical.

DHCP Relay is designed to address this problem. It enables DHCP clients in a subnet to communicate with the DHCP server in another subnet so that the DHCP clients can obtain IP addresses. In this case, the DHCP clients in multiple networks can use the same DHCP server, which can decrease your cost and provide a centralized administration.

1.3.2 DHCP Relay Fundamentals



Picture 1-4. Typical DHCP relay application

DHCP relays can transparently transmit broadcast packets on DHCP clients or servers to the DHCP servers or clients in other network segments.

In the process of dynamic IP address assignment through the DHCP relay, the DHCP client and DHCP server interoperate with each other in a similar way as they do without the DHCP relay. The following sections only describe the forwarding process of the DHCP relay. For the interaction process of the packets, see 1.2.2 Obtaining IP Addresses Dynamically.

The DHCP client broadcasts the DHCP-DISCOVER packet.

After receiving the packets, the network device providing the DHCP relay function unicasts the packet to the designated DHCP server based on the configuration.

The DHCP server assigns IP addresses, and then broadcasts the configuration information to the client through the DHCP relay. The sending mode is determined by the flag in the DHCP-DISCOVER packets from the client. For detailed information, refer to section 1.3 DHCP Packet Format.

1.4 Configure DHCP Relay

Table 1-1 Configure DHCP Relay

Operation	Command	Remarks
Enter global configuration mode	**configure terminal**	-
Enable DHCP Relay	**dhcp-relay**	required
Enter vlan configuration mode	**vlan** <*vid*>	required
Configure vlan ipaddres	**interface ip <ip> <mask> <gateway>**	required
Configure vlan DHCP server	**dhcpserver { ip | backupip } <ip>**	required

2. DHCP Snooping

2.1 Introduction to DHCP Snooping

For the sake of security, the IP addresses used by online DHCP clients need to be tracked for the administrator to verify the corresponding relationship between the IP addresses the DHCP clients obtained from DHCP servers and the MAC addresses of the DHCP clients. Switches can track DHCP client IP addresses through the DHCP snooping function, which listens DHCP broadcast packets.

DHCP snooping listens the following two types of packets to retrieve the IP addresses the DHCP clients obtain from DHCP servers and the MAC addresses of the DHCP clients:

DHCP-ACK packet

DHCP-REQUEST packet

When an unauthorized DHCP server exists in the network, a DHCP client may obtains an illegal IP address. To ensure that the DHCP clients obtain IP addresses from valid DHCP servers, you can specify a port to be a trusted port or an untrusted port by the DHCP snooping function.

Trusted ports can be used to connect DHCP servers or ports of other switches. Untrusted ports can be used to connect DHCP clients or networks.

Untrusted ports drop the DHCP-ACK and DHCP-OFFER packets received from DHCP servers. Trusted ports forward any received DHCP packets to ensure that DHCP clients can obtain IP addresses from valid DHCP servers.

2.2 DHCP Snooping Configuration

Perform following commands in global configuration mode.

Table 1-1 Configure the DHCP snooping function

Operation	Command	Description
Enable DHCP-Snooping	**dhcp-snooping**	By default, DHCP-Snooping is disabled.
Enter interface configuration mode	**interface Ethernet** *port_id (device/slot/port)*	
Configure port connected to DHCP server direction to be Trust	**dhcp-snooping trust**	By default, all ports are untrust port.

2.3 DHCP-Snooping Security Configuration

2.3.1 Configure Max Clients Number

A private DHCP server on a network also answers IP address request packets and assigns IP addresses to DHCP clients. However, the IP addresses they assigned may conflict with those of other hosts. As a result, users cannot normally access networks. This kind of DHCP servers are known as private DHCP servers. Therefore, administrators can:

Restrict the DHCP-Client number connected to switch port. So only the clients connected to the same port with the attacker will suffer the attack.

Restrict the DHCP-Client number in specified VLAN. So only the clients in the same VLAN with the attacker will suffer the attack.

This function should be work with DHCP-Snooping. Perform following commands in interface configuration mode.

Table 1-2Configure max clients number

Operation	Command	Description
Configure max DHCP-Client number connected to switch port	**dhcp-snooping max-clients** *<0-2048>*	By default, the max DHCP-Client number connected to switch port is 2048.
Enter VLAN mode	**vlan** *vlan_list*	
Configure max DHCP-Client number in specified VLAN.	**dhcp-snooping max-clients** *<0-2048>*	By default, the max DHCP-Client number in specified VLAN is 2048.

2.3.2 Configure IP-Source-Guard

IP Source Guard provides source IP address filtering on a Layer 2 port to prevent a malicious host from impersonating a legitimate host by assuming the legitimate host's IP address. The feature uses dynamic DHCP snooping and static IP source binding to match IP addresses to hosts on untrusted Layer 2 access ports. When using IP-Source-Guard, pay attention:

- DHCP-Snooping has been enabled
- Use this function in Trust port

After enabling IP-Source-Guard, all traffic with that IP source address is permitted from that trusted client. Traffic from other hosts is denied. This filtering limits a host's ability to attack the network by claiming a neighbor host's IP address. The filtering info can be source MAC, source IP and source port number.

Perform following commands in global configuration mode:

Table 1-3Configure IP-Source-Guard

Operation	Command	Description
Configure IP-source-guard bind table	**ip-source-guard bind {ip** *A.B.C.D* **|mac** *HH:HH:HH:HH:HH:HH* **|interface ethernet** device-num<0>/slot-num<0-2>/port-num<1-48>}	-
Enter interface configuration mode	**interface ethernet** *device/slot/port*	-
Enable IP-Source-Guard on Trust port	**ip-source-guard**	By default, ip-source-guard on port is disabled.

Caution:

IP source guard filters packets based on the following types of binding entries:

- Source IP
- Source IP + source MAC
- Source IP + source MAC + source port

2.4 Displaying and Debugging DHCP-Snooping

After the above configurations, you can verify the configurations by executing the show command in any configuration mode.

Table 1-4 Displaying and Debugging DHCP-Snooping

Operation	Command
Display DHCP-Snooping clients	**show dhcp-snooping clients**
Display DHCP-Snooping status in interface	**show dhcp-snooping interface** [ethernet device-num<0>/slot-num<0-2>/port-num<1-48>]
Display DHCP-Snooping status in VLAN	**show dhcp-snooping vlan**
Display IP-Source-Guard status in interface	**show ip-source-guard**
Display source IP binding table of IP-Source-Guard	**show ip-source-guard bind [ip** *A.B.C.D***]**

2.5 DHCP-Snooping Configuration Example

I. Network requirements

As shown in Picture 1-6, the GigabitEthernet0/0/1 port of Switch is connected to DHCP Server. A network segment containing some DHCP clients is connected to the GigabitEthernet 0/0/2 port of Switch.

The DHCP snooping function is enabled on Switch.

The GigabitEthernet1/0/1 port of Switch is a trusted port.

II. Network diagram

Picture 1-5. DHCP-Snooping Configuration Example

III. Configuration procedure

All following commands are performed in Switch acting as a DHCP-Snooping device.

1. Enter global configuration mode

Switch#configure terminal

Switch(config)#

2. Enable DHCP-Snooping

Switch(config)#dhcp-snooping

Config DHCP Snooping successfully.

3. Enter interface configuration mode of Ethernet0/0/1

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

4. Set Ethernet0/0/1 to be Trust

Switch(config-if-ethernet-0/0/1)#dhcp-snooping trust

Config DHCP Snooping mode of port successfully.

3. DHCP Option 82

3.1 Introduction to option 82 supporting

Option: A length-variable field in DHCP packets, carrying information such as part of the lease information and packet type. It includes at least one option and at most 255 options.

Option 82: Also known as relay agent information option. This option is a part of the Option field in DHCP packet. According to RFC3046, option 82 lies before option 255 and after the other options. Option 82 includes at least one sub-option and at most 255 sub-options. Currently, the commonly used sub-options in option 82 are sub-option 1 and sub-option 2.

Sub-option 1: A sub-option of option 82. Sub-option 1 represents the agent circuit ID, namely Circuit ID. It holds the port number and VLAN-ID of the switch port connected to the DHCP client, and is usually configured on the DHCP relay. Generally, sub-option 1 and sub-option 2 must be used together to identify information about a DHCP source.

Sub-option 2: A sub-option of option 82. Sub-option 2 represents the remote agent ID, namely Remote ID. It holds the MAC address of the DHCP relay, and is usually configured on the DHCP relay. Generally, sub-option 1 and sub-option 2 must be used together to identify information about a DHCP source.

3.2 DHCP Option82 Configuration

3.2.1 Enable DHCP Option82

To enable option 82, you need to perform the corresponding configuration on the DHCP server and the DHCP relay.

If the packet contains option 82, the DHCP relay processes the packet depending on the configured policy:

- Drop: Specifies to discard the DHCP request packets that carry option 82.
- Keep: Specifies to remain the DHCP request packets that carry option 82 unchanged.
- Replace: Specifies to replace the option 82 carried by a DHCP request packet with that of the DHCP relay.

Perform following commands in global configuration mode:

Table 1-5Enable DHCP Option82

Operation	Command	Description
Enable DHCP Option82	**dhcp option82**	By default, DHCP Option82 is disabled.
Enter interface configuration mode	**interface Ethernet** *port_id (device/slot/port)*	
Configure the strategy for the	**dhcp option82 strategy**	By default, the DHCP

DHCP relay to process request packets containing option 82	{*drop*|*keep*|*replace*}	relay replaces the option 82 carried by a DHCP request packet with its own option 82.

3.2.2 Displaying and Debugging DHCP Option82

Table 1-6 Displaying and Debugging DHCP Option82

Operation	Command
Display DHCP option82	**show dhcp option82**