DHCP Technology White Paper

Keywords: DHCP, BOOTP, DHCP server, DHCP relay agent, DHCP client, DHCP snooping, DHCP security

Abstract: This document covers DHCP basic concepts, features, and networking solutions provided by H3C Technology Co., Ltd.

Acronyms:

Acronym	Full spelling
DHCP	Dynamic Host Configuration Protocol
BOOTP	Bootstrap Protocol
ARP	Address Resolution Protocol
Option 82	DHCP Relay Agent Information Option
TFTP	Trivial File Transfer Protocol

Table of Contents

1 Overview

1.1 Background

To send and receive data on the Internet, a host needs an IP address and other information such as gateway address and DNS server address, which can be obtained through the Bootstrap Protocol (BOOTP).

BOOTP is built on a client-server model. A diskless client contacts a BOOTP server to obtain such information as IP address, server IP address, boot image filename, and gateway IP address.

BOOTP was designed for stable networks where each host gets a permanent network connection. The administrator configures a BOOTP configuration file that contains a set of parameters for each BOOTP client. Because the configuration is seldom changed, the configuration file remains unchanged accordingly for several weeks.

The fast expansion and growing complexity of networks result in scarce IP addresses assignable to hosts. Meanwhile, as many people need to take their laptops across networks, the IP addresses need be changed accordingly. As a result, related configurations on hosts become more complex.

BOOTP cannot solve these problems. Therefore, the Dynamic Host Configuration Protocol (DHCP) was introduced by IETF to provide a mechanism for assigning IP addresses dynamically.

1.2 Benefits

DHCP is an enhanced version of BOOTP. It also adopts the client/server model. The DHCP server assigns network configuration parameters to DHCP clients.

DHCP supports three mechanisms for IP address allocation:

- Manual allocation: The network administrator assigns an IP address to a client like a WWW server, and DHCP conveys the assigned address to the client.
- Automatic allocation: DHCP assigns a permanent IP address to a client.

- Dynamic allocation: DHCP assigns an IP address to a client for a limited period of time, which is called a lease. The client should apply for a new IP address upon lease expiration.

The network administrator can select any of the three mechanisms as needed.

DHCP enhances BOOTP in the following two aspects.

- Fast and dynamic IP address allocation. The network administrator needs to configure a DHCP server to provide a group of IP addresses, called an address pool. Once a host is attached to the network, it communicates with the DHCP server to apply for an IP address. Then, the DHCP server selects an IP address from the configured address pool and assigns the IP address to the host.
- More network configuration information for clients.

2 Introduction to DHCP

2.1 Related Terms

- DHCP server: A DHCP server assigns IP addresses and other network configuration parameters to the DHCP clients.
- DHCP client: A DHCP client obtains an IP address and other network configuration parameters from a DHCP server. It is the initiator of an IP address allocation.
- DHCP relay agent: A DHCP relay agent forwards DHCP messages between a DHCP server and DHCP clients. In this way, the clients need not be located on the same network as the DHCP server.
- DHCP snooping: A DHCP snooping device can record the IP-to-MAC bindings from the received DHCP-ACK and DHCP-REQUEST messages.

2.2 DHCP Message Format

Figure 1 gives the DHCP message format.

Figure 1 DHCP message format

The fields in the DHCP message are described as follows:

- op: Message type defined in option field. 1 = REQ UEST, 2 =REPLY
- htype: Hardware address type.
- hlen: Hardware address length. This field is only applicable to Ethernet and has a fixed length of 6.
- hops: Number of relay agents a request message has traveled.
- xid: Transaction ID, a random number chosen by the client to identify an IP address allocation.
- secs: Filled in by the client, the number of seconds elapsed since the client began address acquisition or renewal process. Currently this field is reserved and set to 0.
- flags: The leftmost bit is defined as the BROADCAST (B) flag. If this flag is set to 0, the DHCP server sent a reply back by unicast; if this flag is set to 1, the DHCP server sent a reply back by broadcast. The remaining bits of the flags field are reserved for future use.
- ciaddr: Client IP address.
- yiaddr: 'your' (client) IP address, assigned by the server.
- siaddr: Server IP address, from which the clients obtained configuration parameters.
- giaddr: IP address of the first relay agent a request message traveled.
- chaddr: Client hardware address.

- sname: Server name, from which the client obtains configuration parameters.
- file: Bootfile name and routing information, defined by the server to the client.
- options: Optional parameters field that is variable in length, which includes the message type, lease, DNS IP address, WINS IP address and so forth.

2.3 Operation of DHCP

Because DHCP messages are broadcast, the DHCP server and clients must be on the same subnet; otherwise, a DHCP relay agent need be used to convey DHCP messages.

The DHCP server and client interact with each other regardless of whether a relay agent exists in between. The following section describes the operation of DHCP in a network where the DHCP server and clients are on the same subnet. For information about the operation of the DHCP relay agent, see section Operation of DHCP Relay Agent.

2.3.1 Dynamic IP Address Allocation Process

A DHCP client obtains a valid IP address from a DHCP server via four steps:

(1) Discovering: The client locates a DHCP server.

(2) Offering: A DHCP server offers configuration parameters such as an IP address to the client.

(3) Selecting: The client selects an IP address assigned by one of the DHCP servers.

(4) Acknowledging: The DHCP server confirms the offered IP address.

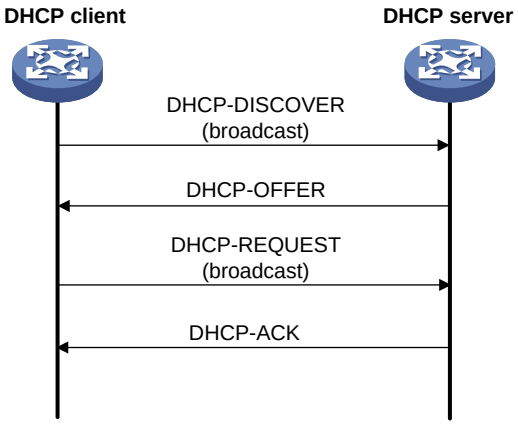

Figure 2 Dynamic IP address allocation process

Figure 2 illustrates the dynamic IP address allocation steps which are described as follows:

1. Discovering

The DHCP client broadcasts a DHCP-DISCOVER message to locate a DHCP server.

Since the DHCP server is unknown to the client, the client needs to broadcast a DHCP-DISCOVER message. All the DHCP servers send replies to the client upon receiving the DHCP-DISCOVER message.

2. Offering

A DHCP server that receives the DHCP-DISCOVER message offers an appropriate IP address with a lease and other configuration parameters (such as gateway IP address and DNS server address) to the client in a DHCP-OFFER message.

The DHCP server maintains assignable IP addresses and other configuration information in an address pool.

A DHCP server assigns an IP address to a client according to the following sequence:

- The IP address manually bound to the client's MAC address or ID
- The IP address that was ever assigned to the client
- The IP address designated by the Option 50 field in the DHCP-DISCOVER message from the client
- The first assignable IP address found in a proper DHCP address pool
- The IP address that was conflicting or passed its lease duration

If no IP address is assignable, the server will not respond.

When assigning an IP address, a DHCP server needs to confirm that the IP address to be assigned is not used by any other device by sending ICMP Echo Request (ping) packets. If the server does not get any response within a specified period, it will ping the IP address once again until a specified number of ping packets are sent. If still no response is received, the server will assign the IP address to the requesting client; otherwise, the IP address will be marked as a conflicting IP address, and the server will choose another IP address.

3. Selecting

If several DHCP servers send DHCP-OFFER messages to the client, the client accepts the first received offer, and broadcasts it in a DHCP-REQUEST message containing Option 54 (the server ID option) to formally request the IP address.

The client broadcasts the DHCP-REQUEST message to notify all the DHCP servers that it will use the IP address offered by the DHCP server specified in Option 54. In this way, other DHCP servers can reclaim the IP addresses they offered to the client.

4. Acknowledging

Upon receiving the DHCP-REQUEST message from the DHCP client, the DHCP server checks the lease record corresponding to the MAC address in the message. If the lease record exists, the server returns a DHCP-ACK message, confirming that the IP address has been allocated to the client. If no such a record exists or the IP address cannot be assigned, the DHCP server returns a DHCP-NAK message, denying the IP address allocation; in this case, the client needs to broadcast a DHCP-DISCOVER message again to apply for another IP address.

After the client receives the DHCP-ACK message, it will probe whether the IP address assigned by the server is in use by broadcasting a gratuitous ARP packet. If the client receives no response within a specified time, it will use this IP address. Otherwise, the client sends a DHCP-DECLINE message to the server to request an IP address again.

2.3.2 Applying for the IP Address Once Assigned

A DHCP client does not send a DHCP-DISCOVER message when it access the network again; instead, it directly sends a DHCP-REQUEST message containing the IP address (specified in Option 50) previously assigned to it. The DHCP server determines whether the client can use the IP address:

(1) If the requested IP address is usable, the DHCP server returns a DHCP-ACK message, and then the DHCP client can use the IP address for communication, as shown in Figure 3 .

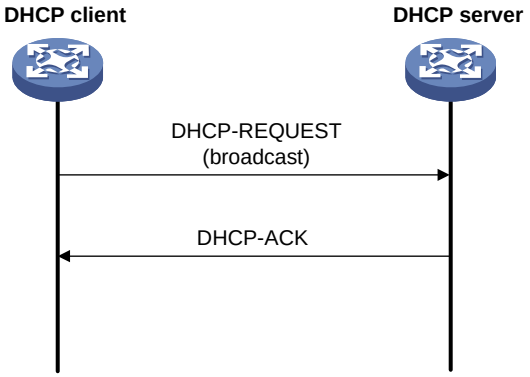

Figure 3 The IP address is usable

(2) If the IP address cannot be assigned to the requesting client (possibly because the IP address is already assigned to another DHCP client), the DHCP server returns a DHCP-NAK message. Then, the client needs to send a DHCP-DISCOVER message to request another IP address, as shown in Figure 4 .

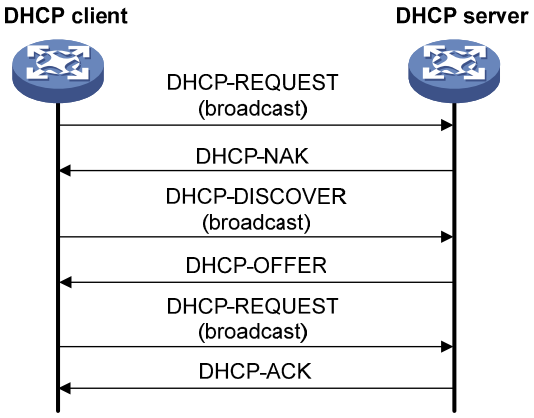

Figure 4 The IP address is unusable

2.3.3 Updating IP Address Lease

The IP address dynamically allocated by a DHCP server to a client has a lease. After the lease duration elapses, the IP address will be reclaimed by the DHCP server. If the client wants to use the IP address again, it has to extend the lease duration.

(1) After the half lease duration (T1) elapses, the DHCP client will send a DHCP-REQUEST unicast message to extend the lease duration. Based upon availability of the IP address, the DHCP server returns a DHCP-ACK unicast confirming that the client's lease duration has been extended, or a DHCP-NAK unicast denying the request.

(2) If the client receives no reply after 87.5% of the lease duration (T2) elapses, it will broadcast another DHCP-REQUEST message for lease extension. The DHCP server will handle the request as above mentioned.

As shown in Figure 5 , when 87.5% of the lease duration elapses, the DHCP client broadcasts a DHCP-REQUEST message. If the DHCP client receives a DHCP-ACK message from the DHCP server, the lease is updated successfully.

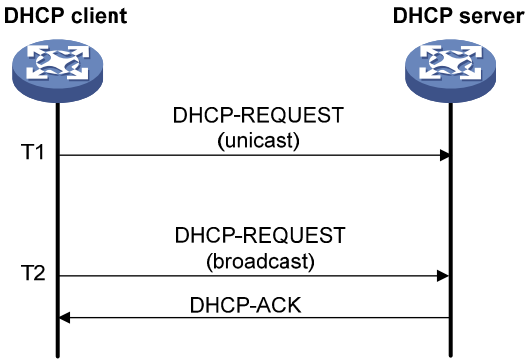

Figure 5 IP address lease extension process

2.3.4 Releasing an IP Address

When a DHCP client need not use its IP address, it sends a DHCP-RELEASE message to notify the DHCP server to release the IP address. The DHCP server will maintain the configuration information for the client to reclaim when it applies for an IP address again.

2.3.5 Applying for Additional Configuration Information

To obtain other configuration information besides an IP address from the DHCP server, the DHCP client sends a DHCP-INFORM message with Option 55 (parameter request list option) to specify the requested configuration parameters.

Upon receiving the DHCP-INFORM message, the DHCP server assigns the requested network parameters to the client through a DHCP-ACK message.

2.4 Operation of DHCP Relay Agent

Since DHCP requests are broadcast, the DHCP server and clients must be on the same subnet. Therefore, a DHCP server must be available on each subnet. It is not

practical.

The DHCP relay agent feature solves the problem. Via a DHCP relay agent, DHCP clients communicate with a DHCP server on another subnet to obtain configuration parameters. Thus, DHCP clients on different subnets can contact the same DHCP server.

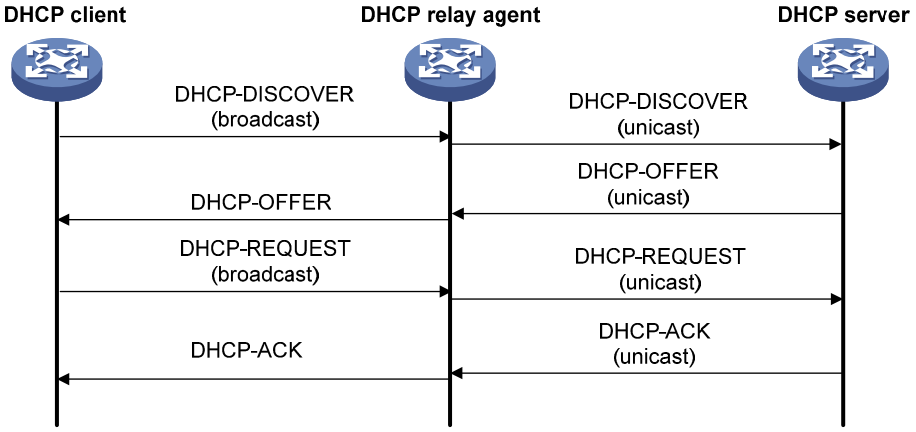

Figure 6 DHCP relay agent working process

Figure 6 illustrates the operation of a DHCP relay agent. After receiving a DHCP request from a DHCP client, the DHCP relay agent processes the request message and forwards the message to the designated DHCP server. Based on the specific information provided in the message, the DHCP server returns corresponding configuration parameters to the relay agent, which conveys them to the client.

(1) Upon receiving a DHCP-DISCOVER or DHCP-REQUEST message, the DHCP relay agent will do the following:

- If the value of the hops field exceeds the upper limit, the DHCP relay agent discards the DHCP request; if not, the DHCP relay agent checks the giaddr field. If the giaddr field is 0, the DHCP relay agent fills this field with the IP address of the interface that received the request. If the receiving interface has multiple IP addresses, it selects one to fill the giaddr field. If the giaddr field is not 0, it will not be modified.
- Then the relay agent increases the value of the hops field by one, which means the message has traveled another DHCP relay agent.

- It sets the TTL value in the request message to its default TTL value, instead of decreasing the value by one. The problems of loops and hop limit can be solved through the hops field.
- It changes the destination IP address in the DHCP request message to the IP address of the DHCP server or the next DHCP relay agent.

(2) Based on the giaddr field, the DHCP server returns an IP address and other configuration parameter to the relay agent, which then does the following:

- The DHCP relay agent assumes all the replies are to be sent to the directly connected DHCP clients. The giaddr field in a reply message identifies the interface directly connected to the client. If the giaddr is not a local interface's IP address, the DHCP relay agent discards the reply.
- Then the relay agent checks the broadcast flag in the reply message. If this flag is set to 1, the DHCP server broadcasts the reply to the DHCP client; otherwise, the DHCP server unicasts the reply to the DHCP client, with the destination IP address being yiaddr and link layer address being chaddr.

2.5 Limitations of DHCP

(1) If there are multiple DHCP servers on a network, one DHCP server does not know which IP addresses have been assigned by the other DHCP servers.

(2) DHCP clients cannot communicate with a DHCP server on another subnet without a DHCP relay agent.

3 DHCP Extended Functions

3.1 DHCP Relay Agent Security Feature

With the DHCP relay agent security feature enabled, the DHCP relay agent records IP-to-MAC bindings of DHCP clients (including dynamic or manual client entry addition, manual client entry deletion and query) and works together with the ARP module to block the unauthorized clients from accessing external networks.

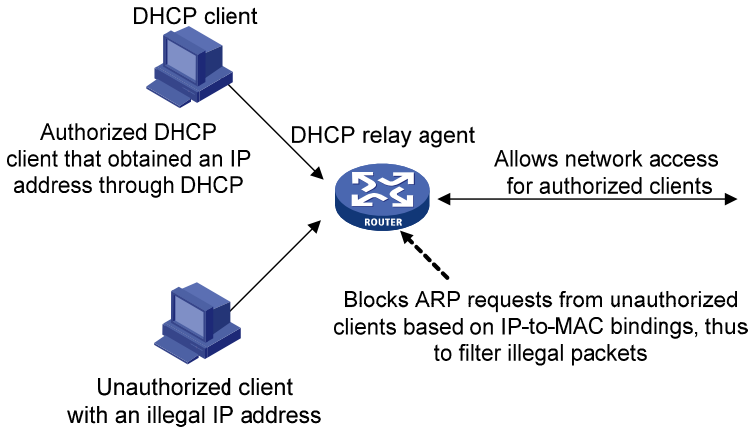

Figure 7 DHCP security function

As shown in Figure 7 , the DHCP relay agent security feature is described as follows:

(1) Maintaining IP-to-MAC bindings

All authorized clients are recorded in the binding table maintained by the DHCP relay agent.

The DHCP relay agent can dynamically record clients' IP-to-MAC bindings after they get IP addresses. It also supports static bindings, which means you can manually configure IP-to-MAC bindings on the DHCP relay agent, so that users can access external networks using fixed IP addresses.

The DHCP relay agent also supports manually deleting and querying the IP-to-MAC bindings.

(2) Blocking unauthorized clients from accessing external networks

This function is implemented in cooperation with ARP. If an ARP request fails to match any IP-to-MAC binding, the DHCP relay agent does not return an ARP reply.

(3) Aging function

Some Layer 3 devices cannot process DHCP-RELEASE messages sent from DHCP clients because they directly forward unicasts packets instead of delivering them to the CPU. Thus, when a DHCP client relinquishes an IP address, the DHCP relay agent still maintains the IP-to-MAC binding of the client. To solve this, the device uses the handshake function to age out DHCP binding entries.

With the handshake function, the DHCP relay agent uses the IP address of a client

and the MAC address of the DHCP relay interface to regularly send a DHCP-REQUEST message to the DHCP server. Upon receiving the request, the DHCP server returns a DHCP-ACK or DHCP-NAK message.

- If the server returns a DHCP-ACK message, which means the IP address has been released, the DHCP relay agent will age out the corresponding client entry.
- If the server returns a DHCP-NAK message, which means the IP address is still in use, the relay agent will not age it out.

Some DHCP servers may not return any message to the DHCP relay agent if the lease of the requested IP address expires. In this case, you can set the maximum number of times for sending a DHCP-REQUEST message. If the DHCP server does not return any message after the number is reached, the DHCP relay agent considers the lease expires and ages out the corresponding entry.

3.2 DHCP Snooping

3.2.1 DHCP Snooping Basic Functions

A DHCP snooping enabled device records clients' MAC and IP addresses by reading the DHCP-REQUEST and DHCP-ACK messages to implement the security feature.

3.2.2 DHCP Snooping Trusted/Untrusted Ports

If there is an unauthorized DHCP server on a network, the DHCP clients may obtain invalid IP addresses. To solve the problem, the ports of a DHCP snooping device can be configured as trusted or untrusted.

- Trusted: A trusted port is connected to an authorized DHCP server directly or indirectly. It forwards DHCP messages normally to guarantee that DHCP clients can obtain valid IP addresses.
- Untrusted: An untrusted port is connected to an unauthorized DHCP server. The DHCP-ACK, DHCP-NAK, and DHCP-OFFER packets received from the port are discarded to prevent DHCP clients from receiving invalid IP addresses.

3.3 DHCP Option 82 Functions

Because the traditional DHCP relay agent feature does not support Option 82, the IP addresses obtained by the DHCP clients in the same VLAN have the same privilege.

Thus, the network administrator cannot implement differentiated control over different users in the VLAN. This becomes a challenge to network security.

The DHCP relay agent option (Option 82) is defined in RFC 3046. The DHCP relay agent can add Option 82 to a DHCP request and send it the DHCP server, so that the DHCP server can locate the DHCP client to provide an individual configuration parameter assignment policy. Option 82 involves two sub-options: sub-option 1 (Circuit ID) and sub-option 2 (Remote ID).

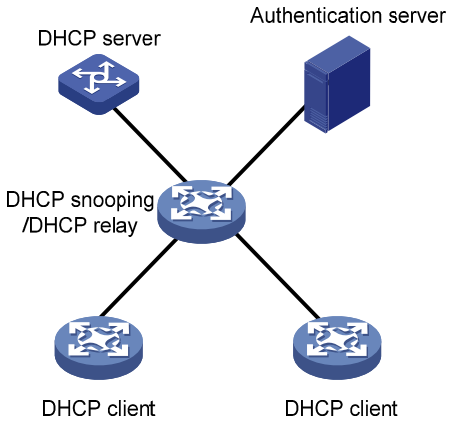

Figure 8 Operation of Option 82

As shown in Figure 8 , Option 82 works as follows:

(1) Before a DHCP client passes the authentication and dynamically obtains an IP address, only authentication packets and DHCP packets can pass the DHCP snooping device/DHCP relay agent.

(2) The client sends an authentication request to the authentication server through the DHCP snooping device/DHCP relay agent.

(3) After verifying the user's validity, the authentication server returns an authentication reply with the client's privilege to the client.

(4) After passing the authentication, the client sends a request with Option 82 containing the privilege information to the DHCP server.

(5) The DHCP server that supports Option 82 assigns an IP address based on the client's privilege to the client.

By cooperating with Option 82 and the authentication system, the DHCP server can assign IP addresses with different privileges to the clients based on the circuit ID and remote ID sub-options defined in Option 82. This helps manage IP addresses more

accurately, implement policy routing based on source IP addresses, and provide users with different network access rights.

Currently, both the DHCP snooping and DHCP relay agent features support Option 82.

3.4 Autoconfiguration Function

The autoconfiguration function allows a device to obtain a configuration file from a remote server when starting up without any configuration file. It works as follows:

The starting device sets an interface (such as the VLAN-interface 1 or the first Ethernet interface) as the DHCP client to request from the DHCP server parameters such as the IP address and name of a TFTP server, and a bootfile name. After getting such parameters, the DHCP client will send a TFTP request to obtain the configuration file from the specified TFTP server for system initialization. If the client cannot get such parameters, it will perform system initialization without loading any configuration file.

4 Application Scenarios

4.1 Address Allocation on the Same Network

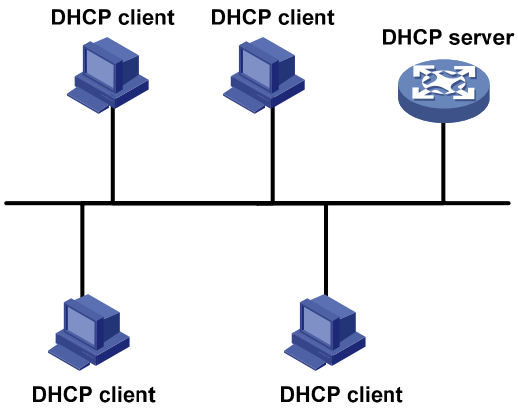

Figure 9 Address allocation on the same network

In the above figure, the DHCP clients dynamically obtain IP addresses and other configuration parameters from the DHCP server on the same network.

You need to configure the address pool and the corresponding interface IP address of the DHCP server to be in the same network segment.

4.2 Cross-Network Address Allocation

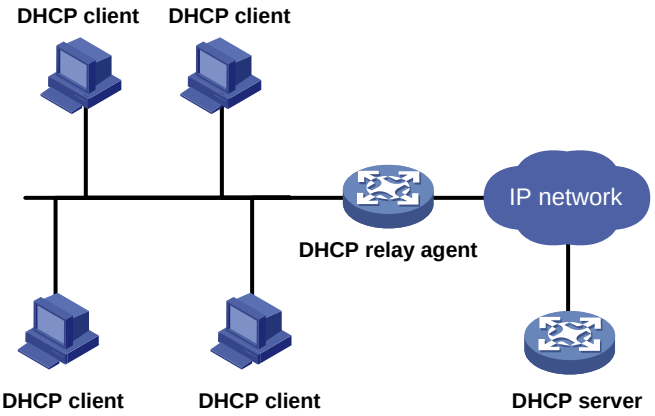

Figure 10 Cross-network address allocation

In the above figure, the DHCP server and the clients reside on different subnets. The clients obtain IP addresses and other network parameters from the DHCP server via a DHCP relay agent.

You need to configure the corresponding interface IP address of the DHCP relay agent and the address pool of the DHCP server to be in the same network segment; otherwise, the IP addresses obtained by DHCP clients may belong to a different network from the gateway, resulting in communication failures. You also need to configure a route to the relay agent on the DHCP server.

4.3 DHCP Snooping Configuration

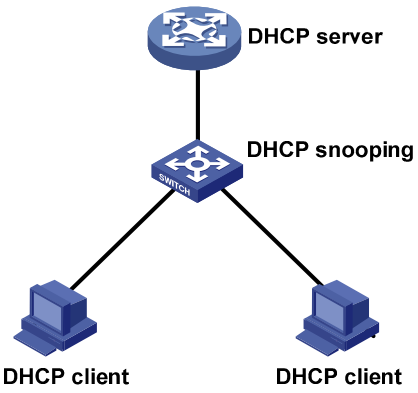

Figure 11 Application of Option 82

In the above figure, the DHCP clients obtain IP addresses from the DHCP server on the same subnet via a DHCP snooping device. After receiving a DHCP request from a client, the DHCP snooping device adds Option 82 to the request message, so that the DHCP server can assign an IP address based on the location information of the DHCP client.

By default, all the ports on a DHCP snooping device are untrusted ports. You need to configure the port connected with the DHCP server as a trusted port; otherwise, DHCP response messages cannot be forwarded to the DHCP clients.

4.4 Autoconfiguration Configuration

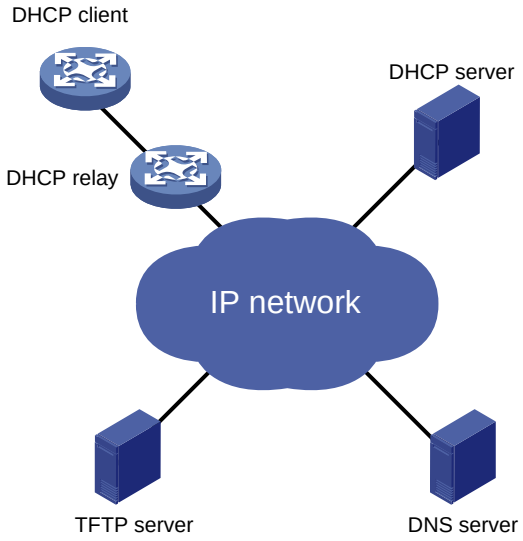

Figure 12 Autoconfiguration application

When a DHCP client starts up without any configuration file, it obtains an IP address, a TFTP server address and a bootfile name from the DHCP server, and then obtains a configuration file from the TFTP server.

4.5 DHCP Comprehensive Configuration

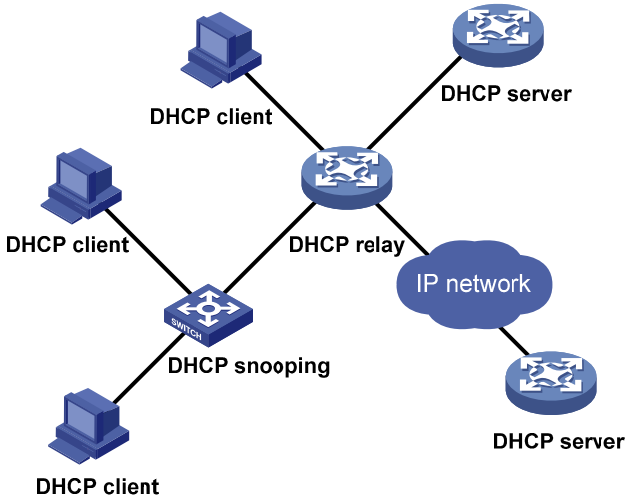

Figure 13 DHCP comprehensive configuration

As shown in Figure 13 , the DHCP clients obtain IP addresses from a DHCP server

that resides on another subnet. DHCP snooping is used to improve security at Layer 2.

5 Summary and Prospects

The DHCP features of H3C, which are implemented based on RFC 2131 and RFC 2132, support the following DHCP basic and extended functions: DHCP client/BOOTP client, DHCP relay agent, DHCP server, DHCP security, DHCP snooping and DHCP autoconfiguration.

With the fast expansion and growing complexity of networks, DHCP will be used in various network environments. H3C provides complete, flexible and convenient DHCP networking solutions for customers by involving a series of products, which have the following features:

- Full range of functionality, including DHCP client, DHCP relay agent, and DHCP server functions
- Excellent service capability and flexible networking schemes
- Good serviceability and configurability
- Interoperability with devices of mainstream vendors, such as Windows or Linux servers
- Easy management, economical deployment and low cost

6 References

- RFC 951: BOOTSTRAP PROTOCOL(BOOTP)
- RFC 1497: BOOTP Vendor Information Extensions
- RFC 2131: Dynamic Host Configuration Protocol(DHCP)
- RFC 2132: DHCP Options and BOOTP Vendor Extensions