DHCP Messages

The following list includes types of messages that can be sent between DHCP clients and servers.

DHCPDiscover

Broadcast by a DHCP client when it first attempts to connect to the network. The DHCPDiscover message requests IP address information from a DHCP server.

DHCPOffer

Broadcast by each DHCP server that receives the client DHCPDiscover message and has an IP address configuration to offer to the client. The DHCPOffer message contains an unleased IP address and additional TCP/IP configuration information, such as the subnet mask and default gateway. More than one DHCP server can respond with a DHCPOffer message. The client accepts the best offer, which for a Windows DHCP client is the first DHCPOffer message that it receives.

DHCPRequest

Broadcast by a DHCP client after it selects a DHCPOffer. The DHCPRequest message contains the IP address from the DHCPOffer that it selected. If the client is renewing or rebinding to a previous lease, this packet might be unicast directly to the server.

DHCPAck

Broadcast by a DHCP server to a DHCP client acknowledging the DHCPRequest message. At this time, the server also forwards any options. Upon receipt of the DHCPAck, the client can use the leased IP address to participate in the TCP/IP network and complete its system startup. This message is typically broadcast, because the DHCP client does not officially have an IP address that it can use at this point. If the DHCPAck is in response to a DHCPInform, then the message is unicast directly to the host that sent the DHCPInform message.

DHCPRelease

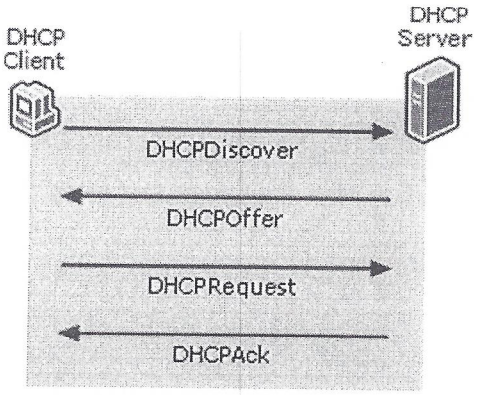
Sent by a DHCP client to a DHCP server, relinquishing an IP address and canceling the remaining lease. This is unicast to the server that provided the lease.

DHCP Lease Process

Obtaining a New Lease

A DHCP client initiates a conversation with a DHCP server when it is seeking a new lease, renewing a lease, rebinding, or restarting. The DHCP conversation consists of a series of DHCP messages passed between the DHCP client and DHCP servers. The following figure shows an overview of this process when the DHCP server and DHCP client are on the same subnet.

DHCP Lease Process Overview



1. The DHCP client requests an IP address by broadcasting a DHCPDiscover message to the local subnet.

2. The client is offered an address when a DHCP server responds with a DHCPOffer message containing an IP address and configuration information for lease to the client. If no DHCP server responds to the client request, the client sends DHCPDiscover messages at intervals of 0, 4, 8, 16, and 32 seconds, plus a random interval of between -1 second and 1 second. If there is no response from a DHCP server after one minute, the client can proceed in one of two ways:

    - If the client is using the Automatic Private IP Addressing (APIPA) alternate configuration, the client self-configures an IP address for its interface.

    - If the client does not support alternate configuration, such as APIPA, or if IP auto-configuration has been disabled, the client network initialization fails.

    In both cases, the client begins a new cycle of DHCPDiscover messages in the background every five minutes, using the same intervals as before (0, 4, 8, 16, and 32 seconds), until it receives a DHCPOffer message from a DHCP server.

3. The client indicates acceptance of the offer by selecting the offered address and broadcasting a DHCPRequest message in response.

4. The client is assigned the address and the DHCP server broadcasts a DHCPAck message in response, finalizing the terms of the lease.

When the client receives acknowledgment, it configures its TCP/IP properties by using the DHCP option information in the reply, and completes its initialization of TCP/IP.

In rare cases, a DHCP server might return a negative acknowledgment to the client. This can happen if a client requests an invalid or duplicate address. If a client receives a negative acknowledgment (DHCPNack), the client must begin the entire lease process again.

When the DHCP client and the DHCP server are on the same IP broadcast subnet, the DHCPDiscover, DHCPOffer, DHCPRequest, and DHCPAck messages are sent to identify clients by means of IP-level broadcasts sent to the limited broadcast address and the media access control (MAC) broadcast address.

When the DHCP server and DHCP client are not on the same subnet either a router or a host on the DHCP client's subnet must act as a DHCP relay agent to support the forwarding of DHCP messages between the DHCP client and the DHCP server.

Renewing a Lease

The DHCP client first attempts to renew its lease when 50 percent of the original lease time, known as *T1*, has passed. At this point the DHCP client sends a unicast DHCPRequest message to the DHCP server that originally granted its lease. If the server is available, and the lease is still available, the server responds with a unicast DHCPAck message and the lease is renewed.

If the original DHCP server is available, but the client's current lease is no longer available, the DHCP server responds with a DHCPNack message, and the client immediately starts the process to obtain a new lease. This can happen if the client has changed subnets or if the DHCP server cannot fulfill the lease request for some other reason.

If there is no response from the DHCP server, the client waits until 87.5 percent of the lease time has passed (known as *T2*). At T2, the client enters the rebinding state, and broadcasts a DHCPRequest message to attempt to renew the lease from any available DHCP server. If no DHCP server is available by the time the lease expires, the client immediately unbinds itself from the existing lease and starts the process to obtain a new lease, beginning with a DHCPDiscover message.

Preventing Address Conflicts

Client Conflict Detection

After the DHCP client receives a lease from the DHCP server, the client sends an Address Resolution Protocol (ARP) request to the address that it has been assigned. If a reply to the ARP request is received, the client has detected a conflict and sends a DHCPDecline message to the DHCP server. The DHCP server attaches a BAD_ADDRESS value to the IP address in the scope for the length of the lease. The client then begins the lease process again, and is offered the next available address in the scope.

Note

- ARP requests do not traverse routers. Clients use ARP requests rather than pings (ICMP Echo messages) because pings require the sender to have an IP address.

Server Conflict Detection

If your network includes older DHCP clients that do not perform conflict detection themselves, you can enable conflict detection on the DHCP server.

To detect conflicts, the DHCP server pings (sends an ICMP Echo message to) an IP address before offering that address to clients in a new lease. The DHCP server only pings addresses that have not been successfully and previously leased. If a client requests a lease on an IP address that it already had or is requesting a renewal, the DHCP server does not ping the IP address.

If conflict detection is enabled, an administrator-defined number of pings are sent. The server waits 1 second for a reply. Because the time required for a client to obtain a lease is equal to the number of pings used, choose this value carefully because it directly impacts the overall performance of the server. In general, one ping is sufficient.

If a response to the ping is received, a conflict is registered and that address is not offered to clients requesting a lease from the server. The DHCP server then attaches a BAD_ADDRESS value to that IP address in the scope. The DHCP server then tries to lease the next available address. If the duplicate address is removed from the network, the BAD_ADDRESS value attached to the IP address can be deleted from the scope's list of active leases, and then the address returns to the pool. Addresses are marked as BAD_ADDRESS for the length of the lease for which the scope is configured. If the BAD_ADDRESS entry is not manually removed, it will automatically be removed after a period of time equal to the lease time for the scope.

APIPA

Short for ***A**utomatic **P**rivate **IP** **A**ddressing*, a feature of later Windows operating systems. With APIPA, DHCP clients can automatically self-configure an IP address and subnet mask when a DHCP server isn't available. When a DHCP client boots up, it first looks for a DHCP server in order to obtain an IP address and subnet mask. If the client is unable to find the information, it uses APIPA to automatically configure itself with an IP address from a range that has been reserved especially for Microsoft. The IP address range is 169.254.0.1 through 169.254.255.254. The client also configures itself with a default class B subnet mask of 255.255.0.0. A client uses the self-configured IP address until a DHCP server becomes available.

The APIPA service also checks regularly for the presence of a DHCP server (every five minutes, according to Microsoft). If it detects a DHCP server on the network, APIPA stops, and the DHCP server replaces the APIPA networking addresses with dynamically assigned addresses.

APIPA is meant for nonrouted small business environments, usually less than 25 clients.