2019

Computer Networks

DHCP Server Documentation

Student: Enachi Vasile

Professor: Nicolae Botezatu

Introduction

The Dynamic Host Configuration Protocol (DHCP) is the host configuration protocol currently used on modern TCP/IP internetworks. It was based on BOOTP and is similar to its predecessor in many respects, including the use of request/reply message exchanges and a nearly identical message format. However, DHCP includes added functionality, the most notable of which is dynamic address assignment, which allows clients to be assigned IP addresses from a shared pool managed by a DHCP server.

DHCP Address Assignment and Allocation Methods

DHCP defines three basic mechanisms for address assignment.

- **Dynamic allocation** is the method most often used, and it works by having each client lease an address from a DHCP server for a period of time. The server chooses the address dynamically from a shared address pool.
- **Automatic allocation** is like dynamic allocation, but the address is assigned permanently instead of being leased.
- **Manual allocation** preassigns an address to a specific device, just as *BOOTP* does, and is normally used only for servers and other permanent, important hosts.

DHCP Leases

DHCP's most significant new feature is dynamic allocation, which changes the way that IP addresses are managed. Where in traditional IP each device owns a particular IP address, in DHCP the server owns all the addresses in the address pool, and each client leases an address from the server, usually for only a limited period of time.

A key decision that a network administrator using DHCP must make is what the network's lease length policy will be. Longer leases allow devices to avoid changing addresses too often; shorter leases are more efficient in terms of reallocating addresses that are no longer required. An administrator can choose from a variety of different lease times and may choose longer leases for some devices than for others.

DHCP Lease Life Cycle Phases

DHCP leases follow a conceptual life cycle. The lease is first assigned to the client through a process of allocation; if the device later reboots, it will reallocate the lease. After a period of time controlled by the renewal timer (T1), the device will attempt to renew its lease with the server that allocated it. If this fails, the rebinding timer (T2) will go off, and the device will attempt to rebind the lease with any available server. The client may also release its IP address if it no longer needs it.

Lease Address Ranges (Scopes)

Each DHCP server maintains a set of IP addresses that it uses to allocate leases to clients. These are usually contiguous blocks of addresses assigned to the server by an administrator, called DHCP *address ranges* or *scopes*.

DHCP Address Management

If a site has multiple DHCP servers, they can be set up with either overlapping or non-overlapping scopes. Overlapping scopes allow each server to assign from the same pool, providing flexibility, but raising the

possibility of two clients being assigned the same address unless a feature such as server conflict detection is employed. non-overlapping scopes are safer because each server has a dedicated set of addresses for its use, but this means one server could run out of addresses while the other still has plenty, and if a server goes down, its addresses will be temporarily unallocatable.

DHCP Server Responsibilities

DHCP servers are devices programmed to provide DHCP services to clients. They manage address information and other parameters and respond to client configuration requests.

- **Address Storage and Management** DHCP servers are the owners of the addresses used by all DHCP clients. The server stores the addresses and manages their use, keeping track of which addresses have been allocated and which are still available.
- **Configuration Parameter Storage and Management** DHCP servers also store and maintain other parameters that are intended to be sent to clients when requested. Many of these are important configuration values that specify in detail how a client is to operate.
- **Lease Management DHCP** servers use leases to dynamically allocate addresses to clients for a limited time. The DHCP server maintains information about each of the leases it has granted to clients, as well as policy information such as lease lengths.
- **Response to Client Requests** DHCP servers respond to different types of requests from clients to implement the DHCP communication protocol. This includes assigning addresses; conveying configuration parameters; and granting, renewing, and terminating leases.
- **Administration Services** To support all of its other responsibilities, the DHCP server includes functionality to allow a human administrator to enter, view, change, and analyze addresses, leases, parameters, and all other information needed to run DHCP.

DHCP Lease Allocation, Reallocation, and Renewal

➢ Initial Lease Allocation Process

The most important configuration process in DHCP is the lease allocation process, used by clients to acquire a lease. The client broadcasts a request to determine if any DHCP servers can hear it. Each DHCP server that is willing to grant the client a lease sends it an offer. The client selects the lease it prefers and sends a response to all servers telling them its choice. The selected server then sends the client its lease information.

➢ DHCP Lease Reallocation Process

If a client starts up and already has a lease, it does not need to go through the full lease allocation process; instead, it can use the shorter reallocation process. The client broadcasts a request to find the server that has the current information on its lease. That server responds back to confirm that the client's lease is still valid.

➢ DHCP Lease Renewal and Rebinding Processes

Each client's lease has associated with it a renewal timer (T1), normally set to 50 percent of the length of the lease, and a rebinding timer (T2), usually set to 87.5 percent of the lease length. When the T1 timer goes off, the client will try to renew its lease by contacting the server that originally granted it. If the client cannot renew the lease by the time the T2 timer expires, it will broadcast a rebinding request to any available server. If the lease is not renewed or rebound by the time the lease expires, the client must start the lease allocation process over again.

- **DHCP Parameter Configuration Process for Clients with Non-DHCP Addresses**

Devices that are not using DHCP to acquire IP addresses can still use its other configuration capabilities. A client can broadcast a DHCPINFORM message to request that any available server send it parameters for how the network is to be used. DHCP servers respond with the requested parameters and/or default parameters, carried in DHCP options of a DHCPACK message.

DHCP Message Generation, Addressing, Transport, and Retransmission

Requests from BOOTP clients are normally sent broadcast, to reach any available DHCP server. However, there are certain exceptions, such as in lease renewal, when a request is sent directly to a known server. DHCP servers can send their replies either broadcast to the special port number reserved for DHCP clients or unicast using layer 2. The DHCP standards specify that layer 2 delivery should be used when possible to avoid unnecessary broadcast traffic.

Like BOOTP, DHCP uses UDP for transport, which does not provide any reliability features. DHCP clients must detect when requests are sent and no response is received, and retransmit requests periodically. Special logic is used to prevent clients from sending excessive numbers of requests during difficult network conditions.

DHCP takes BOOTP's vendor information extensions and formalizes them into an official feature called DHCP options. The BOOTP Vendor Specific Area field becomes the DHCP Options field, and it can contain an arbitrary number of parameters to be sent from the server to the client. Some of these include pieces of data that are actually mandatory for the successful operation of DHCP. There are several dozen DHCP options, which are divided into functional categories.

DHCP Server Implementations

The server maintains the configuration database, keeps track of address ranges, and manages leases. For this reason, DHCP servers are typically much more complex than DHCP clients. In essence, without a DHCP server, there really is no DHCP. Thus, deciding how to implement DHCP servers is a large part of implementing the protocol. A classic DHCP server consists of DHCP server software running on a server hardware platform of one sort or another. A DHCP server usually will not be a dedicated computer, except on very large networks. It is more common for a hardware server to provide DHCP services along with performing other functions, such as acting as an application server, serving as a general database server, providing DNS services, and so forth. So, a DHCP server does not need to be a special computer; any device that can run a DHCP server implementation can act as a server. In fact, the DHCP server may not even need to be a host computer at all. Today, many routers include DHCP functionality. Programming a router to act as a DHCP server allows clients that connect to the router to be automatically assigned IP addresses. This provides numerous potential advantages in an environment where a limited number of public IP addresses is shared among multiple clients, or where IP Network Address Translation (NAT; see Chapter 28) is used to dynamically share a small number of addresses. Since DHCP requires a database, a router that acts as a DHCP server requires some form of permanent storage. This is often implemented using flash memory on routers; "true" servers use hard disk storage.

DHCP Server Software Features

- How clients can be grouped and managed
- How they allow address ranges (scopes) to be defined
- The level of control an administrator has over parameters returned to a client
- The level of control an administrator has over general operation of the protocol, such as specification of the T1 and T2 timers and other variables, and how leases are allocated and renewals handled
- Security features
- Ability to interact with DNS to support dynamic device naming
- Optional features such as BOOTP support, conflict detection, and Automatic
- Private IP Addressing (all discussed later in this chapter)

To permit DHCP clients and DHCP servers to reside on different physical networks, an intermediary device is required to facilitate message exchange between networks. DHCP uses the same mechanism for this as BOOTP: the deployment of BOOTP **relay agents**. The relay agent captures client requests, forwards them to the server, and then returns the server's responses back to the client.

APIPA Operation Autoconfiguration/Automatic Private IP Addressing

An optional DHCP feature called Automatic Private IP Addressing (APIPA) was developed to allow clients to still be able to communicate in the event that they are unable to obtain an IP address from a DHCP server. When enabled, the client chooses a random address from a special reserved block of private IP addresses and checks to make sure the address is not already in use by another device. It continues to check for a DHCP server periodically until it is able to find one.

DHCP Server Conflict Detection

Some DHCP implementations include a feature called server conflict detection. When this feature is activated, it causes each server to always check to make sure an address is not in use before granting it to a client. When conflict detection is used by all DHCP servers on a network, the servers can be given overlapping scopes, so each can assign any of the organization's IP addresses, while at the same time not needing to be concerned about two clients being assigned the same address by different servers.

DHCP Security Concerns

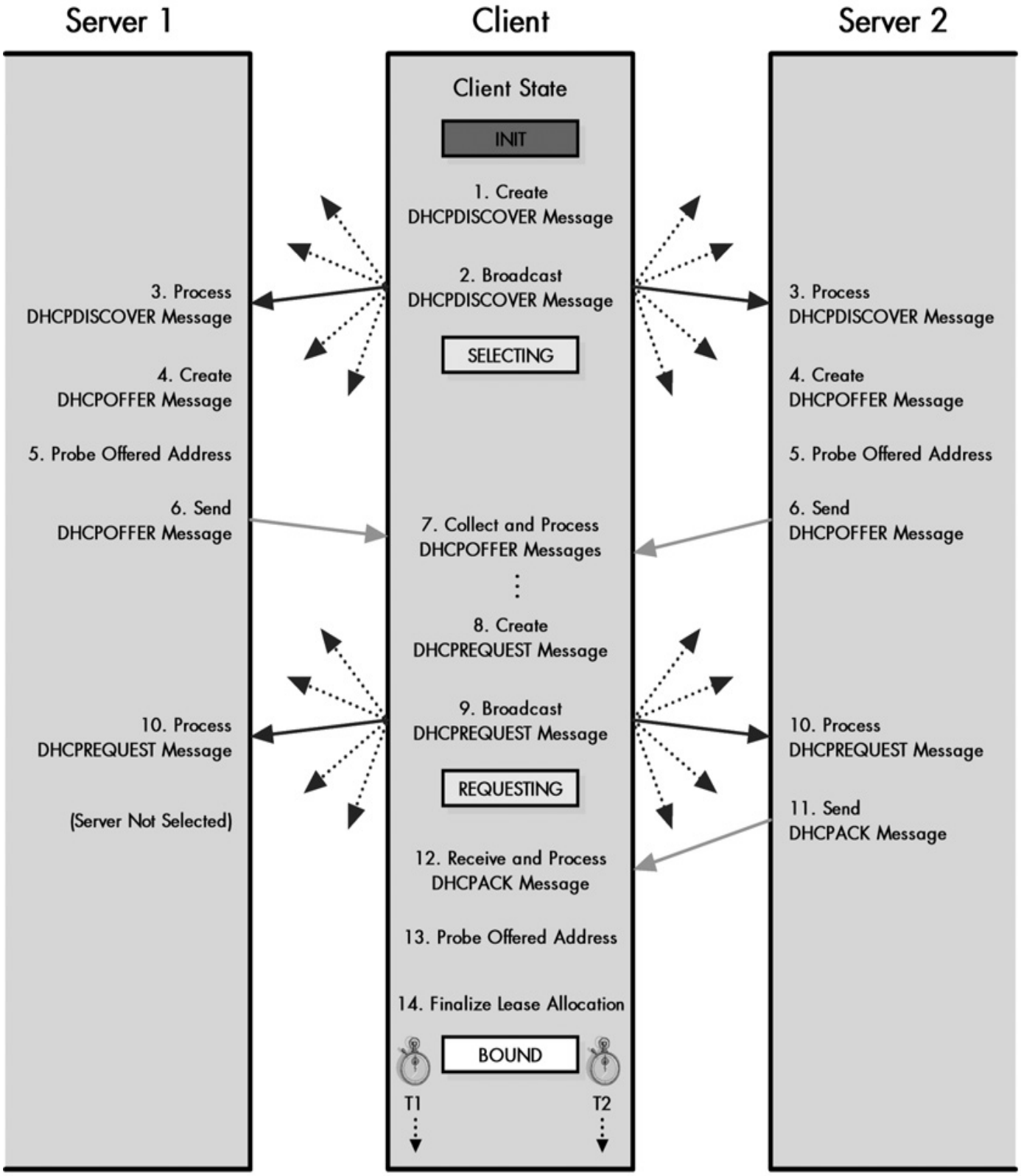
There are two different classes of potential security problems related to DHCP:

Unauthorized DHCP Servers If a malicious person plants a rogue DHCP server, it is possible that this device could respond to client requests and supply them with spurious configuration information. This could be used to make clients unusable on the network, or worse, set them up for further abuse later on. For example, a hacker could exploit a bogus DHCP server to direct a DHCP client to use a router under the hacker's control, rather than the one the client is supposed to use.

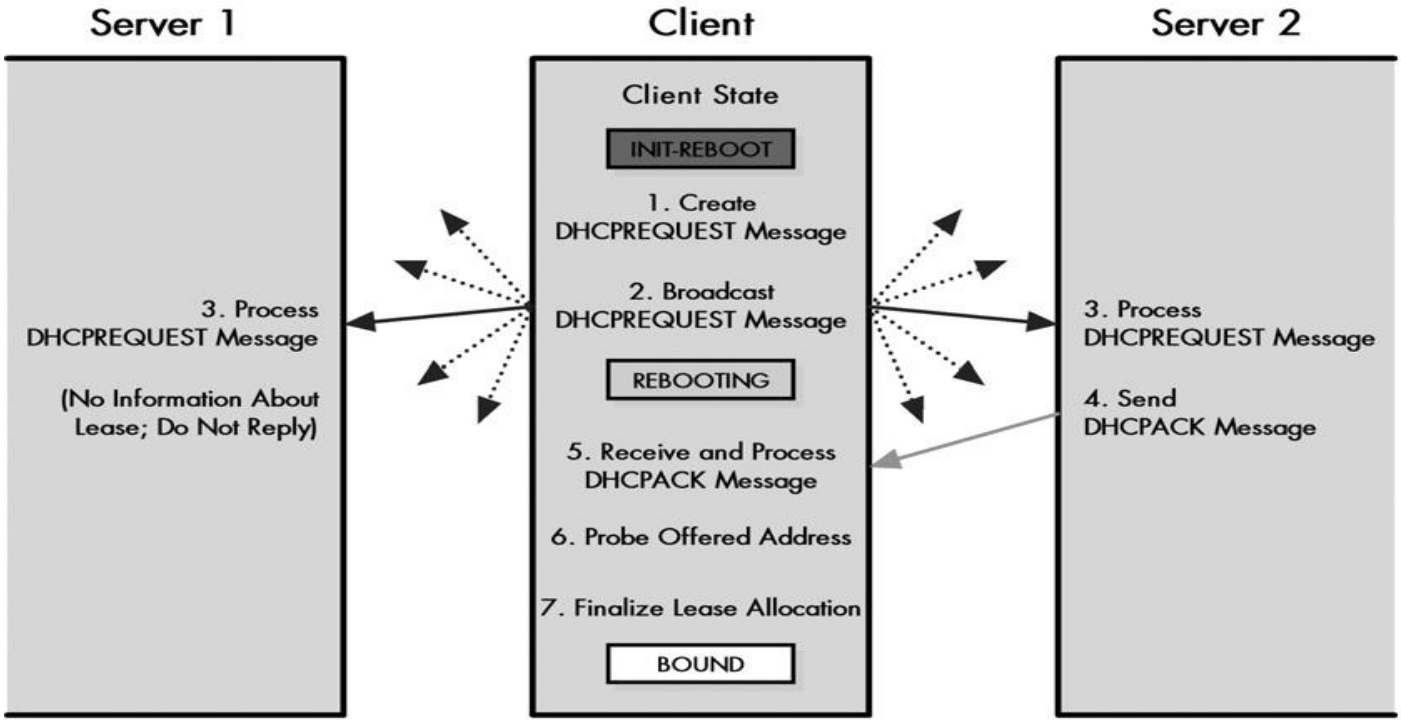
Unauthorized DHCP Clients A client could be set up that masquerades as a legitimate DHCP client and thereby obtain configuration information intended for that client. This information could then be used to compromise the network later on. Alternatively, a malicious person could use software to generate a lot of bogus DHCP client requests to use up all the IP addresses in a DHCP server's pool. More simply, this could be used by a thief to steal an IP address from an organization for his own use.

ANEXĂ

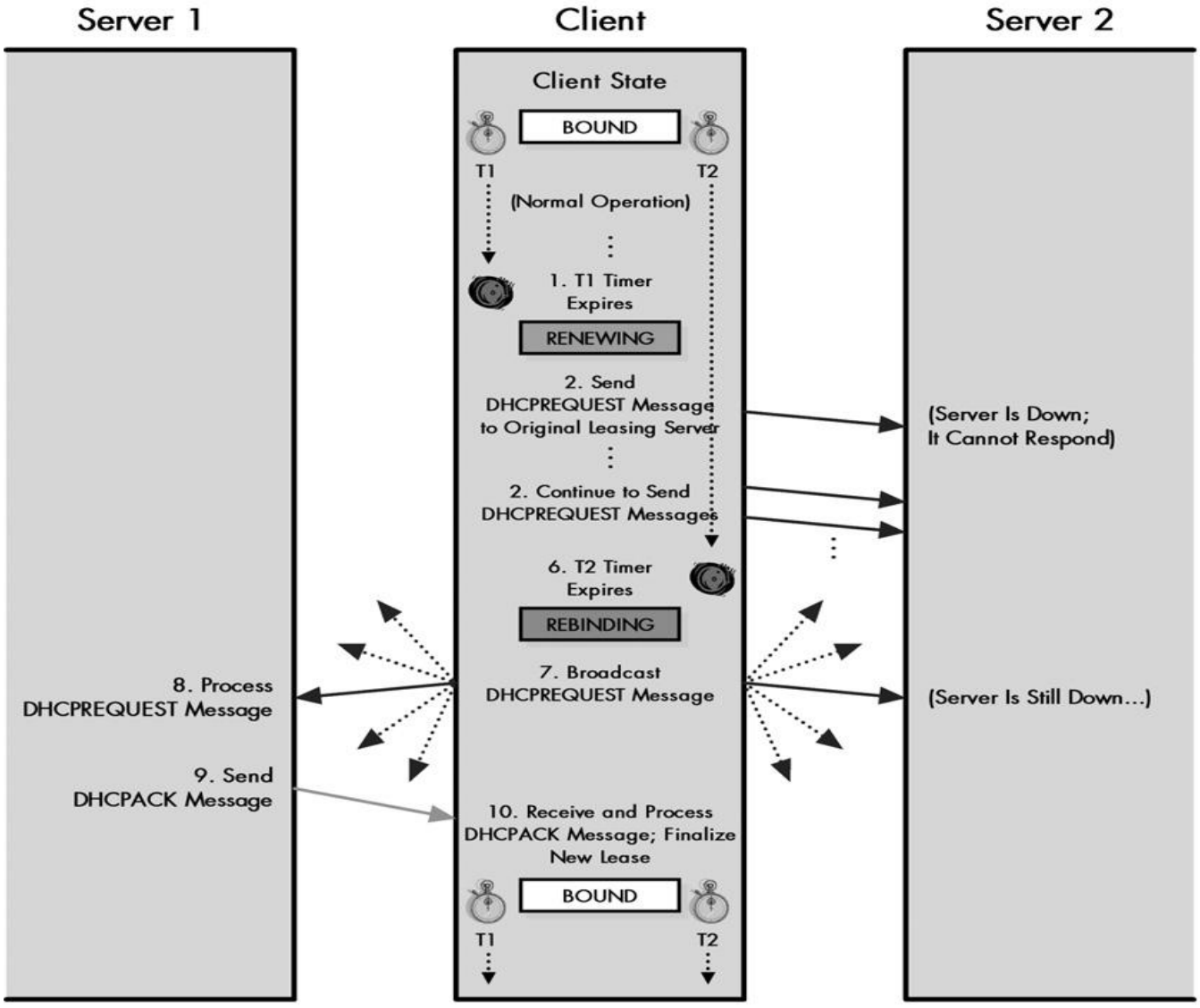
Initial Lease Allocation Process



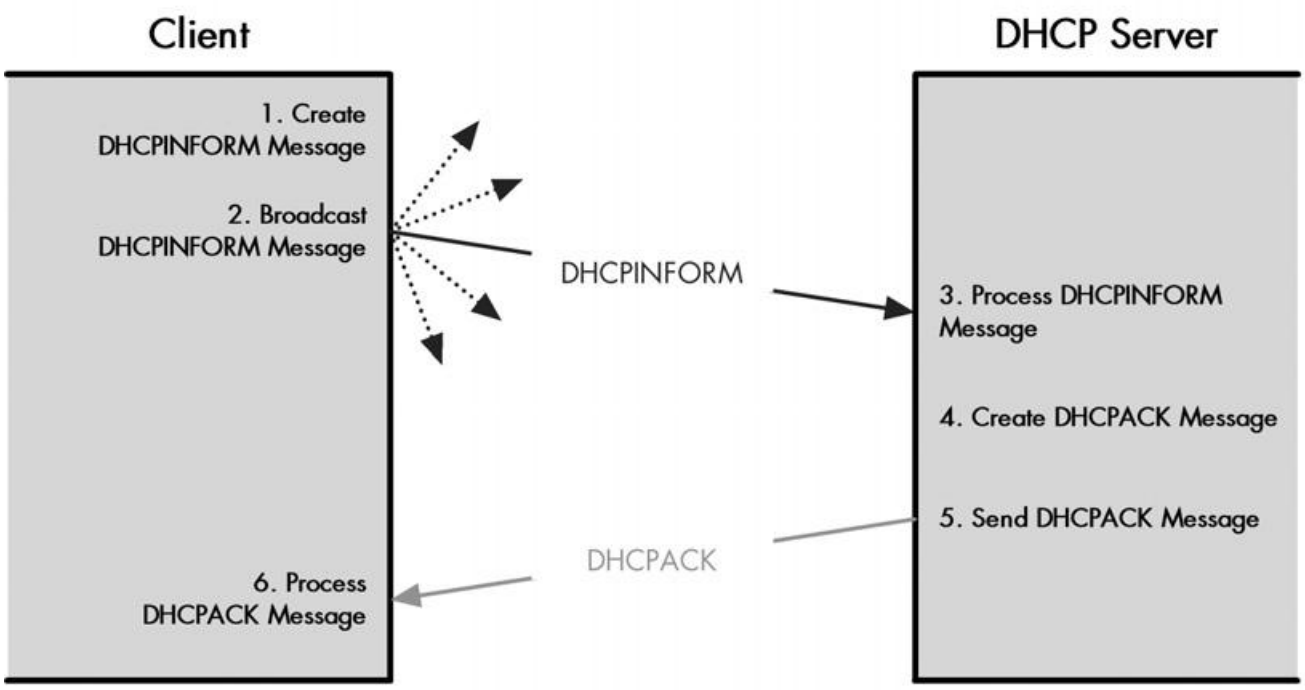
DHCP Lease Reallocation Process



DHCP Lease Renewal and Rebinding Processes



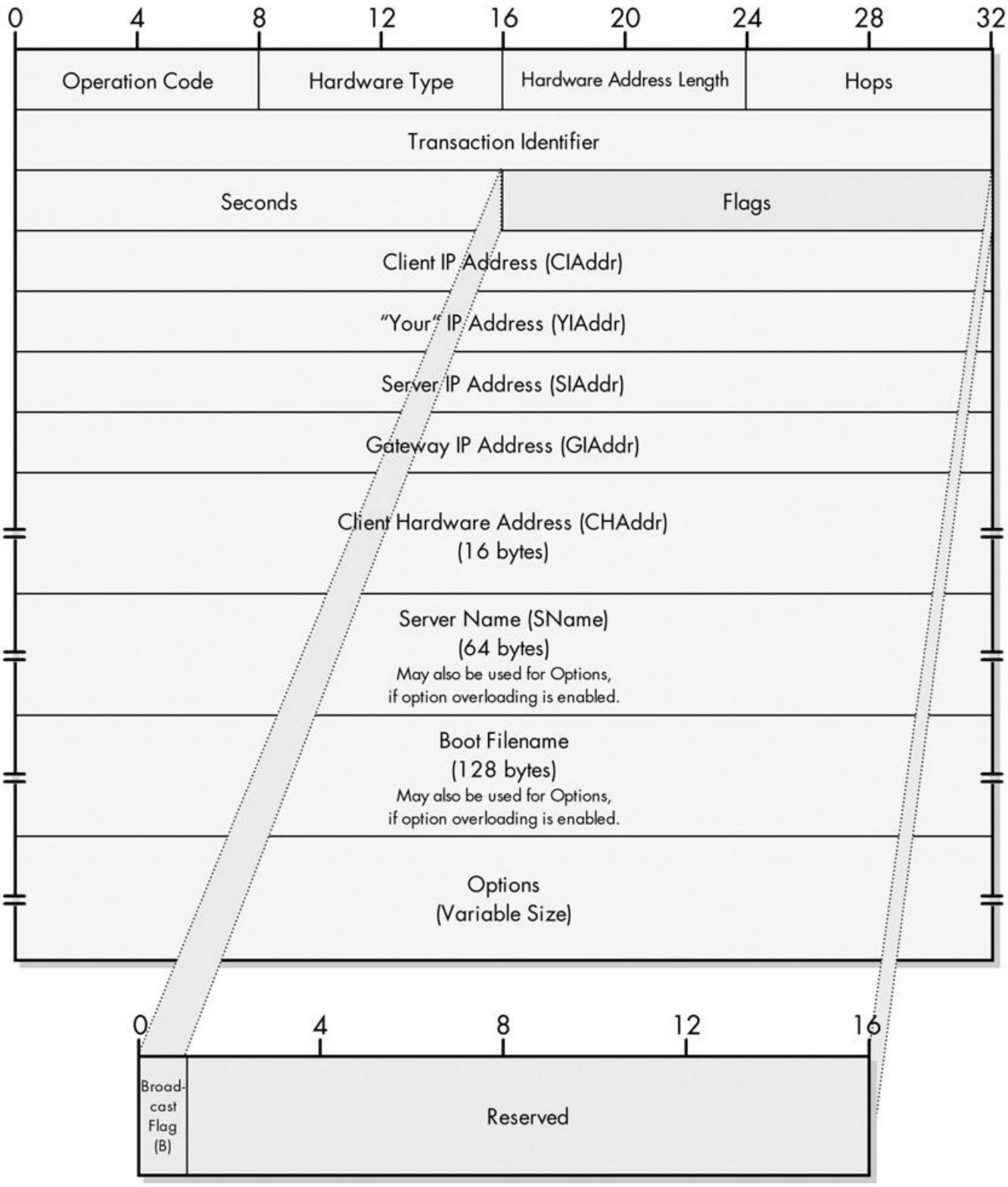
DHCP Parameter Configuration Process for Clients with Non-DHCP Addresses



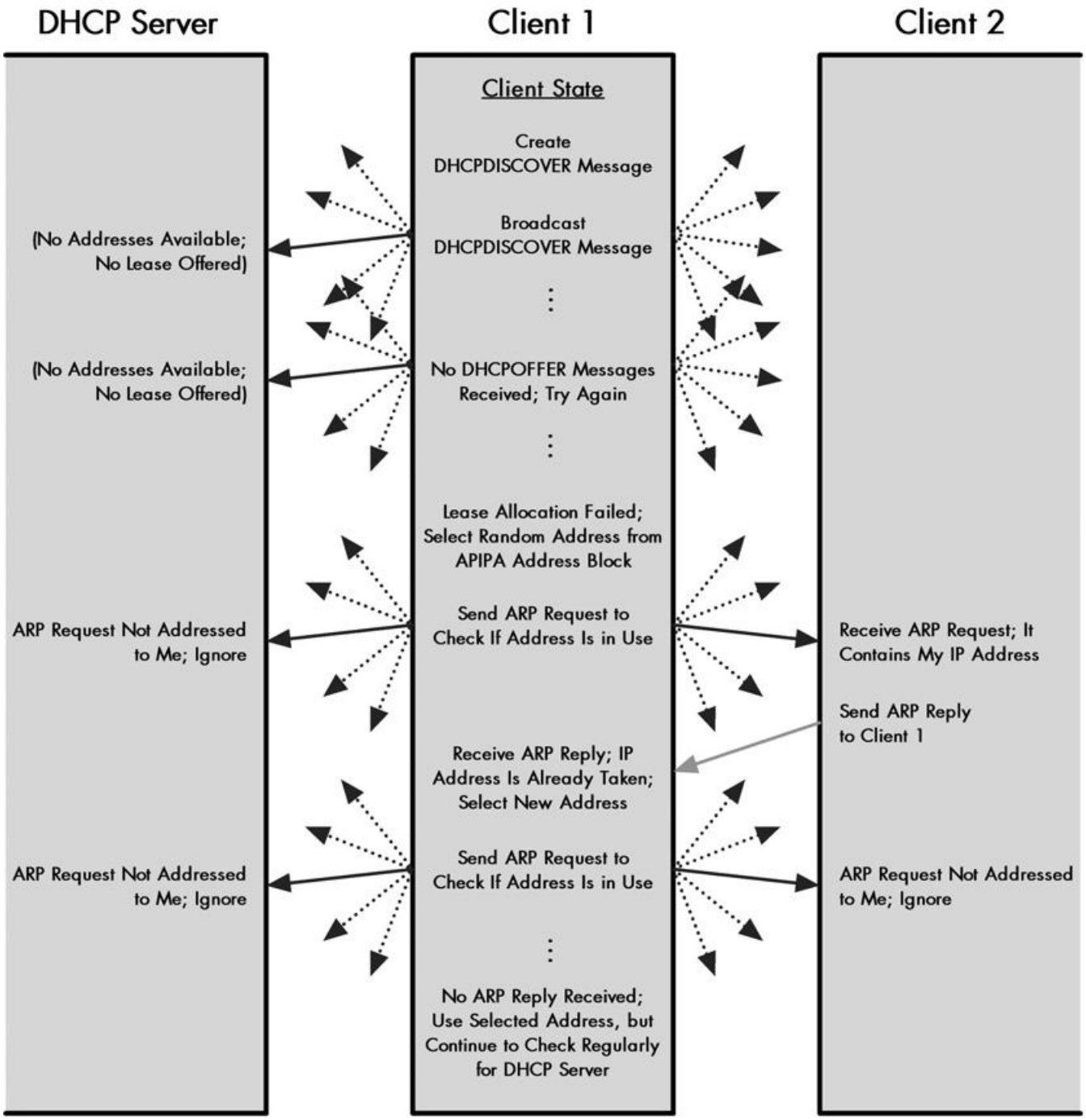
DHCP Message Types

Option 53 Value	DHCP Message Type
1	DHCPDISCOVER
2	DHCPOFFER
3	DHCPREQUEST
4	DHCPDECLINE
5	DHCPACK
6	DHCPNAK
7	DHCPRELEASE
8	DHCPINFORM

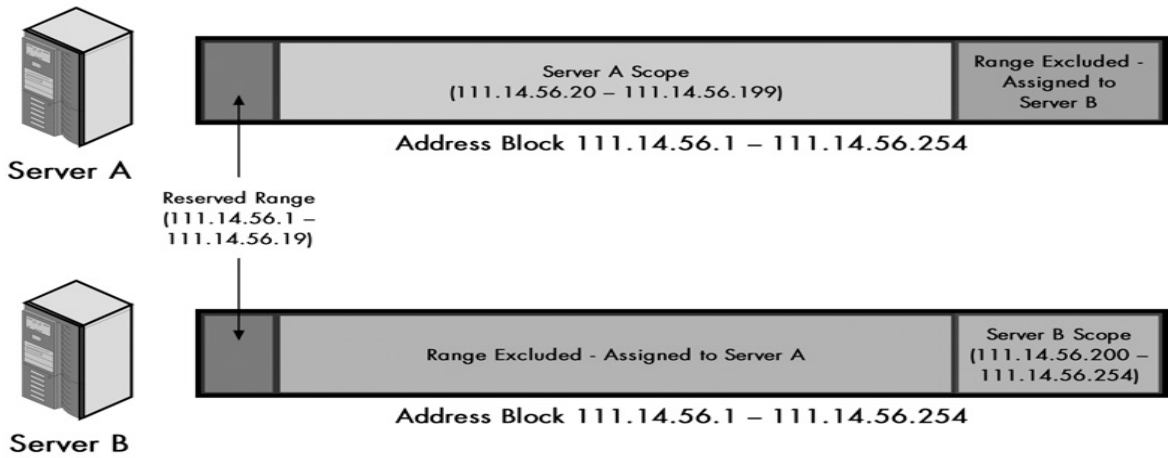
DHCP Message Format



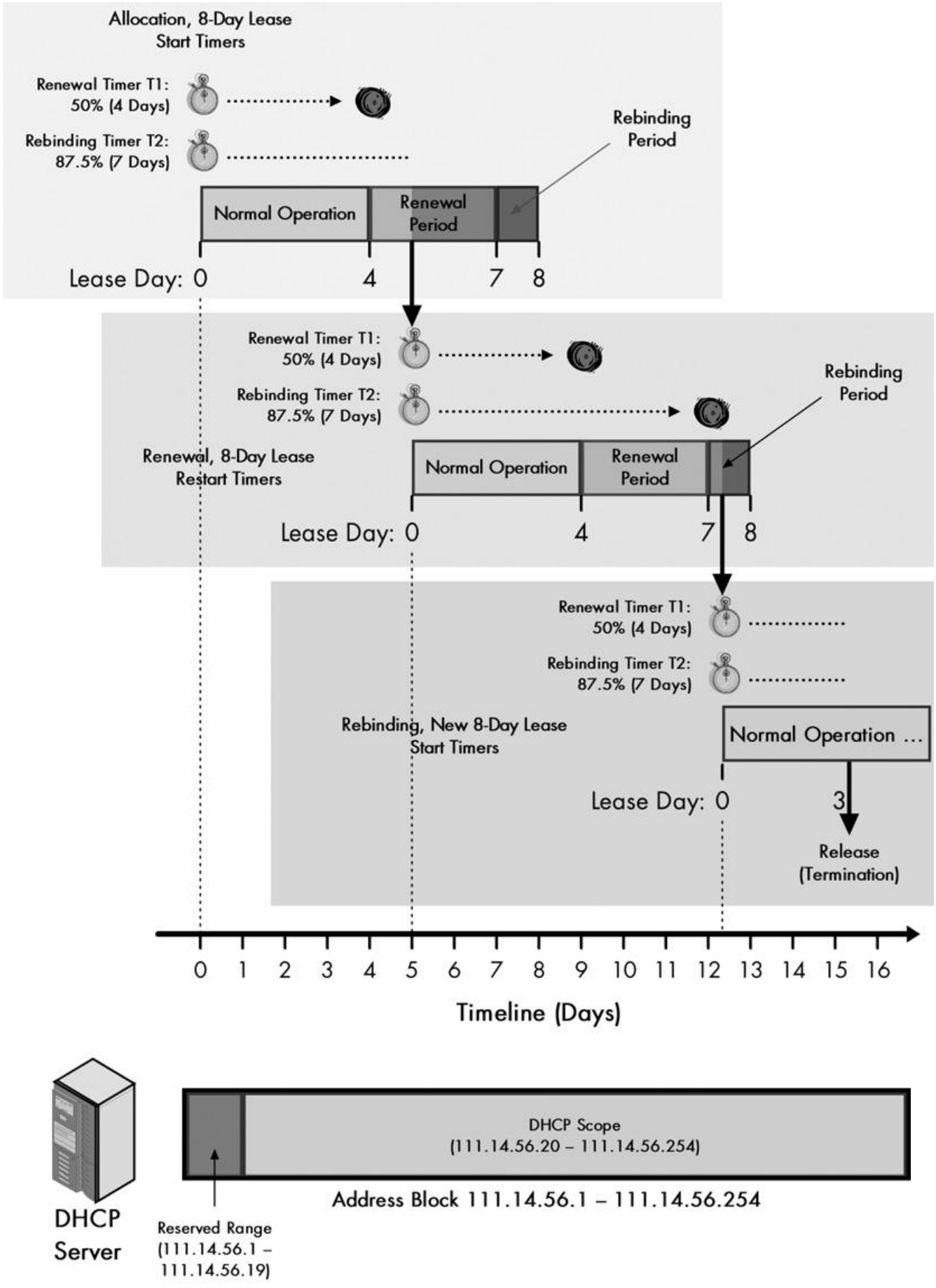
APIPA Operation Autoconfiguration/Automatic Private IP Addressing



DHCP multiple-server non-overlapping scopes



DHCP Lease Life Cycle Phases



DHCP Client FSM(Finite State Machine)