**DHCP Basics**

DHCP is designed to make the assignment of IP addresses and other network configuration information faster and easier. Rather than going around to every device on your network and setting up its network configuration manually, you can use your DHCP server to set up pools of addresses, called scopes, from which clients can request a temporary IP address.

DHCP communicates using User Datagram Protocol (UDP) datagrams through UDP Port 68. DHCP works with most current and past Windows clients, and also Linux, Macintosh, and many network-capable printers.

**Benefits of running DHCP**

Flexible configuration. DHCP makes it easy to implement changes in IP address configuration. Rather than manually configure each device's network connection every time a new DNS server is added, you can go into the DHCP server and make the necessary changes.

Scalable design. Any size network can benefit from DHCP.

Centralized administration. You can make needed configuration changes in a single place. This saves time and effort over going around to every device on your network.

Automatic host configuration. DHCP automates the assignment of IP addresses.

**DHCP components**

These components work together to automate IP addressing.

* DHCP leases
* DHCP scopes
* DHCP reservations
* DHCP options
* DHCP relay agents

DHCP leases define the lease duration, or the amount of time that a client can keep an IP address before releasing it. On the DHCP server, leases act as placeholders in its DHCP database. When the lease is issued, the IP address is removed from the list of available addresses to prevent the issuing of the same address to more than one computer.

To determine the duration of a lease, one must consider the client type, the connection time, and the available range of IP addresses. Client type has to do with the type of devices on your network, such as desktop computers, mobile notebooks, and servers. If you have more than the usual number of laptops on your network, the length of lease duration should decrease.

You should estimate the connection time, or the average length of time your clients spend on the network. If this time is relatively low, such as 2 to 4 hours, your lease duration doesn't have to be as long.

An important factor is the number of IP addresses you have available, as well as the number of clients who need DHCP's range of addresses. If you have a lot of clients in relation to your number of available addresses, shorter lease duration is advisable to avoid running out of IP addresses.

For most networks, the default settings should be sufficient. Shorter lease times would be necessary for networks with many clients that connect for less than a day. A college campus is a good example, since campuses usually offer free wireless access for their students, who are typically connected for a few hours a day.

**DHCP Scope**

A DHCP Scope is a range of IP addresses and related configuration information available by request from a DHCP client. These scopes usually represent a single subnet, or segment of a network. Each scope is a continuous range of IP addresses defined by a beginning IP address and an ending IP address. If you need to exclude IP addresses, you must create exclusions for those addresses. One reason for creating these addresses might be hardware with static IP addresses, like printers.

**DHCP Reservations**

When would you reserve an IP address? Well, in some cases, a network device needs to have a static IP address. An example would be a server, a router, or a network printer. In the DHCP role console, you reserve these addresses using the list below.

**Common DHCP Options**

Use these option codes to reserve IP addresses in DHCP.

3: Router

6: DNS server

15: DNS domain name

42: NTP server

44: WINS server (NetBIOS name server)

45: NetBIOS datagram distribution server (NBDD)

46: WINS/NetBIOS node type

47: NetBIOS scope ID

51: Lease Time

53: DHCP message type

55: Special option type used to communicate a parameter request list to the DHCP server

58: Renewal time value (T1)

59: Rebind time value (T2)

**DHCP Options**

DHCP options are basic settings that a client needs for proper network communication. These options include an IP address, a subnet mask, a default gateway, primary and secondary DNS servers, primary and secondary Windows Internet Name Service (WINS) if applicable, and DHCP lease expiration. You can define these options when creating the scope or change them later.

Server options are settings defined on each server that apply to all scopes on a specific DHCP server. Scope options are settings defined on each scope that apply only to the scope to which they are added. Router options are typically defined using scope options, which override server options. Server options are usually used for network resources whose IP addresses are the same for all scopes, such as DNS and WINS.

**DHCP Relay Agent**

DHCP requests are broadcast messages that cannot be routed, so they are limited to the subnet of the client requesting an IP address. You can choose one of two options to get around this. You can have a DHCP server on each subnet, which may be expensive and, therefore, implausible. Or, you can use a DHCP relay agent to forward DHCP requests. This agent accepts the broadcast packets and converts them to unicast packets that can traverse a routed network and vice versa when the DHCP server replies to the client requesting an IP address. Most modern routers support the passing of DHCP requests.

**DHCP Communication Processes**

DHCP clients and servers go through a series of exchanges in the process of assigning IP addresses and other network settings. They follow these message types, in order:

* First, the client broadcasts a **DHCPDiscover** message designed to locate a DHCP server and suggest values for the network address and lease duration.
* Second, one or more DHCP servers respond with a **DHCPOffer**, which offers configuration information for the client.
* The client then broadcasts a **DHCPRequest message** to, by default, the nearest DHCP server. This accepts the offered configuration information.
* The server then transmits either a **DHCPAck** or a **DHCPNACK** message. The **DHCPAck** confirms a DHCP client's IP address; the **DHCPNack** declines the client's request.
* A client might also transmit a **DCHPDecline** if it senses that an offered address is already in use. This declines an offered IP address. In this case, the client will have to start the process all over again.
* A DHCP client will send a **DHCPRelease** to relinquish its IP address and end its lease. This request is sent to the DHCP server that issued the lease.

A client can also send a **DHCPInform** message requesting local configuration information only.

**Initial Lease Request**

These clients may be new to a network or subnet, or their lease expired after being unable to renew. The initial lease request follows this process:

1. First, the client will seek a DHCP server by broadcasting a DHCPDiscover request. It will wait one second for a response. If it does not receive one, it will rebroadcast its request at intervals of 9, 13, and 16 seconds, with a variable between 0 milliseconds and 1 second. If it cannot reach a DHCP server, it will create an ad-hoc address called an Automatic Private IP Addressing (APIPA) while continuing to broadcast DHCPDiscover requests every 5 minutes. APIPA addresses are IP addresses starting with 169.254.
2. If the client succeeds in finding the DHCP server responsible for its subnet, it answers with a DCHPOffer message, which offers an IP address. Often, more than one server will be able to respond. The server(s) will temporarily reserve the IP address in anticipation of acceptance.
3. When the client receives the DHCP offer or offers, it will choose one and accept it by broadcasting a DHCPRequest. By default, the client will accept the offer of the DHCP server closest to it. Since it is a broadcast, all other servers will know that the client has accepted one of the offers.
4. The DHCP server creates a lease for the address it offered, makes the appropriate changes to its database of available and leased IP addresses, and confirms the IP address assignment with a DHCPAck message.

**Lease Renewals**

When a DHCP client powers on or connects to the network, it will confirm that it can continue to use its currently assigned address. If so, the lease is renewed and the expiration date extended. If not, they will try to renew after 50 percent of the lease time has expired. This renewal time value is referred to as T1.

If the T1 attempt fails, the client will try again after 87.5% of the lease has expired. If unsuccessful, it will broadcast a DHCPDiscover request to receive an IP address from any DHCP server on its network. This binding time value is referred to as T2.

DHCP renewals use a two-message communication process. A DHCP client makes a request to renew its current address by sending a DCHPRequest for the renewal of the lease it currently holds. When the server receives the client's request, it sends a DHCPAck to confirm that the DCHP lease and any DCHP options have been updated. This information includes a new expiration date for the lease.

If a client cannot reach a DHCP server before its lease expires, it will attempt to acquire a new IP address through the Initial Release process.

**dhcpd.conf File**

You can define your server configuration parameters in the dhcpd.conf file which may be located in the /etc the /etc/dhcpd or /etc/dhcp3 directories depending on your version of Linux.

**Note:** The skeleton dhcp.conf file that is created when you install the package may vary in its completeness. In Ubuntu / Debian, the skeleton dhcpd.conf file is extensive with most of the commands deactivated with a # sign at the beginning. In Fedora / RedHat / CentOS an extensive sample is also created with activated commands. It is found in the following location which you can always use as a guide.

/usr/share/doc/dhcp\*/dhcpd.conf.sample

**Note:** The dhcpd.conf configuration file formats in Debian / Ubuntu and Redhat / Fedora are identical.

## [Basic Configuration](http://www.brennan.id.au/10-DHCP_Server.html#top) (http://www.brennan.id.au/10-DHCP\_Server.html)

The main DHCP configuration file should be located at /etc/dhcpd.conf, however it is sometimes missing. This is a configuration safeguard to stop users from accidentally starting a DHCP server without fully configuring its details. Having any unplanned DHCP servers operating on a network can result in major network problems. Therefore the administrator must create the configuration before implementing its services, a physical task to reduce error (some distributions may have the file available).

|  |
| --- |
| [bash]# **vi /etc/dhcpd.conf**  |

The following configuration file is an example for a typical home / small office network.

|  |  |
| --- | --- |
| Note !! | Be sure to change parameters to suit your network and domain name. |

|  |
| --- |
| ##   DHCP Server Config File#ddns-update-style none;ignore client-updates;lease-file-name "/var/lib/dhcpd/dhcpd.leases";authoritative;option domain-name                      "example.com";default-lease-time                      86400;   # 24 hoursmax-lease-time                          172800;  # 48 hourssubnet 192.168.1.0 netmask 255.255.255.0 {        option routers                  192.168.1.1;        option subnet-mask              255.255.255.0;        option broadcast-address        192.168.1.255;        option domain-name-servers      192.168.1.1;        option ntp-servers              192.168.1.1;        option netbios-name-servers     192.168.1.1;        range   192.168.1.101   192.168.1.200;} |

## [Setting Fixed Addresses](http://www.brennan.id.au/10-DHCP_Server.html#top)

There may be a time when it is necessary for a workstation to be assigned a fixed address, this can be easily achieved by setting the following details in the bottom of the /etc/dhcpd.conf file.

|  |
| --- |
| host wkstn1 {        hardware ethernet 00:0d:62:d7:a0:12;        fixed-address 192.168.1.5;} |

## [Setting Daemon Options](http://www.brennan.id.au/10-DHCP_Server.html#top)

The DHCP daemon can be configured with command line options by using the /etc/sysconfig/dhcpd file. For security, DHCP can be bound to an interface so the allocation of addresses are only available to the private internal network.

|  |
| --- |
| [bash]# **vi /etc/sysconfig/dhcpd** |

Setting this option provides queries and assignment only through this interface.

|  |
| --- |
| # Command line options hereDHCPDARGS=eth1 |

There are many more options statements you can use to configure DHCP. These include telling the DHCP clients where to go for services such as finger and IRC. Check the dhcp-options man page after you do your install:

[root@bigboy tmp]# man dhcp-options

# DHCP Servers with Multiple NICs

**Fedora / RedHat / CentOS:** The /etc/sysconfig/dhcpd file must be edited and the DHCPDARGS variable edited to include the preferred interface. In this example interface eth0 is preferred.

# File: /etc/sysconfig/dhcpd

DHCPDARGS=eth1

## Configuring a DHCP Client

Setting up a Linux for dhcp can be done by editing file using a text editor such as vi:
# vi /etc/sysconfig/network-scripts/ifcfg-eth0
Following is sample static configuration:
DEVICE=eth0
BOOTPROTO=static
HWADDR=00:19:D1:2A:BA:A8
IPADDR=10.10.29.66
NETMASK=255.255.255.192
ONBOOT=yes

Replace static configuration with DHCP:
DEVICE=eth0
BOOTPROTO=dhcp
HWADDR=00:19:D1:2A:BA:A8
ONBOOT=yes

The parameters specified in the above sample file are explained below. For more detailed information about the configuration options available, type "man dhcpd.conf" or "man dhcp-options" at the command prompt.

|  |  |
| --- | --- |
| **Parameter** | **Definition** |
| ddns-update-style | Type of DDNS update to use with local DNS Server |
| ignore client-updates | Ignore all client requests for DDNS update |
| lease-file-name | Filename that stores list of active IP lease allocations |
| Authoritative | Set as master server, protects against rogue DHCP servers and misconfigured clients |
| option domain-name | Specifies the Internet Domain Name to append to a client's hostname |
| option domain-name-servers | The DNS servers the clients should use for name resolution |
| default-lease-time | The default time in seconds that the IP is leased |
| max-lease-time | The max time in seconds that the IP is leased |
| option routers | Specifies the **Gateway** for the client to use |
| option subnet-mask | The subnet mask specific to the lease range |
| option broadcast-address | The broadcast address specific to the lease range |
| option ntp-servers | Network Time Protocol servers available to the clients |
| option netbios-name-server | The NetBIOS name server (WINS) |
| option netbios-node-type | The NetBIOS name resolution method (8=hybrid) |
| Range | The range of valid IP addresses available for client offer |