Chapter 5. DHCP Services

This chapter describes DHCP services in NetDefendOS.

5.1. Overview

DHCP (Dynamic Host Configuration Protocol) is a protocol that allows network administrators to automatically assign IP numbers to computers on a network.

IP Address Assignment

A *DHCP Server* implements the task of assigning IP addresses to DHCP clients. These addresses come from a pre-defined IP address pool which DHCP manages. When a DHCP server receives a request from a DHCP client, it returns the configuration parameters (such as an IP address, a MAC address, a domain name, and a lease for the IP address) to the client in a unicast message.

DHCP Leases

Compared to static assignment, where the client owns the address, dynamic addressing by a DHCP server leases the address to each client for a pre-defined period of time. During the lifetime of a lease, the client has permission to keep the assigned address and is guaranteed to have no address collision with other clients.

Before the expiration of the lease, the client needs to renew the lease from the server so it can keep using the assigned IP address. The client may also decide at any time that it no longer wishes to use the IP address it was assigned, and may terminate the lease and release the IP address.

The lease time can be configured in a DHCP server by the administrator.

5.2. DHCP Servers

NetDefendOS has the ability to act as one or more logical DHCP servers. Filtering of DHCP client requests is based on interface, so each NetDefendOS interface can have, at most, one single logical DHCP server associated with it. In other words, NetDefendOS can provision DHCP clients using different address ranges depending on what interface they are located on.

A number of standard options can be configured for each DHCP server instance:

- **IP Address**
- **Netmask** - netmask sent to the DHCP Client.
- **Subnet**
- **Gateway Address** - what IP should be sent to the client for use as the default gateway. If 0.0.0.0 is specified the IP given to the client will be sent as the gateway.
- **Domain Name**
- **Lease Time** - the time, in seconds that a DHCP lease should be provided to a host after which the client must renew the lease.
- **DNS Servers**
- **WINS Servers**
- **Next Server** - the IP address of the next server in the boot process, this is usually a TFTP server.

In addition, *Custom Options* can be specified in order to have the DHCP servers hand out all types of options supported by the DHCP standard.

DHCP servers assign and manage the IP addresses taken the from specified address pool. NetDefendOS DHCP servers are not limited to serving a single range of IP addresses but can use any IP address range that can be specified by a NetDefendOS address object.

Example 5.1. Setting up a DHCP server

This example shows how to set up a DHCP server called *DHCPServer1* which assigns and manages IP addresses from an IP address pool called *DHCPRange1*. This example assumes you have created an IP range for the DHCP Server.

CLI

```
gw-world:/> add DHCPServer DHCPServer1 Interface=lan
            IPAddressPool=DHCPRange1 Netmask=255.255.255.0
```

Web Interface

1. Go to **System > DHCP > DHCP Servers >Add > DHCPServer**
2. Now enter:
   - **Name:** DHCPServer1
   - **Interface Filter:** lan
   - **IP Address Pool:** DHCPRange1
   - **Netmask:** 255.255.255.0
3. Click **OK**

Example 5.2. Checking the status of a DHCP server

Web Interface

Go to **Status > DHCP Server** in the menu bar.

CLI

To see the status of all servers:

```
gw-world:/> dhcpserver
```

To list all configured servers:

```
gw-world:/> show dhcpserver
```

Tip

DHCP leases are remembered by the system between system restarts.

5.3. Static DHCP Assignment

Where the administrator requires a fixed relationship between a client and the assigned IP address, NetDefendOS allows the assignment of a given IP to a specific MAC address.

Example 5.3. Setting up Static DHCP

This example shows how to assign the IP address *192.168.1.1* to the MAC address *00-90-12-13-14-15*. The examples assumes that the DHCP server *DHCPServer1* has already been defined.

CLI

First change to the *DHCPServer1* context:

```
gw-world:/> cc DHCPServer DHCPServer1
```

Now add the static DHCP assignment:

```
gw-world:/> add DHCPServerPoolStaticHost Host=192.168.1.1
                                                MACAddress=00-90-12-13-14-15
```

All static assignments can be listed and each is listed with an index number:

```
gw-world:/> show

   #  Comments
   -  -------
+  1  (none)
```

An individual static assignment can be shown using its index number:

```
gw-world:/> show DHCPServerPoolStaticHost 1

   Property  Value
-----------  -----------------
     Index:  1
      Host:  192.168.1.1
MACAddress:  00-90-12-13-14-15
  Comments:  (none)
```

The assignment could be changed later to IP address *192.168.1.12* with the following command:

```
gw-world:/> set DHCPServerPoolStaticHost 1 Host=192.168.1.12
                                                MACAddress=00-90-12-13-14-15
```

Web Interface

1. Go to **System > DHCP > DHCP Servers > DHCPServer1 > Static Hosts > Add > Static Host Entry**
2. Now enter:
   - **Host:** 19.168.1.1
   - **MAC:** 00-90-12-13-14-15
3. Click **OK**

5.4. DHCP Relaying

With DHCP, clients send requests to locate the DHCP server(s) using broadcast messages. However, broadcasts are normally only propagated across the local network. This means that the DHCP server and client would always need to be in the same physical network area to be able to communicate. In a large Internet-like environment, this means there has to be a different server on every network. This problem is solved by the use of a DHCP relayer.

A DHCP relayer takes the place of the DHCP server in the local network to act as the link between the client and the remote DHCP server. It intercepts requests from clients and relays them to the server. The server then responds to the relayer, which forwards the response to the client. The DHCP relayers follow the BOOTP relay agent functionality and retain the BOOTP message format and communication protocol, and hence, they are often called BOOTP relay agents.

Example 5.4. Setting up a DHCP relayer

This example allows clients on VLAN interfaces to obtain IP addresses from a DHCP server. It is assumed the firewall is configured with VLAN interfaces, "vlan1" and "vlan2", that use DHCP relaying, and the DHCP server IP address is defined in the address book as "ip-dhcp". NetDefendOS will install a route for the client when it has finalized the DHCP process and obtained an IP.

CLI

Adding VLAN interfaces vlan1 and vlan2 that should relay to an interface group named as ipgrp-dhcp:

```
gw-world:/> add Interface InterfaceGroup ipgrp-dhcp Members=vlan1,vlan2
```

Adding a DHCP relay named as "vlan-to-dhcpserver":

```
gw-world:/> add DHCPRelay vlan-to-dhcpserver Action=Relay TargetDHCPServer=ip-dhcp
            SourceInterface=ipgrp-dhcp AddRoute=Yes ProxyARPInterfaces=ipgrp-dhcp
```

Web Interface

Adding VLAN interfaces vlan1 and vlan2 that should relay to an interface group named as ipgrp-dhcp:

1. Go to **Interface > Interface Groups > Add > InterfaceGroup**
2. Now enter:
   - **Name:** ipgrp-dhcp
   - **Interfaces**: select "vlan1" and "vlan2" from the **Available** list and put them into the **Selected** list.
3. Click **OK**

Adding a DHCP relay named as "vlan-to-dhcpserver":

1. Go to **System > DHCP > Add > DHCP Relay**
2. Now enter:
   - **Name:** vlan-to-dhcpserver
   - **Action:** Relay
   - **Source Interface:** ipgrp-dhcp
   - **DHCP Server to relay to:** ip-dhcp
   - **Allowed IP offers from server:** all-nets
3. Under the **Add Route** tab, check **Add dynamic routes for this relayed DHCP lease**
4. Click **OK**

5.5. IP Pools

Overview

IP pools are used to offer other subsystems access to a cache of DHCP IP addresses. These addresses are gathered into a pool by internally maintaining a series of DHCP clients (one per IP). The DHCP servers used by a pool can either be external or be DHCP servers defined in NetDefendOS itself. External DHCP servers can be specified as the server on a specific interface or by a unique IP address. Multiple IP Pools can be set up with different identifying names.

The primary usage of IP Pools is with *IKE Config Mode* which a feature used for allocating IP addresses to remote clients connecting through IPsec tunnels. For more information on this see Section 9.4.3.4, “Using Config Mode”.

Basic IP Pool Options

The basic options available for an IP Pool are:

DHCP Server behind interface — Indicates that the IP pool should use the DHCP server(s) residing on the specified interface.

Server filter — Optional setting used to specify which servers to use. If unspecified any DHCP server on the interface will be used. The order of the provided adddress or ranges (if multiple) will be used to indicate the preferred servers.

Specify DHCP Server Address — Specify DHCP server IP(s) in preferred ascending order to be used. Using the IP loopback address *127.0.0.1* indicates that the DHCP server is NetDefendOS itself.

Client IP filter — Optional setting used to specify which offered IPs are valid to use. In most cases this will be set to the default of **all-nets**. Alternatively a set of IP ranges might be specified. The filter ensures that only certain IP addresses from DHCP servers are acceptable and is used in the situation where there might be a DHCP server response with an unacceptable IP address.

Advanced IP Pool Options

Advanced options available for IP Pool configuration are:

Routing table — Policy routing table to be used for lookups when resolving the destination interfaces for the configured DHCP servers.

Receive interface — "Simulated" receive interface. This can be used in policy based routing rules and/or used to trigger a specific DHCP server rule if the pool is using a DHCP server in NetDefendOS and the IP address of that server has been specified as the loopback interface.

MAC Range — A range of MAC addresses that will be use to create "fake" DHCP clients. Used when the DHCP server(s) map clients by the MAC address. An indication of the need for MAC ranges is when the DHCP server keeps giving out the same IP for each client.

Prefetched leases — Specifies the number of leases to keep prefetched. Prefetching will improve performance since there won't be any wait time when a system requests an IP (while there exists prefetched IPs).

Maximum free — The maximum number of "free" IPs to be kept. Must be equal to or

greater than the prefetch parameter. The pool will start releasing (giving back IPs to the DHCP server) when the number of free clients exceeds this value.

Maximum clients Optional setting used to specify the maximum number of clients (IPs) allowed in the pool.

Using Prefetched Leases

As mentioned in the previous section, the *Prefetched Leases* option specifies the size of the cache of leases which is maintained by NetDefendOS. This cache provides fast lease allocation and can improve overall system performance. It should be noted however that the entire prefetched number of leases is requested at system startup and if this number is too large then this can degrade initial performance.

As leases in the prefetch cache are allocated, requests are made to DHCP servers so that the cache is always full. The administrator therefore has to make a judgement as to the optimal initial size of the prefetch cache.

Example 5.5. Creating an IP Pool

This example shows the creation of an IP Pool object that will use the DHCP server on IP address *28.10.14.1* with 10 prefetched leases. It's assumed that this IP address is already defined in the address book as an IP object called *ippool_dhcp*

CLI

```
gw-world:/> add IPPool ip_pool_1 DHCPServerType=ServerIP ServerIP=ippool_dhcp
```

Web Interface

1. Go to **Objects > IP Pools > Add > IP Pool**
2. Now enter **Name:** ip_pool_1
3. Select **Specify DHCP Server Address**
4. Add *ippool_dhcp* to the **Selected** list
5. Select the **Advanced** tab
6. Set **Prefetched Leases** to *10*
7. Click **OK**