• 75 - DHCP und BOOTCP

DHCP Server

- **Description**
  The ISC DHCP server allows to distribute dynamic and static IP numbers to DHCP clients. The server can serve BOOTP and DHCP requests from clients.

- **Installation:**

Server installation: SuSE CDs Packet : dhcp (ISC DHCP server)

- **Leases concept**
  - After the DHCP server has assigned an IP to a client it writes the leases i the file: `/var/lib/dhcp/dhcpd.leases` . This file SHOULD exist for the server to start.
  - If a client requests a new IP after expiration it will most likely be given the same old IP written in the lease file.

- **Where is what:**

`/etc/dhcpd.conf`	DHCP server configuration file
`/usr/sbin/dhcpd`	Main DHCP server daemon
`/usr/sbin/rcdhcpd`	Link to script for DHCP server start /stop(SuSE)
`/etc/init.d/dhcpd`	Script for DHCP server start /stop
`/var/lib/dhcp/dhcpd.leases`	List of IP Client leases.

- **Info on DHCP configuration**

`man dhcpd`	DHCP server daemon start parameters
`man dhcpd.conf`	Info on dhcpd.conf configuration.
`/usr/share/doc/packages/dhcp/dhcpd.conf`	Example of DHCP server configuration

- **Graphic Tools to configure DHCP server:**

`kcmdhcpd`	- From kde, very easy to use
`webmin`	- From `www.webmin.com`

- **Technical bit**
  The DHCP client sends its first request with:
  broadcast address 255.255.255.255 Port 67.
  eg. extract from `ngrep -d eth0`:

```
0.0.0.0:68 -> 255.255.255.255:67
192.168.100.133:67 -> 192.168.100.200:68
192.168.100.133 -> 192.168.100.200 8:0
192.168.100.200 -> 192.168.100.133 0:0
192.168.100.200 -> 192.168.100.133 3:1
```

  DHCP Server listen on UDP port 67
  DHCP Client listens on UDP port 68

- **To check the server leases in lease cache:**

```
watch -n1 "grep '^lease ' /var/lib/dhcp/dhcpd.leases"
```

- **Notes on DHCP server/client**

- The DHCP server configuration should always declare all the subnets to which it is connected, even if it doesn't respond to the DHCP requests on some of them.

- The DHCP server assigns the last IP of the range first and up to the first IP.

- The DHCP server will not start if it can't find the file:
  `/var/lib/dhcp/dhcpd.leases .`
  In this case create an empty one or copy the backup file
  `/var/lib/dhcp/dhcpd.leases~` to it.

- No security is provided to prevent inserting another DHCP server in the net.
  Only one responsive DHCP server should exist on the same subnet.

- After the DHCP client starts, it stays as a daemon allowing to make requests to the HDCP server regularly after HALF of its lease filespan is spent.

- If the DHCP client dhclient daemon makes a request of lifespan and it is longer than the one assigned in the server, the server settings overrides the client's request.

- If new parameters (Options) are given in the server's configuration, they will be updated only when the clients issue requests (after half their leases' lifespan).

- Each declaration in the ISC DHCP server or client's configuration files should be terminated by a semicolon '`;`'
  Each config block should be enclosed in curly brackets `{...}`

- Extra information for DHCP server/clients can be seen on the Internet at:

  ISC DHCP
  `http://www.isc.org/products/DHCP/`

  Dynamic DNS/DHCP perl script for ISC DHCP server Version 2
  `http://www.heronforge.net/~stephen/DHCP-DNS/dhcp-dns.html`

  Secure DDNS HOWTO:
  `http://ops.iet.org/dns/dynupd/secure-ddns-howto.html`

DHCP Server configuration file

```
#------------ /etc/dhcpd.conf Version 2 and 3 -------------
#------------ Minimal Global parameters -----------
option domain-name              "linux.local";
option domain-name-servers      192.168.100.40, 192.168.100.42;
#============== Leases ==========================
#-------- default lease time : 1 day --------
default-lease-time      86400;
#-------- maximale lease time : 1 week -----
max-lease-time          604800;
#==============Version 2 only ==================================
#-------- ddns-update-style (using older Dynamic DNS update mode)
ddns-update-style ad-hoc; (or none)
===============Version 3 only ==================================
#------------ for ISC-dhcpd Version 3 (SuSE 8.0 and up )----------
authoritative;
#------------ dynamic dns-update-style IMPORTANT-----------
ddns-update-style none; (or interim or ad-hoc)
ddns-updates off; (or on)
#================================================================
#-----------IP Distribution Configuration  for Version 2 and 3 -------
#(A)- Dynamic IP Numbers distribution for a subnet A ------
subnet 192.168.100.0 netmask 255.255.255.0
{ range 192.168.100.1 192.168.100.20;
  range 192.168.100.50 192.168.100.100;
  option subnet-mask              255.255.255.0;
  option broadcast-address        192.168.100.255;
  option routers                  192.168.100.133;
}
#(B)- Dynamic IP Numbers distribution for a subnet B -for DHCP and BOOTP clients
subnet 192.168.80.0 netmask 255.255.255.0
{ range dynamic-bootp 192.168.80.30 192.168.80.130;
  option subnet-mask              255.255.255.0;
  option broadcast-address        192.168.80.255;
  option routers                  192.168.80.133;
}
#(C)----- Dynamic IP Numbers distribution for a subnet C ------
# NOTE: This declaration is empty to prevent the server from responding to DHCP requests #from
this subnet to which the server is also connected.
# A declaration MUST be made for #each subnet to wich the server is connected unless the
# server is started with the interface #names as parameters.  eg.   dhcpd eth0 eth1
subnet 192.168.70.0 netmask 255.255.255.0 {
}
#(D)- Providing a Fixed IP No. to a host (dogan) with a MAC address ----
#  Note: It doesn't matter if the host doesn't have the name  dogan  .He will get the IP.
host dogan {
hardware ethernet 00:80:C8:F6:98:57;
fixed-address 192.168.80.200;
}
```

```
#(E)- Providing a Fixed IP No. to a host (harley) without a MAC address ----
#IMPORTANT NOTE: Here, any host who calls itself harley will be assigned this IP
#even if a lease is already assigned for the same host name!!!
host harley {
fixed-address 192.168.80.201;
}
```

DHCP Clients

Client installation: SuSE CDs Packet : **dhcpcd** (client) or **dhclient**
SuSE installs the dhcpcd by default
or **pump** from redhat distribution.

Notes:

- The SuSE 8.0 script /etc/init.d/dhclient says that it (itself) can handle either the dhclient or dhcpcd properly.
- The dhcpcd can only configure one IP for the eth0 but the ISC dhclientdaemon supposedly can handle multiple IPs.
- Depending on the type of DHCP client, they can make requests to the DHCP server asking for: IP Addr, Router address, DNS addresses etc. via their configuration file. Lease lifespan requests are overriden by the DHCP server's settings if they are longer than the server's settings.

- **dhcpcd**

The dhcpcd client will send requests to the DHCP server and configure the eth0 each time it is started.

Syntax: (see man dhcpcd for more info)

```
dhcpcd [-dknrBCDHRST] [-t timeout] [-c filename]
       [-h hostname] [-i vendorClassID] [-I clientID]
       [-l leasetime] [-s [ipaddr]] [-w windowsize]
       [interface]
```

eg. dhcpcd -R eth0 (has a default timeout of 60 sec.)

-R Prevents dhcpcd from replacing existing /etc/resolv.conf file.

-G Prevents dhcpcd from setting a route to the default gateway. This is useful when multiple processes of dhcpcd are running and you want to control which one is allowed to set the default route.

-S Prevents dhcpcd from modifying the search list in the /etc/resolv.conf

Host IP assignment configuration file:

/var/lib/dhcpcd/dhcpcd-eth0.cache	Where the last IP number obtained is stored. It is normally checked and requested on each startup of the dhcpcd daemon.(This file is binary !!!)
/var/lib/dhcpcd/dhcpcd-eth0.info	Info in text format produced out of above dhcpcd-eth0.cache file.

Note written in `/etc/resolv.conf` after successfull request from dhcpcd
Info: This is a temporary `/etc/resolv.conf` created by service `dhcpcd`.
The previous file has been saved and will be restored later when the `dhcpcd` dies.
If you don't like your `/etc/resolv.conf` to be changed, you can set
`MODIFY_{RESOLV,NAMED}_CONF_DYNAMICALLY=no`
These variables are placed in `/etc/sysconfig/network/config`.
You can also configure service `dhcpcd` not to modify it.
If you don't like dhcpcd to change your nameserver settings then either set:

`DHCLIENT_MODIFY_RESOLV_CONF=no`
in `/etc/sysconfig/network/dhcp`, or set
`MODIFY_RESOLV_CONF_DYNAMICALLY=no`
in `/etc/sysconfig/network/config` or
(manually) use `dhcpcd` with `-R` option.
If you only want to keep your searchlist, set: `DHCLIENT_KEEP_SEARCHLIST=yes`
in `/etc/sysconfig/network/dhcp` or (manually) use the `-S` option.

• `pump` DHCP Client

Note: It is not availabel in the SuSE distribution. RedHat uses it as DHCP client.

Syntax: `pump` is started as follows: `pump -i eth0`

Configuration file: `/etc/pump.conf`

```
device eth0 {
     nodns
}
```

The above configuration prevents pump from modifying the `/etc/resolv.conf`

• `dhclient`

Note: The ISC DHCP client daemon `hdclient`, allow for more flexibility than `dhcpcd` or `pump`. It is the client software created by the same authors than the standard ISC DHCP server.

Syntax:

```
dhclient eth0
```

Configuration file:

```
# /etc/dhclient.conf
timeout 60;
retry 30;
interface "eth0" {
     send host-name "harley";
     send dhcp-lease-time 3600;
     prepend domain-name-servers 127.0.0.1;
     request subnet-mask, broadcast-address, routers,
          domain-name, domain-name-servers, host-name;
     require subnet-mask, domain-name-servers;
}
```

In the above configuration file the dhclient will timeout after 60 sec
and will retry 30 times before giving-up.
When asked to configure the `eth0` it will make a request to the DHCP server to:

- Add (prepend) the address 127.0.0.1 to the provided name server list.
- request a subnet mask, a broadcast address, etc
- but will accept the DHCP's response only if it contains a subnet mask and a domain name server address.

Configure Syslog to log DHCP messages

- **Logging of `dhcpcd` client through Syslog:**

You might want to change the default logfile where `syslog` sends DHCP messages to. (By default it goes to `/var/log/messages`.)
To do this, edit your `/etc/syslog.conf` file and add this to it:

```
# Log dhcpcd operations
local7.*                        /var/log/dhcpcd.log
```

IMPORTANT: Remember to use TABS and NOT spaces in your `syslog.conf` file. Otherwise it won't work.

If you don't want the messages in the `/var/log/messages` as well, then you have to add `local7.none` to your `/var/log/messages` line.
eg.

```
# Log anything (except mail) of level info or higher.
# Don't log private authentication messages!
*.info;mail.none;authpriv.none;local7.none /var/log/messages
```

To force `syslogd` to re-read its config file for these changes to take effect, do:

```
killall -HUP syslogd
```

- **What to do when.....**

Request for a NEW IP from the same client (`dhcpcd`)
After a client has requested and obtained an IP from the DHCP server, the client will likely request the same IP on the next startup. If we want to give him another dynamic IP before his lease expires then we need to do the following:

On the server:
- Stop the DHCP server (`rcdhcpd stop`)
- Erase all leases entries of the client from the file:
  `/var/lib/dhcp/db/dhcpd.leases`
- Restart the DHCP server (`rcdhcpd start`)

On the client: (if the client is a Linux)
- Stop the client daemon (`killall dhcpcd`)
- Erase all the client's dhcpcd files
  `/var/lib/dhcpcd/*`
- Restart the `dhcpcd` client daemon (`/sbin/dhcpcd eth0`)
- Verify new dynamic IP (`ifconfig eth0`)

Configuration for Dynamic DNS update

DHCP SERVER

- **DNS SERVER**
  - Include in `/etc/named.conf` the following line in each zone:
    (forward and reverse)
    `allow-update { 127.0.0.1; local_network_IP; };`
    eg.
    `allow-update { 127.0.0.1; 192.168.100.70; };`
  - Make sure that the `/var/lib/named` directory is owned by `named` user because named needs to create and write in a journal file in this directory.
- **DHCP server (version 2 only)**
  - Enter in `/etc/dhcpd.conf: example:`

```
ddns-update-style ad-hoc;
ddns-domainname "linux.site";
zone linux.site. {
    #----- Primary Forward DNS to update
    primary 192.168.100.70;
    }
zone 168.192.in-addr.arpa. {
    #----- Primary Reverse DNS to update
    primary 192.168.100.70;
    }
```

- **DHCP server (version 3) for SuSE 8.0 and up**
  - Enter in `/etc/dhcpd.conf:`

```
ddns-update-style interim;
ddns-updates on;
ddns-domainname "linux.site";
ignore client-updates;
zone linux.site. {
    #----- Primary Forward DNS to update
    primary 192.168.100.70;
    }
zone 168.192.in-addr.arpa. {
    #----- Primary Reverse DNS to update
    primary 192.168.100.70;
    }
```

- **Manually add or remove a Dynamic DNS entry:**

```
nsupdate <enter>
> server 192.168.100.70
> update add newhost.linux.site 3600 A 192.168.100.1
> update delete sunn.linux.site
> <enter>
```

(blank line.....necessary to send the updates!!!)

Note: To verify the dynamic adding/deleting of DNS entries use the commmand:

```
watch -n1 "host -l linux.site 192.168.100.70"
```

Secure DNS Updating:

1) Use the `genDDNSkey` program provided by BIND9 to generate an MD5 Key:

```
genDDNSkey --key-file /etc/named.key --key-name DHCP_UPDATER
```

A key set will be saved in 3 files:

Example:
```
/etc/Kdhcp_updater.+157+37814.key
/etc/Kdhcp_updater.+157+37814.private
/etc/named.key
```

2) **In the DNS Server** : Include the following line in `/etc/named.conf`:

```
include "/etc/named.key";
```

For every zone of `/etc/named.conf` that needs to dynamically update, add the following line:

```
allow-update { key DHCP_UPDATER; };
```

Example:

```
zone "linux.site" in {
        type master;
        file "linux.site.zone";
        allow-update { key DHCP_UPDATER; };
};

zone "168.192.in-addr.arpa" in {
        type master;
        file "192.168.zone";
        allow-update { key DHCP_UPDATER; };
};
```

- If the BIND9 server runs in chroot(probably is), then make a copy of the key file: `/etc/named.key` into chroot jail:

  ```
  cp /etc/named.key /var/lib/named/etc/
  ```

  or add the filename to the list in:

  `NAMED_CONF_INCLUDE_FILES` in `/etc/sysconfig/named` (SuSE only)

  Also change the path of the database files in the zones definitions, and move the database files there:(`/var/lib/named/dyn/`)
  eg.

```
zone "linux.site" in {
        type master;
        file "dyn/linux.site.zone";
        allow-update { key DHCP_UPDATER; };
};

zone "168.192.in-addr.arpa" in {
        type master;
        file "dyn/192.168.zone";
        allow-update { key DHCP_UPDATER; };
};
```

3) **In DHCP Server:**

Insert the following lines in `/etc/dhcpd.conf`

```
ddns-update-style interim;
ddns-updates on;
ddns-domainname "linux.site";
ignore client-updates;
include "/etc/named.key";
```

and in the subnet declaration:

```
subnet 192.168.100.0 netmask 255.255.255.0 {
  range dynamic-bootp 192.168.100.201 192.168.100.219
  zone linux.site {
          primary 127.0.0.1;
          key DHCP_UPDATER; }
  zone 168.192.in-addr.arpa. {
          primary 127.0.0.1;
          key DHCP_UPDATER; }
}
```

Note:

- If the DHCP server runs in chroot(probably is), then make a copy of the key file `/etc/named.key` into chroot jail:

  ```
  cp /etc/named.key /var/lib/dhcp/etc/
  ```

  or add the filename to the list in:
  `DHCPD_CONF_INCLUDE_FILES` in `/etc/sysconfig/dhcpd` (SuSE only)

- To test the protection, use the `nsupdate` shown above and it shouldn't work.

- **Manually add or remove a Dynamic DNS entry using secure update:**
  Note: The key file is the one generated by the `genDDNSkey` program.

  ```
  nsupdate -k /etc/Kdhcp_updater.+157+37814.private <enter>
  > server 192.168.100.70
  > update add newhost.linux.site 3600 A 192.168.100.1
  > update delete sunn.linux.site
  > <enter>
  ```

  (blank line.....necessary to send the updates!!!)

Note: To verify the dynamic adding/deleting of DNS entries use the commmand:

```
watch -n1 "host -l linux.site 192.168.100.70"
```

Linux DHCP CLIENT:

- Variables settings in `/etc/sysconfig/network/dhcp` should be:
  `DHCLIENT_RELEASE_BEFORE_QUIT="yes"`
  (to make sure the client's DNS entry will be released before client shuts down)
  Note: Windows 98 Client does not provoke a release of the Dynamic DNS entry when he shuts down. The following command in a DOS Window or written in a batch file and triggered by an icon on desktop can do the release before shutting down:
  `ipconfig /release_all`

- Start `yast2` and make sure that the IP of network interface is set to: "`dhcpclient`" and not a fixed IP

- Make sure that the `/etc/resolv.conf` has the right DNS address:
  eg.
  `nameserver 192.168.100.70`

- The start/stop of the DHCP client is done through command:
  `rcdhclient start`
  `rcdhclient stop`

Examples of working Dynamic DNS Configuration files:

/etc/dhcpd.conf

```
option nbgrub-menu code 150 = text;

#--------- Dynamic DNS Update section -----------
ddns-update-style interim;
ddns-updates      on;
ddns-domainname   "linux.site";
ignore client-updates;
include           "/etc/named.key";
#------------------------------------------------

# --- default gateway
option routers                  192.168.100.70;
option subnet-mask              255.255.255.0;
option nis-domain               "linux.site";
option domain-name-servers      192.168.100.70;

#     option time-offset            -18000;     # Eastern Standard Time
#     option ntp-servers            192.168.1.1;
#     option netbios-name-servers   192.168.1.1;
# --- Selects point-to-point node (default is hybrid).
#     Don't change this unless you understand Netbios very well
#     option netbios-node-type 2;

subnet 192.168.100.0 netmask 255.255.255.0 {
      range dynamic-bootp 192.168.100.200 192.168.100.220;

      #-------- Dynamic DNS Update section ------------------
      zone linux.site { primary 192.168.100.70; key DHCP_UPDATER; }
      zone 168.192.in-addr.arpa. {
                  primary 192.168.100.70;
                  key DHCP_UPDATER; }
      #------------------------------------------------
      default-lease-time 21600;
      max-lease-time 43200;
#     next-server 10.1.2.1;

#-------------- PXES THIN CLIENT Section -------------------
      filename "pxes/pxes-0.9.nbi";

      host pxes {
        hardware ethernet 00:0C:29:B1:4E:4B;
        fixed-address 192.168.100.201;
        option tftp-server-name "192.168.100.70";
        log(debug, substring(option vendor-class-identifier, 0, 9));
        if substring (option vendor-class-identifier, 0, 9) = "PXEClient" {
            filename "pxes/grub/pxegrub";
            }
        elsif substring (option vendor-class-identifier, 0, 9) = "Etherboot" {
            filename "pxes/grub/nbgrub";
      #option vendor-encapsulated-options 3c:09:45:74:68:65:72:62:6f:6f:74:ff;
            }
        option nbgrub-menu "(nd)pxes/grub/menu.lst";
        option root-path "192.168.100.70:/opt/ltsp/i386";
      }
}
```

/etc/named.conf

```
# Copyright (c) 2001-2003 SuSE Linux AG, Nuernberg, Germany
#
# Author: Frank Bodammer, Lars Mueller <lmuelle@suse.de>
#
# /etc/named.conf
#
# This is a sample configuration file for the name server BIND 9.
#
# A sample configuration for setting up your own domain can be
# found in /usr/share/doc/packages/bind9/sample-config.
#
# A description of all available options can be found in
# /usr/share/doc/packages/bind9/misc/options.

options {

      # The directory statement defines the name server's
      # working directory

      directory "/var/lib/named";

      # The forwarders record contains a list of servers to
      # which queries should be forwarded. Enable this line and
      # modify the IP-address to your provider's name server.
      # Up to three servers may be listed.

      #forwarders { 10.11.12.13; 10.11.12.14; };
      #forwarders { 213.20.148.142; 193.189.244.205; 217.237.151.33; };

      # Enable the next entry to prefer usage of the name
      # server declared in the forwarders section.

      #forward first;

      # The listen-on record contains a list of local network
      # interfaces to listen on. Optionally the port can be
      # specified. Default is to listen on all interfaces found
      # on your system. The default port is 53.

      #listen-on port 53 { 127.0.0.1; };

      # The listen-on-v6 record enables or disables listening
      # on IPV6 interfaces. Allowed values are 'any' and 'none'
      # or a list of addresses. IPv6 can only be used with
      # kernel 2.4 in this release.

      listen-on-v6 { any; };

      # The next three statements may be needed if a firewall
      # stands between the local server and the internet.

      #query-source address * port 53;
      #transfer-source * port 53;
      #notify-source * port 53;

      # The allow-query record contains a list of networks or
      # IP-addresses to accept and deny queries from. The
      # default is to allow queries from all hosts.
      #allow-query { 127.0.0.1; };

      # If notify is set to yes (default), notify messages are
      # sent to other name servers when the the zone data is
```

```
      # changed. Instead of setting a global 'notify' statement
      # in the 'options' section, a separate 'notify' can be
      # added to each zone definition.

      notify no;
};

# Remove the leading '#' characters if you want a log of the queries send to
# your name server. The log file size is limited to 100 MB.
#logging {
#     channel query_logging {
#           file "/var/log/named_querylog"
#                 versions 3 size 100M;
#           print-time yes;               // timestamp log entries
#     };
#     category queries {
#           query_logging;
#     };
#     category lame-servers { null; };
#};

# The following zone definitions don't need any modification.
# The first one is the definition of the root name servers.
# The second one defines localhost while the third defines the reverse lookup
# for localhost.

zone "." in {
      type hint;
      file "root.hint";
};

zone "localhost" in {
      type master;
      file "localhost.zone";
};

zone "0.0.127.in-addr.arpa" in {
      type master;
      file "127.0.0.zone";
};

# You can insert further zone records for your own domains below.

include "/etc/named.key";

zone "linux.site" in {
      type master;
      file "dyn/linux.site.zone";
#     allow-update { 127.0.0.1; 192.168.100.70; };
      allow-update { key DHCP_UPDATER; };

};

zone "168.192.in-addr.arpa" in {
      type master;
      file "dyn/192.168.zone";
#     allow-update { 127.0.0.1; 192.168.100.70; };
      allow-update { key DHCP_UPDATER; };
};
```