Prof. Dr. Christian Schindelhauer
Hoor K. Al-Hasani, Elmar Haussmann

Freiburg, 18-11-2009

Practical Exercises

Communication Systems (Rechnernetze II)

Topic IP/DHCP Solution

Exercise 1:

1. `user@host: $ sudo avahi-autoipd ethX`
   The result would look like:
   ```
   Found user 'avahi-autoipd' (UID 104) and group 'avahi-autoipd'
   (GID 110). Successfully called chroot().
   Successfully dropped root privileges.
   Starting with address xx.xx.xx.xx
   Callout BIND, address xx.xx.xx.xx on interface ethX
   Successfully claimed IP address xx.xx.xx.xx
   ```

2. `user@host: $ sudo avahi-browse -a -t`
   The result would look for example like:
   ```
   + wlanX IPv4 USER-LAPTOP-4 [00:50:56:00:10:0e] Workstation
   + ethX IPv4 RANDUSR [dd:21:66:61:7c:fd] Workstation
   ...
   ```
   You can also see Multicast DNS (mDNS) packets in wireshark. mDNS allows resolving names into IP addresses without a central DNS server.

Exercise 2:

1. Configure the dhcp server.
   - `gedit /etc/dhcp3/dhcpd.conf`
   - Change e.g. the subnet configuration starting in line 54 to:
     ```
     subnet 10.5.5.1 netmask 255.255.255.224 {
     range 10.5.5.26 10.5.5.30;
     option domain-name-servers ns1.internal.example.org;
     option domain-name "internal.example.org";
     option routers 10.5.5.2;
     option broadcast-address 10.5.5.31;
     default-lease-time 600;
     max-lease-time 7200;
     }
     ```
   - `sudo /etc/init.d/dhcp3-server restart`

2. `sudo dhclient ethX`
   To avoid server load and keep implementation simple the client is responsible for the renew process. There are no keep-alive packets between the server and the client. If the client doesn't respond within the lease-time provided the server assumes the client is no longer on the network and the IP address is available for other clients again.
   In general the answer of a DHCP server can't be trusted. Imagine an attacker is able to introduce a DHCP server into a network and can configure the clients' gateway address. This gives rise to a man-in-the-middle attack, allowing the attacker to see all traffic going through the gateway.

3. `sudo gedit /etc/dhcp3/dhclient.conf`
   `interface "ethX" {send dhcp-requested-address 10.230.4.255;}`
   Look at the packets in wireshark in the details section.
   Remember to delete it again afterwards.

4. `cat /var/lib/dhcp3/dhclient-ethX.lease`

5. Add the following options to your dhcpd.conf in the subnet section:

   - `host test {hardware ethernet 00:00:00:00:00:00; fixed-address XX.XX.XX.XX;}`
     use the hardware address of the client, who will receive the same IP address every time he joins the network.

6. `option ntp-server XX.XX.XX.XX;`
   check the lease file of the client.

After each change in the configuration, save the file and restart the DHCP server:

```
sudo /etc/init.d/dhcp3-server restart
sudo dhclient ethX
```