Report 2: DHCP Relay

Bram Gotink – Michiel Staessen

End-user documentation

The Dynamic Host Configuration Protocol (DHCP) is used to hand out network configuration to new clients in a network. When network capabilities on the client are turned on, it sends a broadcast message in its subnet. This DHCPDISCOVER message is a UDP sent to port 67, originating from port 68. If a DHCP server is present in the subnet, it will answer the request with the appropriate network settings and the host will configure itself (see figure 1).

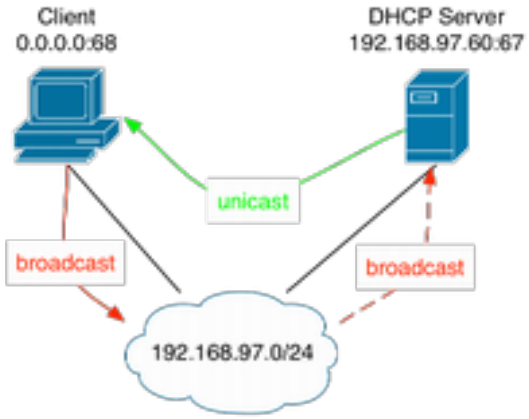

Figure 1: the DHCP protocol with the server in the same subnet

In large networks, it is not practical and sometimes not desirable to install a DHCP server in every subnet but on the other hand, broadcast messages cannot cross the subnet boundaries, i.e. routers. In these cases, a DHCP relay is used. The relay will forward DHCP broadcast messages of clients in its subnet to the DHCP server using unicast (see figure 2).

In order to get this setup working, some configuration is required.
First, the relay must know the IP address of the DHCP server and the MAC address of the gateway. The MAC address is needed because you cannot alter routing tables on the PIC and thus you have to do some layer 2 networking. The relay must also have a static IP address such that the DHCP server can send answers to the relay.
Second, the DHCP server needs a route to the clients network. Otherwise, it cannot know where to send the message.

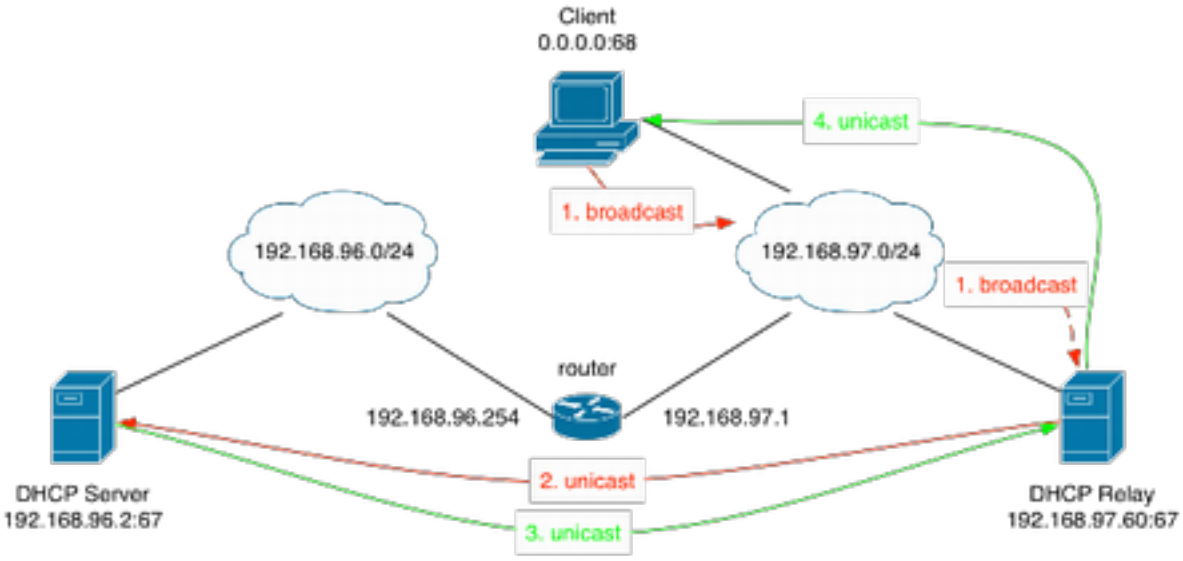

Figure 2: the DHCP protocol with one relay

Also, make sure there are no other DHCP servers or relays running on the same network and that Network Address Translation (NAT) is disabled on the router. If NAT is enabled, the DHCP server will reject the incoming DHCP packets because they originate from a random source port.

System engineer documentation

Configuring the program

The program needs to be configured before compiling it. All configuration is done in `DHCPRelayConfig.h`. This file contains the IP address and MAC of the relay, the netmask and default gateway IP of the network, the IP address of the DHCP server and finally the MAC address of the default gateway.

To install the program on a PIC controller, two steps have to be taken. First, the source code has to be compiled into an executable. This is done by simply running `` `make` `` in the source directory. Afterwards, the executable must be uploaded to the PIC.
This is done by opening a terminal in the source directory, and running:

```
$ tftp 192.168.97.60
> binary
> trace
> verbose
```

Press the reset button on the PIC board and wait for the activity light on the router to light up. Now run

```
> put Main.hex
```

After the upload, the program will run.

Testing the program

The test configuration currently configured can be tested as follows:
Start the router and the PIC board, connect the PIC to the router. It will take address `192.168.97.60`. Plug a computer in the router, but not on the WAN-port. Use a static IP in the `192.168.97/24` range to upload the program as described above.
Next, unplug the computer, change the IP address to `192.168.96.2` and plug it in the WAN port (port 1) of the router.
All traffic on the DHCP server can be logged using '`tcpdump -vvv -i <iface>`', with `<iface>` the interface connected to the WAN port of the router.
Finally, connect a different computer to the router and request an IP address using DHCP. Most operating systems will do this automatically, unless they're configured not to. The computer will get an IP address in the `192.168.97/24` IP range. The output of `tcpdump` will show the packets sent and received on the server.

Programmer documentation

Specification

The program has only one responsibility: forwarding DHCP packets. When a package from the client is received, it is forwarded to the server. When a package from the server is received, it is forwarded to the client. This behaviour is summarized in an ASG diagram in figure 3.

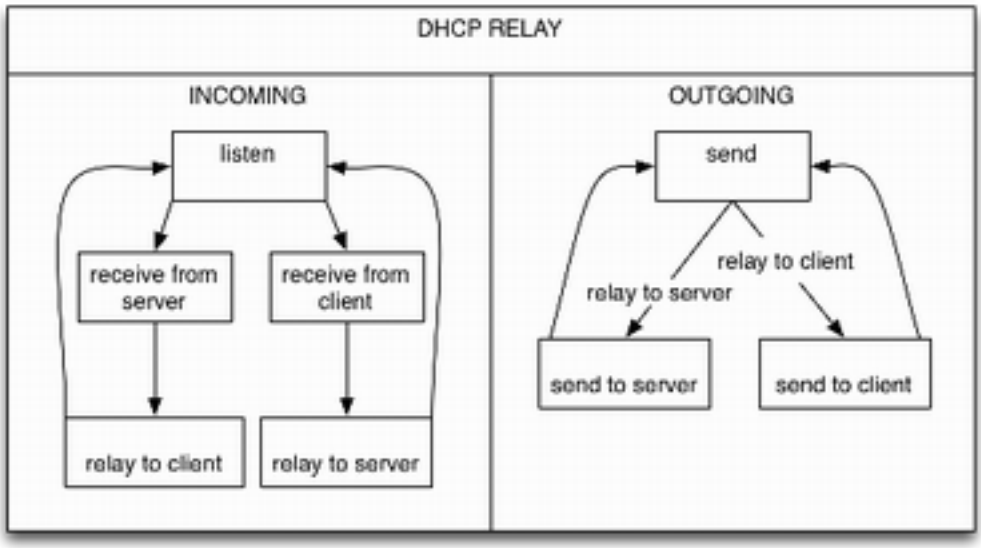

Figure 3: Overview of the program in ASG

Implementation details

Clients send broadcast messages, originating from port 68 to port 67. A DHCP server or relay listen on port 67 and can answer these requests. When a relay forwards a DHCP packet, the source port is altered to 67. This is one way for the server to know that the packet is forwarded through a relay. The relay also encodes its IP address in the DHCP packet (in the GIADDR field). The DHCP server can use that address to determine from which pool it should allocate an IP address.
The relay does no more than forward these DHCP packets. There is no checking whether the package is indeed a DHCP packet, or if the packet is valid. The implementation sets the GIADDR and forwards the packet, no other actions are taken.

No client routing information is saved by the relay. The address information of the client is taken from the DHCP packets sent by the server. This is only the MAC address, as the client doesn't have an IP address yet. The only route stored on the relay is the route to the server.