When first setting out on this lab, I had to make sure that there were no DHCP leases given out or saved in the router. So, the first thing that had to be done was to erase the dhcpd.leases and dhcpd.leases~ files. After that was done then the BackTracker machine was turned on and I created the packet that would be sent to the router to starve all the IP addresses that it had in its pool. The code I wrote went through and requested each IP address in the pool 10.10.111.100 to 10.10.111.200 but I skipped over the address 10.10.111.107 because that was the address that was being used by the BackTracker machine I was using. I noticed on WireShark that just running my attack once wasn't getting all the IP's from the pool, so I added a for loop to the beginning of the code so that it would run four times every time I implement to attack. Again, I noticed that all the IP's were not being taken from the router so I made sure to run the attack twice, which was basically the same as running it 8 different times. This did the trick and I was able to bind all the IP addresses from the pool to random MAC address.

Figure 1: The starvation code

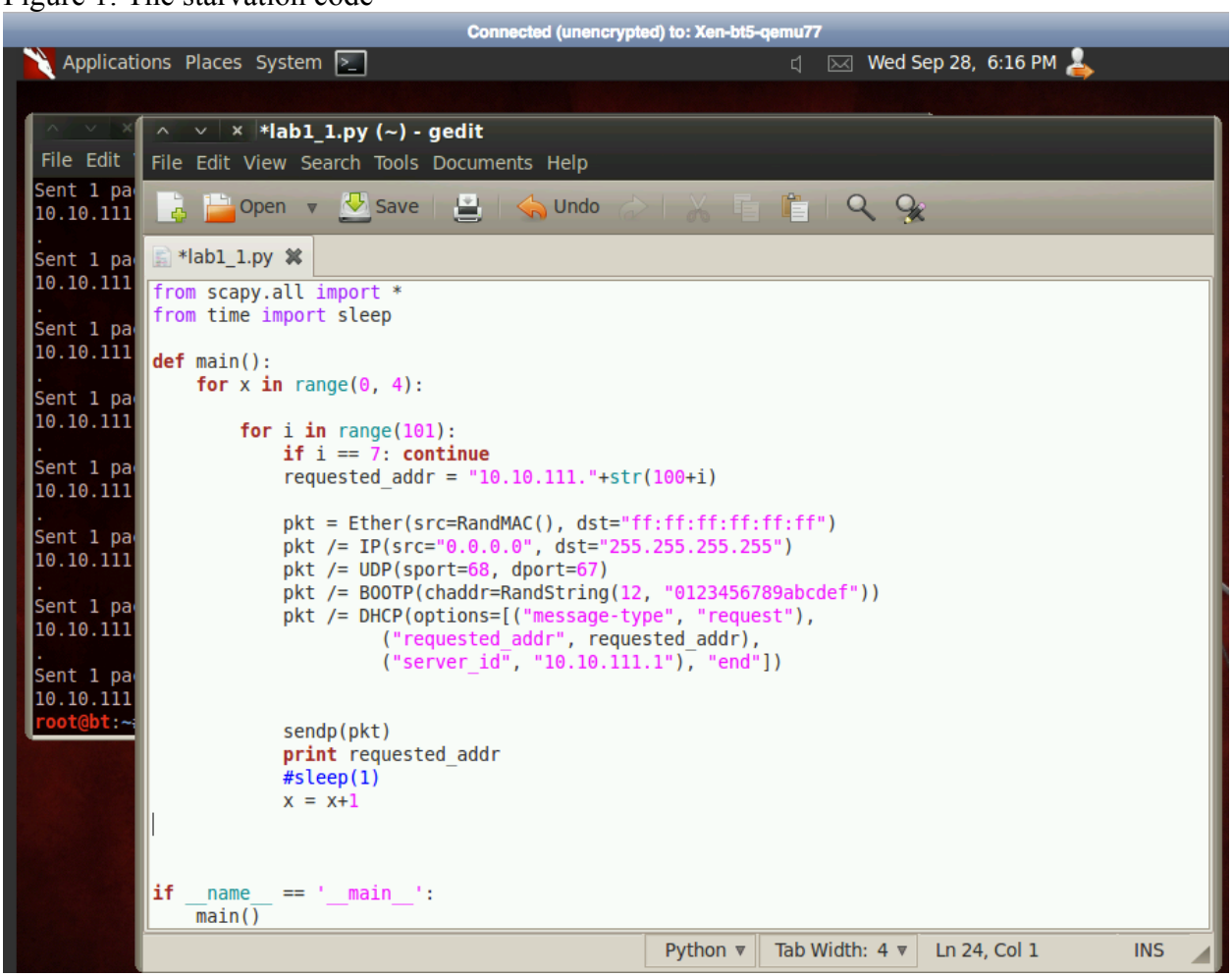


Figure 2: Router showing both lease files before the attack

```
Connected (unencrypted) to: Xen-rtr_new_base77

router login: root
Password:
Last login: Sun Sep 25 13:15:29 EDT 2016 on tty1
Linux router 2.6.26-2-amd64 #1 SMP Thu Feb 11 00:59:32 UTC 2010 x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
router:~# cd /var/lib/dhcp3
router:/var/lib/dhcp3# ls
dhclient.eth0.leases  dhclient.leases  dhcpd.leases  dhcpd.leases~
router:/var/lib/dhcp3# more dhcpd.leases
# The format of this file is documented in the dhcpd.leases(5) manual page.
# This lease file was written by isc-dhcp-V3.1.1

router:/var/lib/dhcp3# more dhcpd.leases~
# The format of this file is documented in the dhcpd.leases(5) manual page.
# This lease file was written by isc-dhcp-V3.1.1


router:/var/lib/dhcp3# _
```

Figure 3 - 36: Router after the attack (the IP addresses are not in order since I had to run it multiple times to bind them all)

```
Connected (unencrypted) to: Xen-rtr_new_base77
# The format of this file is documented in the dhcpd.leases(5) manual page.
# This lease file was written by isc-dhcp-V3.1.1

lease 10.10.111.107 {
  starts 1 2016/09/26 03:48:16;
  ends 1 2016/09/26 04:48:16;
  cltt 1 2016/09/26 03:48:16;
  binding state active;
  next binding state free;
  hardware ethernet 02:00:4d:42:0b:01;
  client-hostname "bt";
}
lease 10.10.111.101 {
  starts 1 2016/09/26 03:48:38;
  ends 1 2016/09/26 04:48:38;
  cltt 1 2016/09/26 03:48:38;
  binding state active;
  next binding state free;
  hardware ethernet 61:38:62:39:63:62;
}
lease 10.10.111.102 {
  starts 1 2016/09/26 03:48:38;
  ends 1 2016/09/26 04:48:38;
  cltt 1 2016/09/26 03:48:38;
--More--(3%)_
```

Connected (unencrypted) to: Xen-rtr_new_base77

```
  binding state active;
  next binding state free;
  hardware ethernet 37:61:34:39:39:63;
}
lease 10.10.111.105 {
  starts 1 2016/09/26 03:48:38;
  ends 1 2016/09/26 04:48:38;
  cltt 1 2016/09/26 03:48:38;
  binding state active;
  next binding state free;
  hardware ethernet 35:39:32:61:36:33;
}
lease 10.10.111.106 {
  starts 1 2016/09/26 03:48:38;
  ends 1 2016/09/26 04:48:38;
  cltt 1 2016/09/26 03:48:38;
  binding state active;
  next binding state free;
  hardware ethernet 65:39:34:36:30:33;
}
lease 10.10.111.108 {
  starts 1 2016/09/26 03:48:38;
  ends 1 2016/09/26 04:48:38;
  cltt 1 2016/09/26 03:48:38;
--More--(6%)
```

Connected (unencrypted) to: Xen-rtr_new_base77

```
  binding state active;
  next binding state free;
  hardware ethernet 39:30:36:38:64:36;
}
lease 10.10.111.109 {
  starts 1 2016/09/26 03:48:38;
  ends 1 2016/09/26 04:48:38;
  cltt 1 2016/09/26 03:48:38;
  binding state active;
  next binding state free;
  hardware ethernet 30:32:37:36:36:39;
}
lease 10.10.111.110 {
  starts 1 2016/09/26 03:48:38;
  ends 1 2016/09/26 04:48:38;
  cltt 1 2016/09/26 03:48:38;
  binding state active;
  next binding state free;
  hardware ethernet 32:65:31:31:38:37;
}
lease 10.10.111.112 {
  starts 1 2016/09/26 03:48:38;
  ends 1 2016/09/26 04:48:38;
  cltt 1 2016/09/26 03:48:38;
--More--(9%)_
```

Connected (unencrypted) to: Xen-rtr_new_base77

```
  binding state active;
  next binding state free;
  hardware ethernet 62:62:63:39:37:66;
}
lease 10.10.111.113 {
  starts 1 2016/09/26 03:48:38;
  ends 1 2016/09/26 04:48:38;
  cltt 1 2016/09/26 03:48:38;
  binding state active;
  next binding state free;
  hardware ethernet 30:63:62:62:31:61;
}
lease 10.10.111.115 {
  starts 1 2016/09/26 03:48:38;
  ends 1 2016/09/26 04:48:38;
  cltt 1 2016/09/26 03:48:38;
  binding state active;
  next binding state free;
  hardware ethernet 33:62:31:37:61:38;
}
lease 10.10.111.116 {
  starts 1 2016/09/26 03:48:38;
  ends 1 2016/09/26 04:48:38;
  cltt 1 2016/09/26 03:48:38;
--More--(12%)_
```

Connected (unencrypted) to: Xen-rtr_new_base77

```
  binding state active;
  next binding state free;
  hardware ethernet 61:31:30:35:37:34;
}
lease 10.10.111.118 {
  starts 1 2016/09/26 03:48:38;
  ends 1 2016/09/26 04:48:38;
  cltt 1 2016/09/26 03:48:38;
  binding state active;
  next binding state free;
  hardware ethernet 33:32:38:66:34:38;
}
lease 10.10.111.121 {
  starts 1 2016/09/26 03:48:39;
  ends 1 2016/09/26 04:48:39;
  cltt 1 2016/09/26 03:48:39;
  binding state active;
  next binding state free;
  hardware ethernet 31:64:66:62:63:61;
}
lease 10.10.111.122 {
  starts 1 2016/09/26 03:48:39;
  ends 1 2016/09/26 04:48:39;
  cltt 1 2016/09/26 03:48:39;
--More--(15%)_
```

Connected (unencrypted) to: Xen-rtr_new_base77

```
  binding state active;
  next binding state free;
  hardware ethernet 64:31:39:36:32:33;
}
lease 10.10.111.124 {
  starts 1 2016/09/26 03:48:39;
  ends 1 2016/09/26 04:48:39;
  cltt 1 2016/09/26 03:48:39;
  binding state active;
  next binding state free;
  hardware ethernet 39:65:66:31:36:31;
}
lease 10.10.111.127 {
  starts 1 2016/09/26 03:48:39;
  ends 1 2016/09/26 04:48:39;
  cltt 1 2016/09/26 03:48:39;
  binding state active;
  next binding state free;
  hardware ethernet 66:66:61:65:36:34;
}
lease 10.10.111.128 {
  starts 1 2016/09/26 03:48:39;
  ends 1 2016/09/26 04:48:39;
  cltt 1 2016/09/26 03:48:39;
--More--(17%)
```

Connected (unencrypted) to: Xen-rtr_new_base77

```
  binding state active;
  next binding state free;
  hardware ethernet 64:33:66:35:62:65;
}
lease 10.10.111.130 {
  starts 1 2016/09/26 03:48:39;
  ends 1 2016/09/26 04:48:39;
  cltt 1 2016/09/26 03:48:39;
  binding state active;
  next binding state free;
  hardware ethernet 64:38:62:36:30:35;
}
lease 10.10.111.131 {
  starts 1 2016/09/26 03:48:39;
  ends 1 2016/09/26 04:48:39;
  cltt 1 2016/09/26 03:48:39;
  binding state active;
  next binding state free;
  hardware ethernet 61:32:35:33:33:35;
}
lease 10.10.111.133 {
  starts 1 2016/09/26 03:48:40;
  ends 1 2016/09/26 04:48:40;
  cltt 1 2016/09/26 03:48:40;
--More--(20%)
```

Connected (unencrypted) to: Xen-rtr_new_base77

```
  binding state active;
  next binding state free;
  hardware ethernet 64:38:63:32:33:31;
}
lease 10.10.111.136 {
  starts 1 2016/09/26 03:48:40;
  ends 1 2016/09/26 04:48:40;
  cltt 1 2016/09/26 03:48:40;
  binding state active;
  next binding state free;
  hardware ethernet 31:30:35:36:30:62;
}
lease 10.10.111.138 {
  starts 1 2016/09/26 03:48:40;
  ends 1 2016/09/26 04:48:40;
  cltt 1 2016/09/26 03:48:40;
  binding state active;
  next binding state free;
  hardware ethernet 64:34:61:65:39:30;
}
lease 10.10.111.139 {
  starts 1 2016/09/26 03:48:40;
  ends 1 2016/09/26 04:48:40;
  cltt 1 2016/09/26 03:48:40;
--More--(23%)_
```

Connected (unencrypted) to: Xen-rtr_new_base77

```
  binding state active;
  next binding state free;
  hardware ethernet 63:37:37:35:37:33;
}
lease 10.10.111.141 {
  starts 1 2016/09/26 03:48:40;
  ends 1 2016/09/26 04:48:40;
  cltt 1 2016/09/26 03:48:40;
  binding state active;
  next binding state free;
  hardware ethernet 62:37:31:61:65:30;
}
lease 10.10.111.143 {
  starts 1 2016/09/26 03:48:40;
  ends 1 2016/09/26 04:48:40;
  cltt 1 2016/09/26 03:48:40;
  binding state active;
  next binding state free;
  hardware ethernet 63:39:30:65:31:30;
}
lease 10.10.111.145 {
  starts 1 2016/09/26 03:48:40;
  ends 1 2016/09/26 04:48:40;
  cltt 1 2016/09/26 03:48:40;
--More--(26%)_
```

Connected (unencrypted) to: Xen-rtr_new_base77

```
  binding state active;
  next binding state free;
  hardware ethernet 62:37:36:38:30:39;
}
lease 10.10.111.146 {
  starts 1 2016/09/26 03:48:41;
  ends 1 2016/09/26 04:48:41;
  cltt 1 2016/09/26 03:48:41;
  binding state active;
  next binding state free;
  hardware ethernet 35:36:34:35:62:32;
}
lease 10.10.111.148 {
  starts 1 2016/09/26 03:48:41;
  ends 1 2016/09/26 04:48:41;
  cltt 1 2016/09/26 03:48:41;
  binding state active;
  next binding state free;
  hardware ethernet 39:64:34:34:30:32;
}
lease 10.10.111.150 {
  starts 1 2016/09/26 03:48:41;
  ends 1 2016/09/26 04:48:41;
  cltt 1 2016/09/26 03:48:41;
--More--(29%)
```

Connected (unencrypted) to: Xen-rtr_new_base77

```
  binding state active;
  next binding state free;
  hardware ethernet 36:35:30:65:63:62;
}
lease 10.10.111.153 {
  starts 1 2016/09/26 03:48:41;
  ends 1 2016/09/26 04:48:41;
  cltt 1 2016/09/26 03:48:41;
  binding state active;
  next binding state free;
  hardware ethernet 64:32:64:64:65:61;
}
lease 10.10.111.158 {
  starts 1 2016/09/26 03:48:41;
  ends 1 2016/09/26 04:48:41;
  cltt 1 2016/09/26 03:48:41;
  binding state active;
  next binding state free;
  hardware ethernet 37:35:37:31:30:64;
}
lease 10.10.111.159 {
  starts 1 2016/09/26 03:48:41;
  ends 1 2016/09/26 04:48:41;
  cltt 1 2016/09/26 03:48:41;
--More--(32%)
```

Connected (unencrypted) to: Xen-rtr_new_base77

```
  binding state active;
  next binding state free;
  hardware ethernet 36:33:66:32:38:36;
}
lease 10.10.111.162 {
  starts 1 2016/09/26 03:48:42;
  ends 1 2016/09/26 04:48:42;
  cltt 1 2016/09/26 03:48:42;
  binding state active;
  next binding state free;
  hardware ethernet 31:37:33:65:61:37;
}
lease 10.10.111.165 {
  starts 1 2016/09/26 03:48:42;
  ends 1 2016/09/26 04:48:42;
  cltt 1 2016/09/26 03:48:42;
  binding state active;
  next binding state free;
  hardware ethernet 32:66:37:33:65:61;
}
lease 10.10.111.166 {
  starts 1 2016/09/26 03:48:42;
  ends 1 2016/09/26 04:48:42;
  cltt 1 2016/09/26 03:48:42;
--More--(35%)
```

Connected (unencrypted) to: Xen-rtr_new_base77

```
  binding state active;
  next binding state free;
  hardware ethernet 34:35:35:35:30:34;
}
lease 10.10.111.168 {
  starts 1 2016/09/26 03:48:42;
  ends 1 2016/09/26 04:48:42;
  cltt 1 2016/09/26 03:48:42;
  binding state active;
  next binding state free;
  hardware ethernet 38:66:36:31:66:37;
}
lease 10.10.111.170 {
  starts 1 2016/09/26 03:48:42;
  ends 1 2016/09/26 04:48:42;
  cltt 1 2016/09/26 03:48:42;
  binding state active;
  next binding state free;
  hardware ethernet 30:32:39:30:38:63;
}
lease 10.10.111.171 {
  starts 1 2016/09/26 03:48:42;
  ends 1 2016/09/26 04:48:42;
  cltt 1 2016/09/26 03:48:42;
--More--(38%)
```

Connected (unencrypted) to: Xen-rtr_new_base77

```
  binding state active;
  next binding state free;
  hardware ethernet 63:62:62:66:39:35;
}
lease 10.10.111.174 {
  starts 1 2016/09/26 03:48:42;
  ends 1 2016/09/26 04:48:42;
  cltt 1 2016/09/26 03:48:42;
  binding state active;
  next binding state free;
  hardware ethernet 64:61:64:63:36:63;
}
lease 10.10.111.179 {
  starts 1 2016/09/26 03:48:43;
  ends 1 2016/09/26 04:48:43;
  cltt 1 2016/09/26 03:48:43;
  binding state active;
  next binding state free;
  hardware ethernet 37:61:31:66:30:61;
}
lease 10.10.111.182 {
  starts 1 2016/09/26 03:48:43;
  ends 1 2016/09/26 04:48:43;
  cltt 1 2016/09/26 03:48:43;
--More--(41%)
```

Connected (unencrypted) to: Xen-rtr_new_base77

```
  binding state active;
  next binding state free;
  hardware ethernet 64:61:39:37:35:64;
}
lease 10.10.111.183 {
  starts 1 2016/09/26 03:48:43;
  ends 1 2016/09/26 04:48:43;
  cltt 1 2016/09/26 03:48:43;
  binding state active;
  next binding state free;
  hardware ethernet 64:65:61:66:34:35;
}
lease 10.10.111.185 {
  starts 1 2016/09/26 03:48:43;
  ends 1 2016/09/26 04:48:43;
  cltt 1 2016/09/26 03:48:43;
  binding state active;
  next binding state free;
  hardware ethernet 64:33:37:34:37:32;
}
lease 10.10.111.186 {
  starts 1 2016/09/26 03:48:43;
  ends 1 2016/09/26 04:48:43;
  cltt 1 2016/09/26 03:48:43;
--More--(44%)
```

Connected (unencrypted) to: Xen-rtr_new_base77

```
  binding state active;
  next binding state free;
  hardware ethernet 35:34:33:31:62:38;
}
lease 10.10.111.189 {
  starts 1 2016/09/26 03:48:43;
  ends 1 2016/09/26 04:48:43;
  cltt 1 2016/09/26 03:48:43;
  binding state active;
  next binding state free;
  hardware ethernet 63:33:62:62:31:30;
}
lease 10.10.111.193 {
  starts 1 2016/09/26 03:48:44;
  ends 1 2016/09/26 04:48:44;
  cltt 1 2016/09/26 03:48:44;
  binding state active;
  next binding state free;
  hardware ethernet 38:35:34:35:64:66;
}
lease 10.10.111.194 {
  starts 1 2016/09/26 03:48:44;
  ends 1 2016/09/26 04:48:44;
  cltt 1 2016/09/26 03:48:44;
--More--(47%)_
```

Connected (unencrypted) to: Xen-rtr_new_base77

```
  binding state active;
  next binding state free;
  hardware ethernet 66:35:32:35:64:66;
}
lease 10.10.111.195 {
  starts 1 2016/09/26 03:48:44;
  ends 1 2016/09/26 04:48:44;
  cltt 1 2016/09/26 03:48:44;
  binding state active;
  next binding state free;
  hardware ethernet 62:37:30:62:34:30;
}
lease 10.10.111.197 {
  starts 1 2016/09/26 03:48:44;
  ends 1 2016/09/26 04:48:44;
  cltt 1 2016/09/26 03:48:44;
  binding state active;
  next binding state free;
  hardware ethernet 66:36:32:39:31:30;
}
lease 10.10.111.198 {
  starts 1 2016/09/26 03:48:44;
  ends 1 2016/09/26 04:48:44;
  cltt 1 2016/09/26 03:48:44;
--More--(50%)_
```

Connected (unencrypted) to: Xen-rtr_new_base77

```
  binding state active;
  next binding state free;
  hardware ethernet 37:35:37:65:63:36;
}
lease 10.10.111.103 {
  starts 1 2016/09/26 03:48:44;
  ends 1 2016/09/26 04:48:44;
  cltt 1 2016/09/26 03:48:44;
  binding state active;
  next binding state free;
  hardware ethernet 39:64:32:62:38:66;
}
lease 10.10.111.117 {
  starts 1 2016/09/26 03:48:45;
  ends 1 2016/09/26 04:48:45;
  cltt 1 2016/09/26 03:48:45;
  binding state active;
  next binding state free;
  hardware ethernet 38:35:65:65:34:34;
}
lease 10.10.111.126 {
  starts 1 2016/09/26 03:48:46;
  ends 1 2016/09/26 04:48:46;
  cltt 1 2016/09/26 03:48:46;
--More--(53%)
```

Connected (unencrypted) to: Xen-rtr_new_base77

```
  binding state active;
  next binding state free;
  hardware ethernet 32:66:35:31:61:34;
}
lease 10.10.111.132 {
  starts 1 2016/09/26 03:48:46;
  ends 1 2016/09/26 04:48:46;
  cltt 1 2016/09/26 03:48:46;
  binding state active;
  next binding state free;
  hardware ethernet 32:63:34:62:33:61;
}
lease 10.10.111.142 {
  starts 1 2016/09/26 03:48:47;
  ends 1 2016/09/26 04:48:47;
  cltt 1 2016/09/26 03:48:47;
  binding state active;
  next binding state free;
  hardware ethernet 39:32:34:35:38:33;
}
lease 10.10.111.144 {
  starts 1 2016/09/26 03:48:47;
  ends 1 2016/09/26 04:48:47;
  cltt 1 2016/09/26 03:48:47;
--More--(56%)
```

Connected (unencrypted) to: Xen-rtr_new_base77

```
  binding state active;
  next binding state free;
  hardware ethernet 65:62:34:32:61:62;
}
lease 10.10.111.147 {
  starts 1 2016/09/26 03:48:47;
  ends 1 2016/09/26 04:48:47;
  cltt 1 2016/09/26 03:48:47;
  binding state active;
  next binding state free;
  hardware ethernet 34:32:66:63:63:32;
}
lease 10.10.111.149 {
  starts 1 2016/09/26 03:48:47;
  ends 1 2016/09/26 04:48:47;
  cltt 1 2016/09/26 03:48:47;
  binding state active;
  next binding state free;
  hardware ethernet 32:34:35:33:32:32;
}
lease 10.10.111.151 {
  starts 1 2016/09/26 03:48:48;
  ends 1 2016/09/26 04:48:48;
  cltt 1 2016/09/26 03:48:48;
--More--(59%)_
```

Connected (unencrypted) to: Xen-rtr_new_base77

```
  binding state active;
  next binding state free;
  hardware ethernet 38:32:66:61:34:64;
}
lease 10.10.111.161 {
  starts 1 2016/09/26 03:48:48;
  ends 1 2016/09/26 04:48:48;
  cltt 1 2016/09/26 03:48:48;
  binding state active;
  next binding state free;
  hardware ethernet 66:30:32:30:37:66;
}
lease 10.10.111.163 {
  starts 1 2016/09/26 03:48:48;
  ends 1 2016/09/26 04:48:48;
  cltt 1 2016/09/26 03:48:48;
  binding state active;
  next binding state free;
  hardware ethernet 63:66:31:34:61:65;
}
lease 10.10.111.164 {
  starts 1 2016/09/26 03:48:48;
  ends 1 2016/09/26 04:48:48;
  cltt 1 2016/09/26 03:48:48;
--More--(62%)_
```

Connected (unencrypted) to: Xen-rtr_new_base77

```
  binding state active;
  next binding state free;
  hardware ethernet 31:63:61:62:35:37;
}
lease 10.10.111.176 {
  starts 1 2016/09/26 03:48:49;
  ends 1 2016/09/26 04:48:49;
  cltt 1 2016/09/26 03:48:49;
  binding state active;
  next binding state free;
  hardware ethernet 64:63:63:30:39:61;
}
lease 10.10.111.181 {
  starts 1 2016/09/26 03:48:50;
  ends 1 2016/09/26 04:48:50;
  cltt 1 2016/09/26 03:48:50;
  binding state active;
  next binding state free;
  hardware ethernet 32:62:35:32:33:37;
}
lease 10.10.111.187 {
  starts 1 2016/09/26 03:48:50;
  ends 1 2016/09/26 04:48:50;
  cltt 1 2016/09/26 03:48:50;
--More--(65%)_
```

Connected (unencrypted) to: Xen-rtr_new_base77

```
  binding state active;
  next binding state free;
  hardware ethernet 30:33:62:64:66:62;
}
lease 10.10.111.196 {
  starts 1 2016/09/26 03:48:51;
  ends 1 2016/09/26 04:48:51;
  cltt 1 2016/09/26 03:48:51;
  binding state active;
  next binding state free;
  hardware ethernet 39:32:37:38:32:37;
}
lease 10.10.111.104 {
  starts 1 2016/09/26 03:48:51;
  ends 1 2016/09/26 04:48:51;
  cltt 1 2016/09/26 03:48:51;
  binding state active;
  next binding state free;
  hardware ethernet 31:30:32:30:31:30;
}
lease 10.10.111.111 {
  starts 1 2016/09/26 03:48:52;
  ends 1 2016/09/26 04:48:52;
  cltt 1 2016/09/26 03:48:52;
--More--(68%)_
```

Connected (unencrypted) to: Xen-rtr_new_base77

```
  binding state active;
  next binding state free;
  hardware ethernet 65:34:64:39:63:34;
}
lease 10.10.111.114 {
  starts 1 2016/09/26 03:48:52;
  ends 1 2016/09/26 04:48:52;
  cltt 1 2016/09/26 03:48:52;
  binding state active;
  next binding state free;
  hardware ethernet 35:38:36:34:33:65;
}
lease 10.10.111.119 {
  starts 1 2016/09/26 03:48:52;
  ends 1 2016/09/26 04:48:52;
  cltt 1 2016/09/26 03:48:52;
  binding state active;
  next binding state free;
  hardware ethernet 63:30:64:32:35:66;
}
lease 10.10.111.120 {
  starts 1 2016/09/26 03:48:52;
  ends 1 2016/09/26 04:48:52;
  cltt 1 2016/09/26 03:48:52;
--More--(71%)
```

Connected (unencrypted) to: Xen-rtr_new_base77

```
  binding state active;
  next binding state free;
  hardware ethernet 63:62:32:61:61:32;
}
lease 10.10.111.123 {
  starts 1 2016/09/26 03:48:52;
  ends 1 2016/09/26 04:48:52;
  cltt 1 2016/09/26 03:48:52;
  binding state active;
  next binding state free;
  hardware ethernet 33:34:63:35:65:32;
}
lease 10.10.111.125 {
  starts 1 2016/09/26 03:48:52;
  ends 1 2016/09/26 04:48:52;
  cltt 1 2016/09/26 03:48:52;
  binding state active;
  next binding state free;
  hardware ethernet 61:66:66:31:34:30;
}
lease 10.10.111.135 {
  starts 1 2016/09/26 03:48:53;
  ends 1 2016/09/26 04:48:53;
  cltt 1 2016/09/26 03:48:53;
--More--(74%)
```

Connected (unencrypted) to: Xen-rtr_new_base77

```
  binding state active;
  next binding state free;
  hardware ethernet 35:61:65:31:31:63;
}
lease 10.10.111.140 {
  starts 1 2016/09/26 03:48:54;
  ends 1 2016/09/26 04:48:54;
  cltt 1 2016/09/26 03:48:54;
  binding state active;
  next binding state free;
  hardware ethernet 65:34:37:61:66:33;
}
lease 10.10.111.152 {
  starts 1 2016/09/26 03:48:55;
  ends 1 2016/09/26 04:48:55;
  cltt 1 2016/09/26 03:48:55;
  binding state active;
  next binding state free;
  hardware ethernet 33:33:35:34:66:33;
}
lease 10.10.111.172 {
  starts 1 2016/09/26 03:48:56;
  ends 1 2016/09/26 04:48:56;
  cltt 1 2016/09/26 03:48:56;
--More--(76%)
```

Connected (unencrypted) to: Xen-rtr_new_base77

```
  binding state active;
  next binding state free;
  hardware ethernet 62:65:31:38:63:38;
}
lease 10.10.111.173 {
  starts 1 2016/09/26 03:48:56;
  ends 1 2016/09/26 04:48:56;
  cltt 1 2016/09/26 03:48:56;
  binding state active;
  next binding state free;
  hardware ethernet 35:39:63:34:62:35;
}
lease 10.10.111.178 {
  starts 1 2016/09/26 03:48:56;
  ends 1 2016/09/26 04:48:56;
  cltt 1 2016/09/26 03:48:56;
  binding state active;
  next binding state free;
  hardware ethernet 38:36:30:35:38:33;
}
lease 10.10.111.180 {
  starts 1 2016/09/26 03:48:56;
  ends 1 2016/09/26 04:48:56;
  cltt 1 2016/09/26 03:48:56;
--More--(79%)
```

Connected (unencrypted) to: Xen-rtr_new_base77

```
  binding state active;
  next binding state free;
  hardware ethernet 34:63:33:38:30:31;
}
lease 10.10.111.184 {
  starts 1 2016/09/26 03:48:57;
  ends 1 2016/09/26 04:48:57;
  cltt 1 2016/09/26 03:48:57;
  binding state active;
  next binding state free;
  hardware ethernet 34:38:65:32:62:64;
}
lease 10.10.111.190 {
  starts 1 2016/09/26 03:48:57;
  ends 1 2016/09/26 04:48:57;
  cltt 1 2016/09/26 03:48:57;
  binding state active;
  next binding state free;
  hardware ethernet 34:32:38:63:37:38;
}
lease 10.10.111.191 {
  starts 1 2016/09/26 03:48:57;
  ends 1 2016/09/26 04:48:57;
  cltt 1 2016/09/26 03:48:57;
--More--(82%)
```

Connected (unencrypted) to: Xen-rtr_new_base77

```
  binding state active;
  next binding state free;
  hardware ethernet 36:39:36:36:35:33;
}
lease 10.10.111.199 {
  starts 1 2016/09/26 03:48:58;
  ends 1 2016/09/26 04:48:58;
  cltt 1 2016/09/26 03:48:58;
  binding state active;
  next binding state free;
  hardware ethernet 32:63:62:63:37:34;
}
lease 10.10.111.100 {
  starts 1 2016/09/26 03:48:58;
  ends 1 2016/09/26 04:48:58;
  cltt 1 2016/09/26 03:48:58;
  binding state active;
  next binding state free;
  hardware ethernet 33:35:39:66:63:61;
}
lease 10.10.111.129 {
  starts 1 2016/09/26 03:49:00;
  ends 1 2016/09/26 04:49:00;
  cltt 1 2016/09/26 03:49:00;
--More--(85%)
```

Connected (unencrypted) to: Xen-rtr_new_base77

```
  binding state active;
  next binding state free;
  hardware ethernet 63:65:61:33:66:37;
}
lease 10.10.111.137 {
  starts 1 2016/09/26 03:49:00;
  ends 1 2016/09/26 04:49:00;
  cltt 1 2016/09/26 03:49:00;
  binding state active;
  next binding state free;
  hardware ethernet 66:32:63:63:35:61;
}
lease 10.10.111.155 {
  starts 1 2016/09/26 03:49:02;
  ends 1 2016/09/26 04:49:02;
  cltt 1 2016/09/26 03:49:02;
  binding state active;
  next binding state free;
  hardware ethernet 37:37:61:31:30:36;
}
lease 10.10.111.169 {
  starts 1 2016/09/26 03:49:02;
  ends 1 2016/09/26 04:49:02;
  cltt 1 2016/09/26 03:49:02;
--More--(88%)
```

Connected (unencrypted) to: Xen-rtr_new_base77

```
  binding state active;
  next binding state free;
  hardware ethernet 64:32:63:30:36:32;
}
lease 10.10.111.175 {
  starts 1 2016/09/26 03:49:03;
  ends 1 2016/09/26 04:49:03;
  cltt 1 2016/09/26 03:49:03;
  binding state active;
  next binding state free;
  hardware ethernet 62:30:62:64:38:66;
}
lease 10.10.111.154 {
  starts 1 2016/09/26 03:49:13;
  ends 1 2016/09/26 04:49:13;
  cltt 1 2016/09/26 03:49:13;
  binding state active;
  next binding state free;
  hardware ethernet 32:30:30:62:31:37;
}
lease 10.10.111.160 {
  starts 1 2016/09/26 03:49:13;
  ends 1 2016/09/26 04:49:13;
  cltt 1 2016/09/26 03:49:13;
--More--(91%)
```

Connected (unencrypted) to: Xen-rtr_new_base77

```
  binding state active;
  next binding state free;
  hardware ethernet 62:35:30:32:39:38;
}
lease 10.10.111.192 {
  starts 1 2016/09/26 03:49:15;
  ends 1 2016/09/26 04:49:15;
  cltt 1 2016/09/26 03:49:15;
  binding state active;
  next binding state free;
  hardware ethernet 38:35:64:30:32:33;
}
lease 10.10.111.200 {
  starts 1 2016/09/26 03:49:16;
  ends 1 2016/09/26 04:49:16;
  cltt 1 2016/09/26 03:49:16;
  binding state active;
  next binding state free;
  hardware ethernet 62:30:37:65:31:37;
}
lease 10.10.111.156 {
  starts 1 2016/09/26 03:49:20;
  ends 1 2016/09/26 04:49:20;
  cltt 1 2016/09/26 03:49:20;
--More--(94%)
```

Connected (unencrypted) to: Xen-rtr_new_base77

```
  binding state active;
  next binding state free;
  hardware ethernet 61:35:66:36:35:36;
}
lease 10.10.111.177 {
  starts 1 2016/09/26 03:49:21;
  ends 1 2016/09/26 04:49:21;
  cltt 1 2016/09/26 03:49:21;
  binding state active;
  next binding state free;
  hardware ethernet 62:31:36:61:32:61;
}
lease 10.10.111.188 {
  starts 1 2016/09/26 03:49:22;
  ends 1 2016/09/26 04:49:22;
  cltt 1 2016/09/26 03:49:22;
  binding state active;
  next binding state free;
  hardware ethernet 39:66:36:65:34:36;
}
lease 10.10.111.134 {
  starts 1 2016/09/26 03:49:32;
  ends 1 2016/09/26 04:49:32;
  cltt 1 2016/09/26 03:49:32;
--More--(97%)
```

Connected (unencrypted) to: Xen-rtr_new_base77

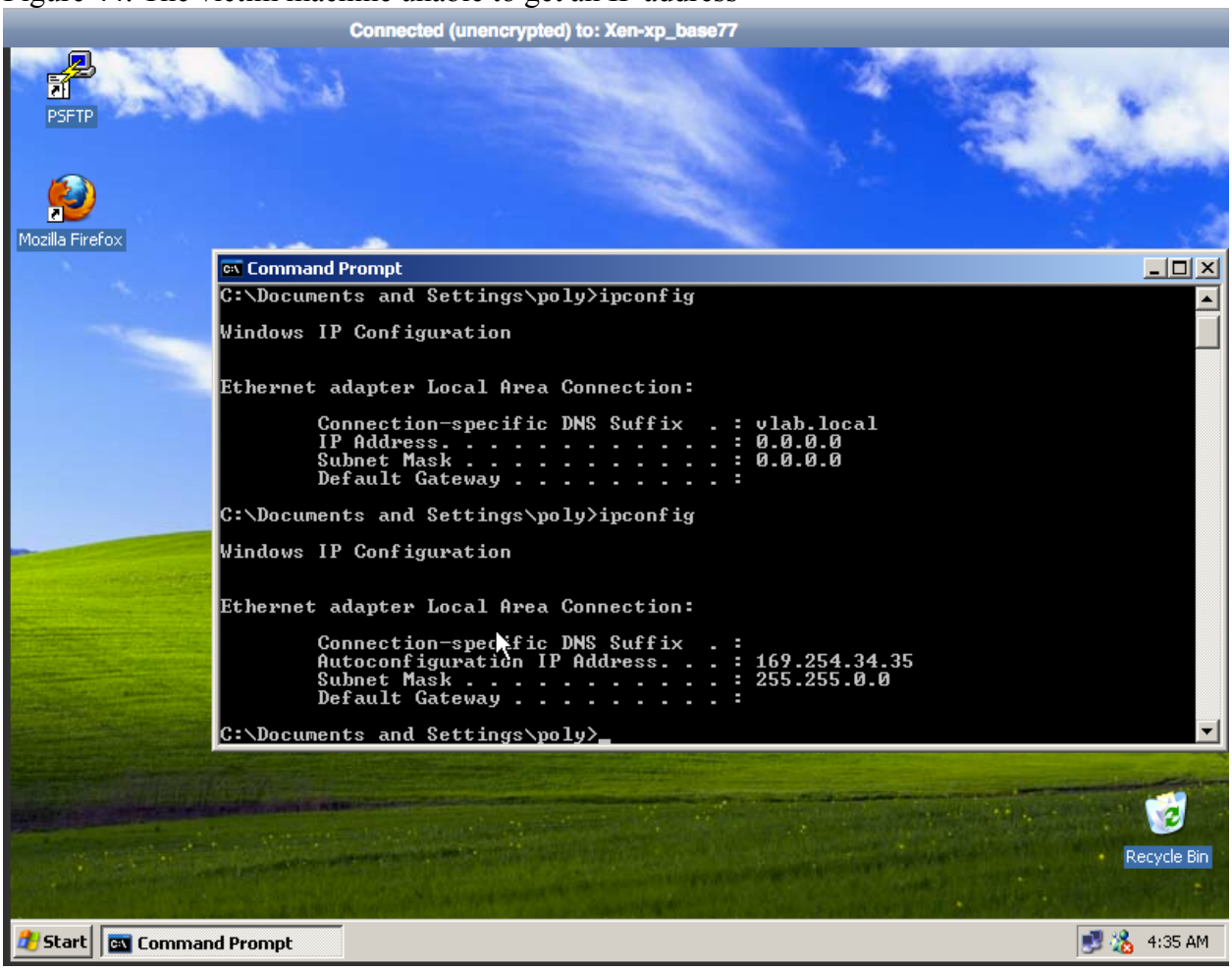
```
lease 10.10.111.134 {
  starts 1 2016/09/26 03:49:32;
  ends 1 2016/09/26 04:49:32;
  cltt 1 2016/09/26 03:49:32;
  binding state active;
  next binding state free;
  hardware ethernet 61:37:37:36:36:38;
}
lease 10.10.111.157 {
  starts 1 2016/09/26 03:49:34;
  ends 1 2016/09/26 04:49:34;
  cltt 1 2016/09/26 03:49:34;
  binding state active;
  next binding state free;
  hardware ethernet 64:35:65:66:31:65;
}
lease 10.10.111.167 {
  starts 1 2016/09/26 03:49:35;
  ends 1 2016/09/26 04:49:35;
  cltt 1 2016/09/26 03:49:35;
  binding state active;
  next binding state free;
  hardware ethernet 32:31:34:39:34:31;
}
router:/var/lib/dhcp3# _
```

Figure 37 - 43: WireShark (I sorted the WireShark dump by DestinationIP to get them in order)

No.	Time	Source	Destination	Protocol	Info
1291	1490.564347	02:00:4d:5e:0d:02	02:00:4d:42:0b:01	ARP	10.10.111.1 is at 02:00:4d:5e:0d:02
1294	1493.076200	02:00:4d:5e:0d:02	02:00:4d:42:0b:01	ARP	Who has 10.10.111.107? Tell 10.10.111.1
1295	1493.076242	02:00:4d:42:0b:01	02:00:4d:5e:0d:02	ARP	10.10.111.107 is at 02:00:4d:42:0b:01
1292	1490.564371	10.10.111.107	10.10.111.1	DHCP	DHCP Request - Transaction ID 0x8b0ec268
452	20.337012	10.10.111.1	10.10.111.100	DHCP	DHCP ACK - Transaction ID 0x0
3	0.095316	10.10.111.1	10.10.111.101	DHCP	DHCP ACK - Transaction ID 0x0
5	0.164773	10.10.111.1	10.10.111.102	DHCP	DHCP ACK - Transaction ID 0x0
157	6.948813	10.10.111.1	10.10.111.103	DHCP	DHCP ACK - Transaction ID 0x0
299	13.803803	10.10.111.1	10.10.111.104	DHCP	DHCP ACK - Transaction ID 0x0
9	0.348335	10.10.111.1	10.10.111.105	DHCP	DHCP ACK - Transaction ID 0x0
11	0.404920	10.10.111.1	10.10.111.106	DHCP	DHCP ACK - Transaction ID 0x0
1293	1490.578477	10.10.111.1	10.10.111.107	DHCP	DHCP ACK - Transaction ID 0x8b0ec268
13	0.468607	10.10.111.1	10.10.111.108	DHCP	DHCP ACK - Transaction ID 0x0
15	0.535956	10.10.111.1	10.10.111.109	DHCP	DHCP ACK - Transaction ID 0x0
17	0.587613	10.10.111.1	10.10.111.110	DHCP	DHCP ACK - Transaction ID 0x0
308	14.235975	10.10.111.1	10.10.111.111	DHCP	DHCP ACK - Transaction ID 0x0
20	0.667407	10.10.111.1	10.10.111.112	DHCP	DHCP ACK - Transaction ID 0x0
22	0.722444	10.10.111.1	10.10.111.113	DHCP	DHCP ACK - Transaction ID 0x0
314	14.479326	10.10.111.1	10.10.111.114	DHCP	DHCP ACK - Transaction ID 0x0
25	0.861588	10.10.111.1	10.10.111.115	DHCP	DHCP ACK - Transaction ID 0x0
27	0.924552	10.10.111.1	10.10.111.116	DHCP	DHCP ACK - Transaction ID 0x0
176	7.770951	10.10.111.1	10.10.111.117	DHCP	DHCP ACK - Transaction ID 0x0
30	1.034989	10.10.111.1	10.10.111.118	DHCP	DHCP ACK - Transaction ID 0x0
323	14.711787	10.10.111.1	10.10.111.119	DHCP	DHCP ACK - Transaction ID 0x0
325	14.763446	10.10.111.1	10.10.111.120	DHCP	DHCP ACK - Transaction ID 0x0
34	1.237799	10.10.111.1	10.10.111.121	DHCP	DHCP ACK - Transaction ID 0x0
36	1.332794	10.10.111.1	10.10.111.122	DHCP	DHCP ACK - Transaction ID 0x0
330	14.929050	10.10.111.1	10.10.111.123	DHCP	DHCP ACK - Transaction ID 0x0
39	1.510684	10.10.111.1	10.10.111.124	DHCP	DHCP ACK - Transaction ID 0x0
333	15.074425	10.10.111.1	10.10.111.125	DHCP	DHCP ACK - Transaction ID 0x0
189	8.521956	10.10.111.1	10.10.111.126	DHCP	DHCP ACK - Transaction ID 0x0
43	1.687825	10.10.111.1	10.10.111.127	DHCP	DHCP ACK - Transaction ID 0x0
45	1.753194	10.10.111.1	10.10.111.128	DHCP	DHCP ACK - Transaction ID 0x0
495	22.215836	10.10.111.1	10.10.111.129	DHCP	DHCP ACK - Transaction ID 0x0
48	1.948475	10.10.111.1	10.10.111.130	DHCP	DHCP ACK - Transaction ID 0x0
50	2.055031	10.10.111.1	10.10.111.131	DHCP	DHCP ACK - Transaction ID 0x0
197	8.878281	10.10.111.1	10.10.111.132	DHCP	DHCP ACK - Transaction ID 0x0
53	2.202855	10.10.111.1	10.10.111.133	DHCP	DHCP ACK - Transaction ID 0x0
1103	55.059848	10.10.111.1	10.10.111.134	DHCP	DHCP ACK - Transaction ID 0x0
348	15.838799	10.10.111.1	10.10.111.135	DHCP	DHCP ACK - Transaction ID 0x0
57	2.357528	10.10.111.1	10.10.111.136	DHCP	DHCP ACK - Transaction ID 0x0
506	22.812530	10.10.111.1	10.10.111.137	DHCP	DHCP ACK - Transaction ID 0x0
60	2.503609	10.10.111.1	10.10.111.138	DHCP	DHCP ACK - Transaction ID 0x0
62	2.574303	10.10.111.1	10.10.111.139	DHCP	DHCP ACK - Transaction ID 0x0
355	16.197932	10.10.111.1	10.10.111.140	DHCP	DHCP ACK - Transaction ID 0x0
65	2.716800	10.10.111.1	10.10.111.141	DHCP	DHCP ACK - Transaction ID 0x0
212	9.568120	10.10.111.1	10.10.111.142	DHCP	DHCP ACK - Transaction ID 0x0
68	2.832604	10.10.111.1	10.10.111.143	DHCP	DHCP ACK - Transaction ID 0x0
215	9.668747	10.10.111.1	10.10.111.144	DHCP	DHCP ACK - Transaction ID 0x0
71	3.028013	10.10.111.1	10.10.111.145	DHCP	DHCP ACK - Transaction ID 0x0
73	3.118553	10.10.111.1	10.10.111.146	DHCP	DHCP ACK - Transaction ID 0x0
221	9.931170	10.10.111.1	10.10.111.147	DHCP	DHCP ACK - Transaction ID 0x0
76	3.289027	10.10.111.1	10.10.111.148	DHCP	DHCP ACK - Transaction ID 0x0
225	10.040586	10.10.111.1	10.10.111.149	DHCP	DHCP ACK - Transaction ID 0x0
79	3.387932	10.10.111.1	10.10.111.150	DHCP	DHCP ACK - Transaction ID 0x0
229	10.136301	10.10.111.1	10.10.111.151	DHCP	DHCP ACK - Transaction ID 0x0
374	17.104811	10.10.111.1	10.10.111.152	DHCP	DHCP ACK - Transaction ID 0x0
83	3.551389	10.10.111.1	10.10.111.153	DHCP	DHCP ACK - Transaction ID 0x0
678	35.406106	10.10.111.1	10.10.111.154	DHCP	DHCP ACK - Transaction ID 0x0
530	24.125181	10.10.111.1	10.10.111.155	DHCP	DHCP ACK - Transaction ID 0x0
830	42.458035	10.10.111.1	10.10.111.156	DHCP	DHCP ACK - Transaction ID 0x0
1139	56.613565	10.10.111.1	10.10.111.157	DHCP	DHCP ACK - Transaction ID 0x0
89	3.828574	10.10.111.1	10.10.111.158	DHCP	DHCP ACK - Transaction ID 0x0
91	3.891153	10.10.111.1	10.10.111.159	DHCP	DHCP ACK - Transaction ID 0x0

685	35.778932	10.10.111.1	10.10.111.160	DHCP	DHCP ACK	- Transaction ID 0x0
240	10.809473	10.10.111.1	10.10.111.161	DHCP	DHCP ACK	- Transaction ID 0x0
95	4.149589	10.10.111.1	10.10.111.162	DHCP	DHCP ACK	- Transaction ID 0x0
244	10.951350	10.10.111.1	10.10.111.163	DHCP	DHCP ACK	- Transaction ID 0x0
246	11.032855	10.10.111.1	10.10.111.164	DHCP	DHCP ACK	- Transaction ID 0x0
99	4.423808	10.10.111.1	10.10.111.165	DHCP	DHCP ACK	- Transaction ID 0x0
101	4.482676	10.10.111.1	10.10.111.166	DHCP	DHCP ACK	- Transaction ID 0x0
1154	57.329323	10.10.111.1	10.10.111.167	DHCP	DHCP ACK	- Transaction ID 0x0
104	4.601956	10.10.111.1	10.10.111.168	DHCP	DHCP ACK	- Transaction ID 0x0
550	24.955283	10.10.111.1	10.10.111.169	DHCP	DHCP ACK	- Transaction ID 0x0
107	4.730080	10.10.111.1	10.10.111.170	DHCP	DHCP ACK	- Transaction ID 0x0
109	4.808259	10.10.111.1	10.10.111.171	DHCP	DHCP ACK	- Transaction ID 0x0
402	18.515336	10.10.111.1	10.10.111.172	DHCP	DHCP ACK	- Transaction ID 0x0
404	18.577942	10.10.111.1	10.10.111.173	DHCP	DHCP ACK	- Transaction ID 0x0
113	5.000587	10.10.111.1	10.10.111.174	DHCP	DHCP ACK	- Transaction ID 0x0
558	25.486420	10.10.111.1	10.10.111.175	DHCP	DHCP ACK	- Transaction ID 0x0
261	11.876250	10.10.111.1	10.10.111.176	DHCP	DHCP ACK	- Transaction ID 0x0
862	44.021796	10.10.111.1	10.10.111.177	DHCP	DHCP ACK	- Transaction ID 0x0
412	18.840513	10.10.111.1	10.10.111.178	DHCP	DHCP ACK	- Transaction ID 0x0
119	5.294464	10.10.111.1	10.10.111.179	DHCP	DHCP ACK	- Transaction ID 0x0
416	19.001366	10.10.111.1	10.10.111.180	DHCP	DHCP ACK	- Transaction ID 0x0
267	12.325376	10.10.111.1	10.10.111.181	DHCP	DHCP ACK	- Transaction ID 0x0
123	5.455639	10.10.111.1	10.10.111.182	DHCP	DHCP ACK	- Transaction ID 0x0
125	5.526147	10.10.111.1	10.10.111.183	DHCP	DHCP ACK	- Transaction ID 0x0
424	19.268556	10.10.111.1	10.10.111.184	DHCP	DHCP ACK	- Transaction ID 0x0
128	5.649051	10.10.111.1	10.10.111.185	DHCP	DHCP ACK	- Transaction ID 0x0
130	5.712797	10.10.111.1	10.10.111.186	DHCP	DHCP ACK	- Transaction ID 0x0
276	12.683295	10.10.111.1	10.10.111.187	DHCP	DHCP ACK	- Transaction ID 0x0
877	44.725480	10.10.111.1	10.10.111.188	DHCP	DHCP ACK	- Transaction ID 0x0
134	5.936523	10.10.111.1	10.10.111.189	DHCP	DHCP ACK	- Transaction ID 0x0
432	19.625644	10.10.111.1	10.10.111.190	DHCP	DHCP ACK	- Transaction ID 0x0
434	19.674950	10.10.111.1	10.10.111.191	DHCP	DHCP ACK	- Transaction ID 0x0
731	38.023339	10.10.111.1	10.10.111.192	DHCP	DHCP ACK	- Transaction ID 0x0
139	6.263611	10.10.111.1	10.10.111.193	DHCP	DHCP ACK	- Transaction ID 0x0
141	6.318098	10.10.111.1	10.10.111.194	DHCP	DHCP ACK	- Transaction ID 0x0
143	6.386360	10.10.111.1	10.10.111.195	DHCP	DHCP ACK	- Transaction ID 0x0
287	13.254558	10.10.111.1	10.10.111.196	DHCP	DHCP ACK	- Transaction ID 0x0
146	6.514956	10.10.111.1	10.10.111.197	DHCP	DHCP ACK	- Transaction ID 0x0
148	6.553810	10.10.111.1	10.10.111.198	DHCP	DHCP ACK	- Transaction ID 0x0
449	20.216275	10.10.111.1	10.10.111.199	DHCP	DHCP ACK	- Transaction ID 0x0
745	38.557615	10.10.111.1	10.10.111.200	DHCP	DHCP ACK	- Transaction ID 0x0

Figure 44: The victim machine unable to get an IP address



Mitigation:

There are a few ways to protect your DHCP sever from an attack like this. The first way would to be to limit the number of MAC addresses allow on a certain port. On a Cisco switch this is done with the *switchport port-security maximum* command. Another way is to turn DHCP snooping on for the vlan's that you want protected. This is done with the *ip dhcp snooping* command then specifying the vlan's you want to protect (ex. *ip dhcp snooping vlan1)* and connecting it to a database to use (ex. *ip dhcp snooping database* (listing a database to use via tftp)) and lastly making sure it verifies the MAC address that's requesting the dhcp lease (ex. *ip dhcp snooping verify mac-address)*.

References

Class lecture slides via https://newclasses.nyu.edu/portal/site/a60fc113-1000-46e8-8494-fe34c757d950/page/9341f776-4200-4715-b9ac-0923689381d7

http://www.revolutionwifi.net/revolutionwifi/2011/03/preventing-dhcp-starvation-attacks.html