Sumedh Karande
N13311003

Assignment No.4 – DHCP Starvation using Scapy.

DHCP Starvation Attack:

Illustration:

1) Clear dhcpd.leases and dhcpd.leases~ to release any leases that were previously allotted.
2) Increase the Router's lease time to 24 hrs.
3) Now send a DHCP Discover message with Random MAC address to the router to starve addresses from the range of 10.10.111.100 – 10.10.111.200
4) Wait for an ACK message from the Router, if received add the IP address to the pool of starved addresses.
5) If ACK is not received, then send a request again requesting for the same IP address.
6) After all the ACKs are received the targeted router is out of IP addresses for lease. Thus DHCP Starvation is successful.

Leases before attack.

```
Connected (unencrypted) to: Xen-rtr_new_base82
  GNU nano 2.0.7              File: 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

lease 10.10.111.100 {
  starts 4 2010/03/11 00:29:55;
  ends 4 2010/03/11 01:29:55;
  tstp 4 2010/03/11 01:29:55;
  cltt 4 2010/03/11 00:29:55;
  binding state free;
  hardware ethernet 00:16:3e:03:00:0b;
}
lease 10.10.111.102 {
  starts 4 2010/03/11 17:48:47;
  ends 4 2010/03/11 18:12:52;
  tstp 4 2010/03/11 18:12:52;
  cltt 4 2010/03/11 17:48:47;
  binding state free;
  hardware ethernet 02:36:0e:01:13:93;
  uid "\001\0026\016\001\023\223";
}

^G Get Help  ^O WriteOut  ^R Read File ^Y Prev Page ^K Cut Text  ^C Cur Pos
^X Exit      ^J Justify   ^W Where Is  ^V Next Page ^U UnCut Text^T To Spell
```

```
Connected (unencrypted) to: Xen-rtr_new_base82
  GNU nano 2.0.7              File: dhcpd.leases

lease 10.10.111.101 {
  starts 4 2010/03/11 18:12:52;
  ends 4 2010/03/11 19:12:52;
  tstp 4 2010/03/11 19:12:52;
  cltt 4 2010/03/11 18:12:52;
  binding state free;
  hardware ethernet 02:36:0e:01:13:93;
  uid "\001\0026\016\001\023\223";
}
lease 10.10.111.103 {
  starts 2 2011/02/01 04:02:44;
  ends 2 2011/02/01 05:02:44;
  tstp 2 2011/02/01 05:02:44;
  cltt 2 2011/02/01 04:02:44;
  binding state free;
  hardware ethernet 02:36:1e:b2:75:94;
}
lease 10.10.111.105 {
  starts 0 2012/03/25 20:19:52;
  ends 0 2012/03/25 21:19:52;

^G Get Help  ^O WriteOut  ^R Read File ^Y Prev Page ^K Cut Text  ^C Cur Pos
^X Exit      ^J Justify   ^W Where Is  ^V Next Page ^U UnCut Text^T To Spell
```

```
Connected (unencrypted) to: Xen-rtr_new_base82
  GNU nano 2.0.7              File: 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

lease 10.10.111.100 {
  starts 4 2010/03/11 00:29:55;
  ends 4 2010/03/11 01:29:55;
  tstp 4 2010/03/11 01:29:55;
  cltt 4 2010/03/11 00:29:55;
  binding state free;
  hardware ethernet 00:16:3e:03:00:0b;
}
lease 10.10.111.102 {
  starts 4 2010/03/11 17:48:47;
  ends 4 2010/03/11 18:12:52;
  tstp 4 2010/03/11 18:12:52;
  cltt 4 2010/03/11 17:48:47;
  binding state free;
  hardware ethernet 02:36:0e:01:13:93;
  uid "\001\0026\016\001\023\223";
}
                              [ Read 148 lines ]
^G Get Help  ^O WriteOut  ^R Read File ^Y Prev Page ^K Cut Text  ^C Cur Pos
^X Exit      ^J Justify   ^W Where Is  ^V Next Page ^U UnCut Text^T To Spell
```

```
Connected (unencrypted) to: Xen-rtr_new_base82
  GNU nano 2.0.7              File: dhcpd.leases~

lease 10.10.111.101 {
  starts 4 2010/03/11 18:12:52;
  ends 4 2010/03/11 19:12:52;
  tstp 4 2010/03/11 19:12:52;
  cltt 4 2010/03/11 18:12:52;
  binding state free;
  hardware ethernet 02:36:0e:01:13:93;
  uid "\001\0026\016\001\023\223";
}
lease 10.10.111.103 {
  starts 2 2011/02/01 04:02:44;
  ends 2 2011/02/01 05:02:44;
  tstp 2 2011/02/01 05:02:44;
  cltt 2 2011/02/01 04:02:44;
  binding state free;
  hardware ethernet 02:36:1e:b2:75:94;
}
lease 10.10.111.105 {
  starts 0 2012/03/25 20:19:52;
  ends 0 2012/03/25 21:19:52;

^G Get Help  ^O WriteOut  ^R Read File ^Y Prev Page ^K Cut Text  ^C Cur Pos
^X Exit      ^J Justify   ^W Where Is  ^V Next Page ^U UnCut Text^T To Spell
```

Sumedh Karande
N13311003

Leases after attack

```
Connected (unencrypted) to: Xen-rtr_new_base82
  GNU nano 2.0.7              File: 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

lease 10.10.111.104 {
  starts 4 2016/10/06 18:31:24;
  ends 4 2016/10/06 20:31:24;
  cltt 4 2016/10/06 18:31:24;
  binding state active;
  next binding state free;
  hardware ethernet 38:63:30:66:65:61;
}
lease 10.10.111.106 {
  starts 4 2016/10/06 18:31:26;
  ends 4 2016/10/06 20:31:26;
  cltt 4 2016/10/06 18:31:26;
  binding state active;
  next binding state free;
  hardware ethernet 63:63:30:35:63:33;
}
lease 10.10.111.111 {
                              [ Read 821 lines ]
^G Get Help  ^O WriteOut  ^R Read File ^Y Prev Page ^K Cut Text  ^C Cur Pos
^X Exit      ^J Justify   ^W Where Is  ^V Next Page ^U UnCut Text^T To Spell
```

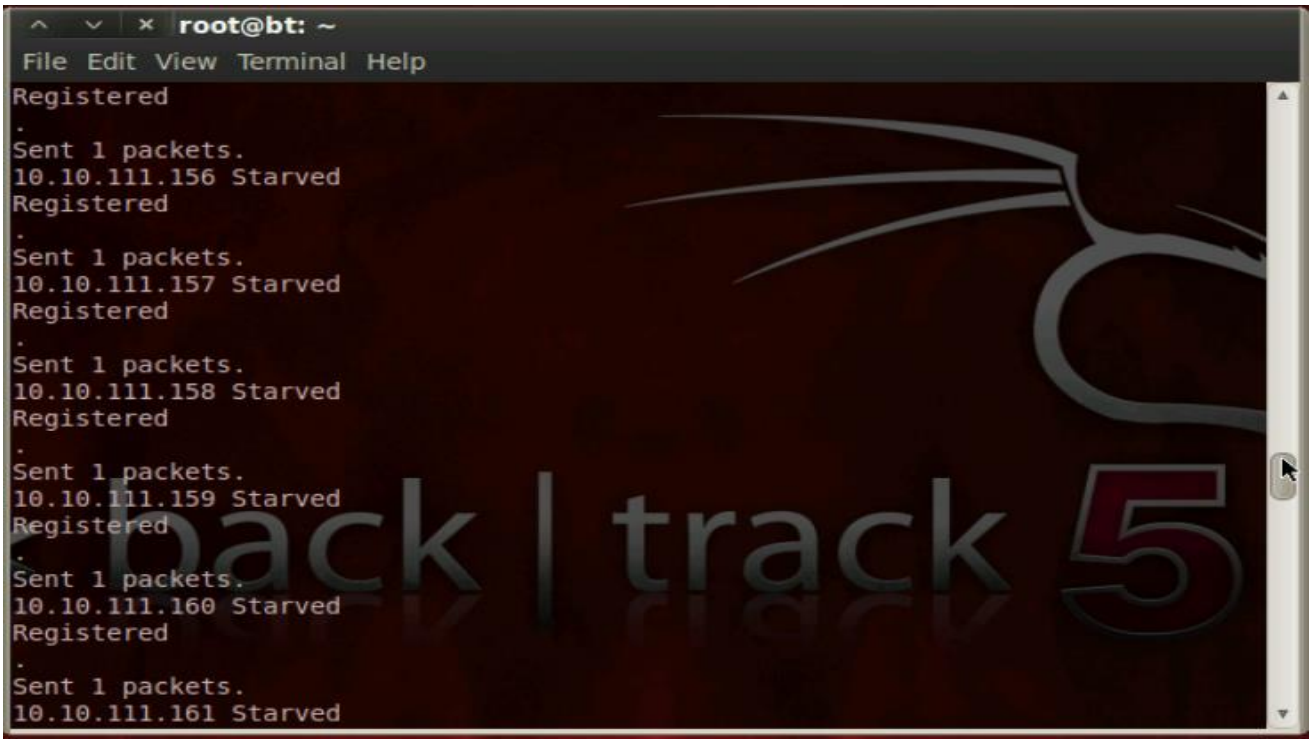
```
Connected (unencrypted) to: Xen-rtr_new_base82
  GNU nano 2.0.7              File: dhcpd.leases

}
lease 10.10.111.130 {
  starts 4 2016/10/06 18:31:51;
  ends 4 2016/10/06 20:31:51;
  cltt 4 2016/10/06 18:31:51;
  binding state active;
  next binding state free;
  hardware ethernet 64:35:30:61:38:35;
}
lease 10.10.111.133 {
  starts 4 2016/10/06 18:31:55;
  ends 4 2016/10/06 20:31:55;
  cltt 4 2016/10/06 18:31:55;
  binding state active;
  next binding state free;
  hardware ethernet 38:30:63:38:39:64;
}
lease 10.10.111.135 {
  starts 4 2016/10/06 18:31:57;
  ends 4 2016/10/06 20:31:57;

^G Get Help  ^O WriteOut  ^R Read File ^Y Prev Page ^K Cut Text  ^C Cur Pos
^X Exit      ^J Justify   ^W Where Is  ^V Next Page ^U UnCut Text^T To Spell
```

```
Connected (unencrypted) to: Xen-rtr_new_base82
  GNU nano 2.0.7              File: dhcpd.leases

}
lease 10.10.111.168 {
  starts 4 2016/10/06 18:32:32;
  ends 4 2016/10/06 20:32:32;
  cltt 4 2016/10/06 18:32:32;
  binding state active;
  next binding state free;
  hardware ethernet 39:32:61:39:30:38;
}
lease 10.10.111.169 {
_ starts 4 2016/10/06 18:32:33;
  ends 4 2016/10/06 20:32:33;
  cltt 4 2016/10/06 18:32:33;
  binding state active;
  next binding state free;
  hardware ethernet 38:39:30:63:32:64;
}
lease 10.10.111.170 {
  starts 4 2016/10/06 18:32:34;
  ends 4 2016/10/06 20:32:34;

^G Get Help  ^O WriteOut  ^R Read File ^Y Prev Page ^K Cut Text  ^C Cur Pos
^X Exit      ^J Justify   ^W Where Is  ^V Next Page ^U UnCut Text^T To Spell
```

```
Connected (unencrypted) to: Xen-rtr_new_base82
  GNU nano 2.0.7              File: dhcpd.leases

}
lease 10.10.111.184 {
  starts 4 2016/10/06 18:32:48;
  ends 4 2016/10/06 20:32:48;
  cltt 4 2016/10/06 18:32:48;
  binding state active;
  next binding state free;
  hardware ethernet 30:33:64:30:66:63;
}
lease 10.10.111.185 {
_ starts 4 2016/10/06 18:32:50;
  ends 4 2016/10/06 20:32:50;
  cltt 4 2016/10/06 18:32:50;
  binding state active;
  next binding state free;
  hardware ethernet 32:66:33:36:65:39;
}
lease 10.10.111.192 {
  starts 4 2016/10/06 18:32:57;
  ends 4 2016/10/06 20:32:57;

^G Get Help  ^O WriteOut  ^R Read File ^Y Prev Page ^K Cut Text  ^C Cur Pos
^X Exit      ^J Justify   ^W Where Is  ^V Next Page ^U UnCut Text^T To Spell
```

Sumedh Karande
N13311003

Bt5 Output

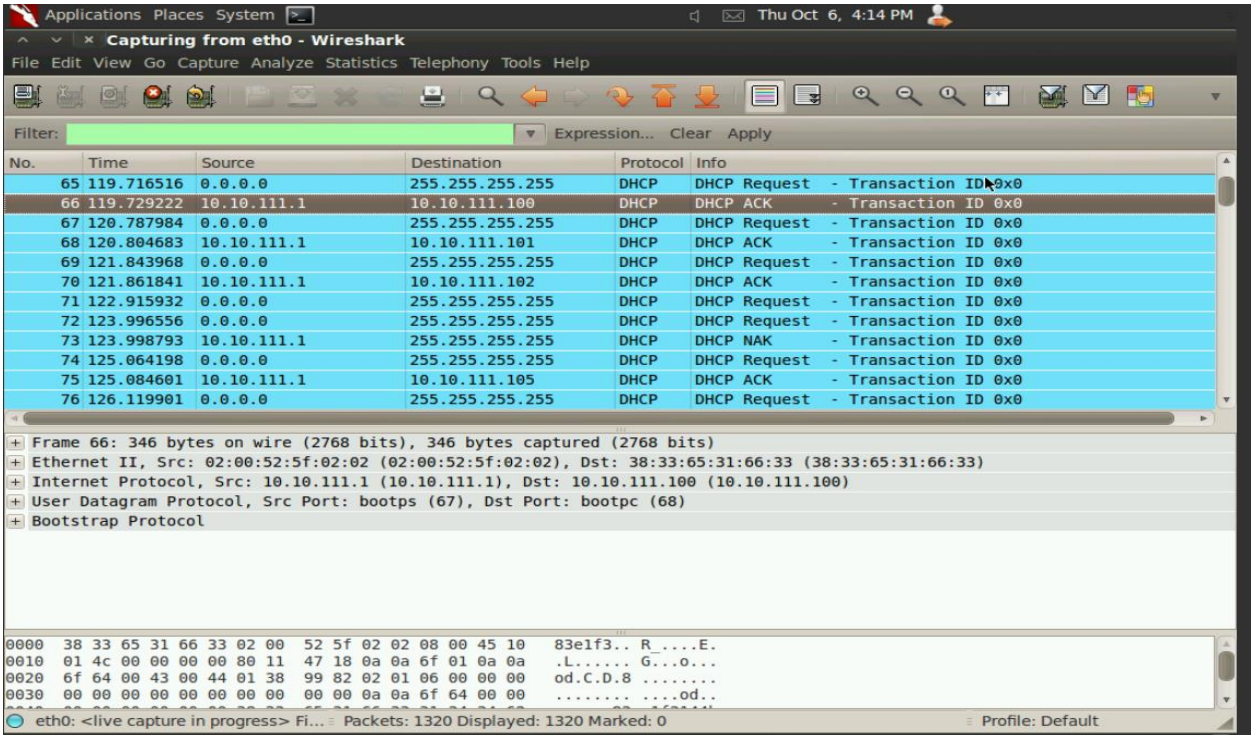


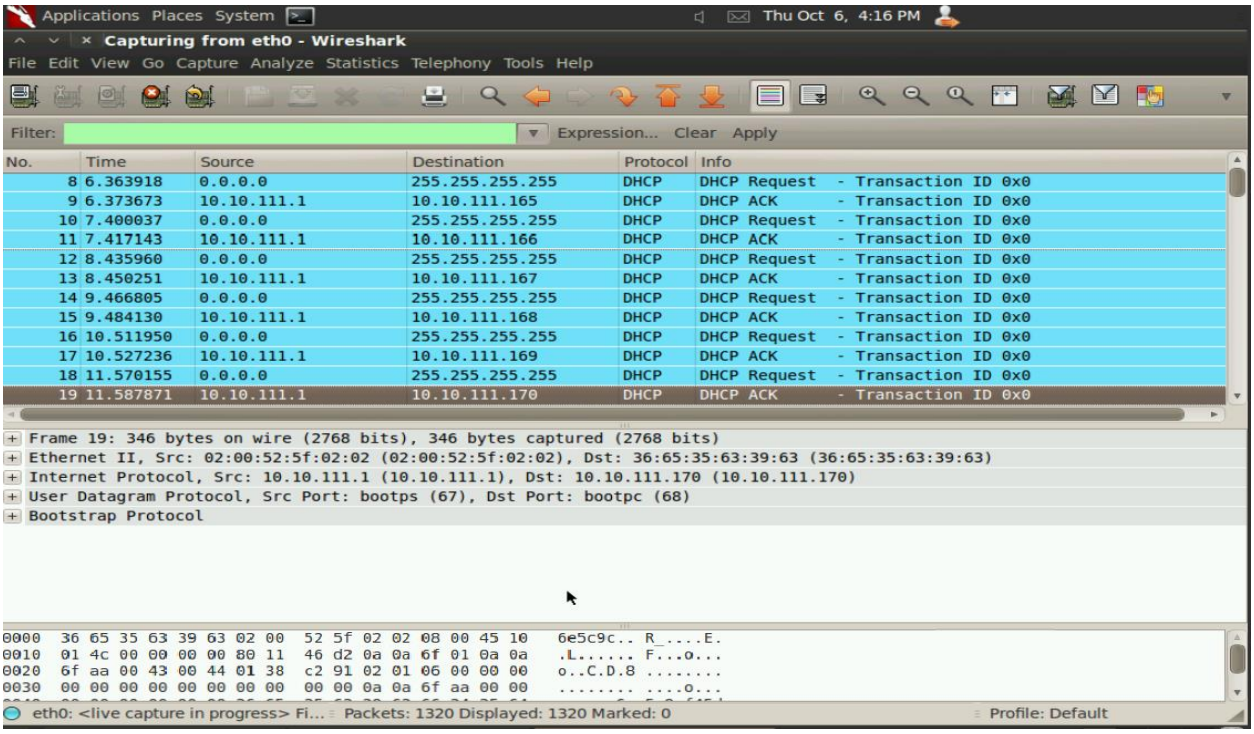
```
root@bt: ~
File  Edit  View  Terminal  Help
Sent 1 packets.
10.10.111.181 Starved
Registered
.
Sent 1 packets.
10.10.111.182 Starved
Registered
.
Sent 1 packets.
10.10.111.183 Starved
Registered
.
Sent 1 packets.
10.10.111.184 Starved
Registered
.
Sent 1 packets.
10.10.111.185 Starved
Registered
.
Sent 1 packets.
10.10.111.186 Starved
Registered
.
```

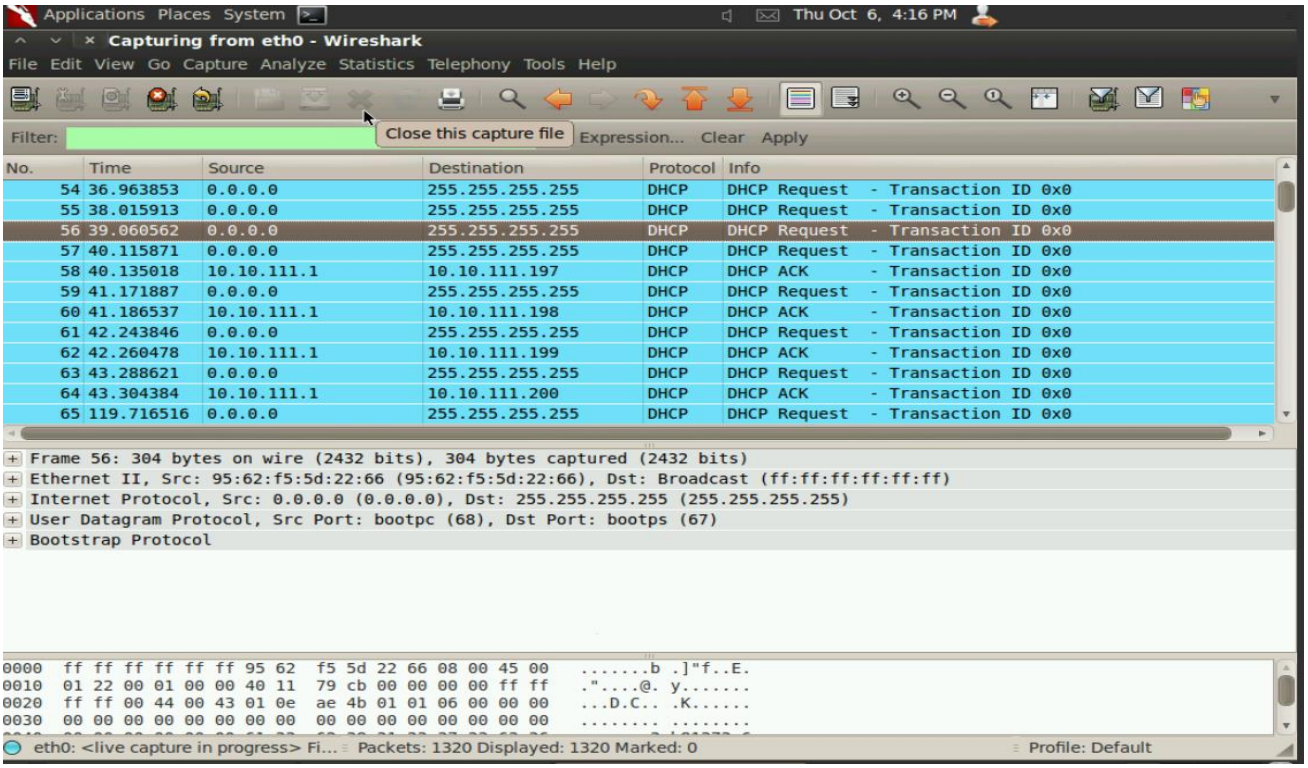
```
root@bt: ~
File  Edit  View  Terminal  Help
The starved IPs are:
['10.10.111.100', '10.10.111.101', '10.10.111.102', '10.10.111.103', '10.10.111.
104', '10.10.111.105', '10.10.111.106', '10.10.111.108', '10.10.111.109', '10.10
.111.110', '10.10.111.111', '10.10.111.112', '10.10.111.113', '10.10.111.114', '
10.10.111.115', '10.10.111.116', '10.10.111.117', '10.10.111.118', '10.10.111.11
9', '10.10.111.120', '10.10.111.121', '10.10.111.122', '10.10.111.123', '10.10.1
11.124', '10.10.111.125', '10.10.111.126', '10.10.111.127', '10.10.111.128', '10
.10.111.129', '10.10.111.130', '10.10.111.131', '10.10.111.132', '10.10.111.133'
, '10.10.111.134', '10.10.111.135', '10.10.111.136', '10.10.111.137', '10.10.111
.138', '10.10.111.139', '10.10.111.140', '10.10.111.141', '10.10.111.142', '10.1
0.111.143', '10.10.111.144', '10.10.111.145', '10.10.111.146', '10.10.111.147',
'10.10.111.148', '10.10.111.149', '10.10.111.150', '10.10.111.151', '10.10.111.1
52', '10.10.111.153', '10.10.111.154', '10.10.111.155', '10.10.111.156', '10.10.
111.157', '10.10.111.158', '10.10.111.159', '10.10.111.160', '10.10.111.161', '1
0.10.111.162', '10.10.111.163', '10.10.111.164', '10.10.111.165', '10.10.111.166
', '10.10.111.167', '10.10.111.168', '10.10.111.169', '10.10.111.170', '10.10.11
1.171', '10.10.111.172', '10.10.111.173', '10.10.111.174', '10.10.111.175', '10.
10.111.176', '10.10.111.177', '10.10.111.178', '10.10.111.179', '10.10.111.180',
 '10.10.111.181', '10.10.111.182', '10.10.111.183', '10.10.111.184', '10.10.111.
185', '10.10.111.186', '10.10.111.187', '10.10.111.188', '10.10.111.189', '10.10
.111.190', '10.10.111.191', '10.10.111.192', '10.10.111.193', '10.10.111.194', '
10.10.111.195', '10.10.111.196', '10.10.111.197', '10.10.111.198', '10.10.111.19
9', '10.10.111.200']
root@bt:~#
```

Sumedh Karande
N13311003

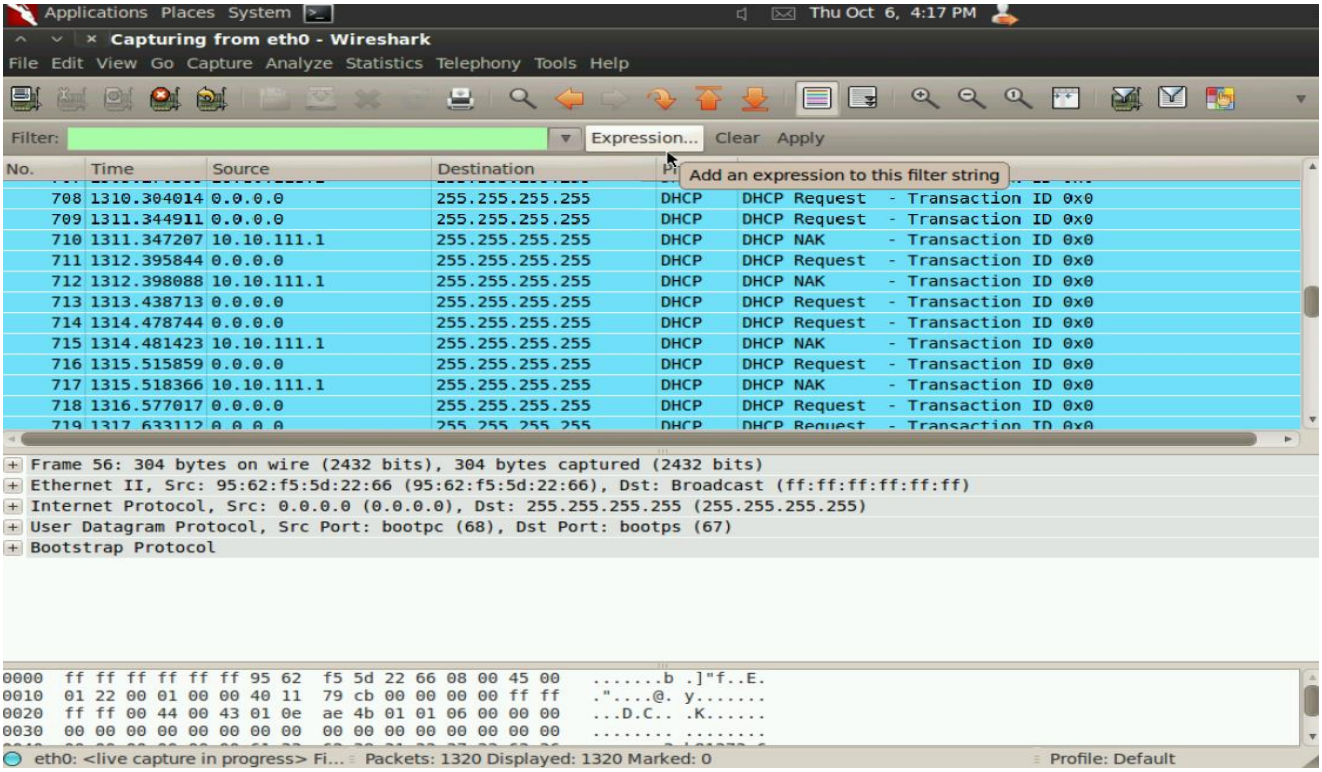
Wireshark Dump



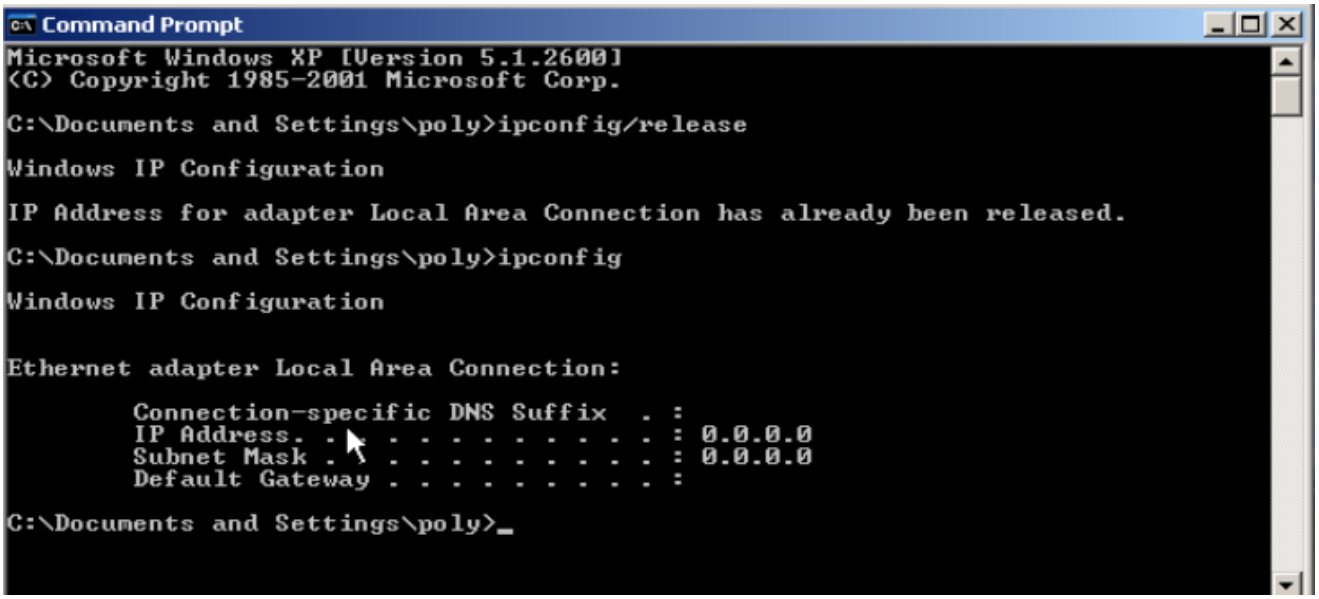



Applications Places System
Thu Oct 6, 4:16 PM
Capturing from eth0 - Wireshark
File Edit View Go Capture Analyze Statistics Telephony Tools Help
Filter:
Close this capture file
Expression... Clear Apply
No. Time Source Destination Protocol Info
54 36.963853 0.0.0.0 255.255.255.255 DHCP DHCP Request - Transaction ID 0x0
55 38.015913 0.0.0.0 255.255.255.255 DHCP DHCP Request - Transaction ID 0x0
56 39.060562 0.0.0.0 255.255.255.255 DHCP DHCP Request - Transaction ID 0x0
57 40.115871 0.0.0.0 255.255.255.255 DHCP DHCP Request - Transaction ID 0x0
58 40.135018 10.10.111.1 10.10.111.197 DHCP DHCP ACK - Transaction ID 0x0
59 41.171887 0.0.0.0 255.255.255.255 DHCP DHCP Request - Transaction ID 0x0
60 41.186537 10.10.111.1 10.10.111.198 DHCP DHCP ACK - Transaction ID 0x0
61 42.243846 0.0.0.0 255.255.255.255 DHCP DHCP Request - Transaction ID 0x0
62 42.260478 10.10.111.1 10.10.111.199 DHCP DHCP ACK - Transaction ID 0x0
63 43.288621 0.0.0.0 255.255.255.255 DHCP DHCP Request - Transaction ID 0x0
64 43.304384 10.10.111.1 10.10.111.200 DHCP DHCP ACK - Transaction ID 0x0
65 119.716516 0.0.0.0 255.255.255.255 DHCP DHCP Request - Transaction ID 0x0
Frame 56: 304 bytes on wire (2432 bits), 304 bytes captured (2432 bits)
Ethernet II, Src: 95:62:f5:5d:22:66 (95:62:f5:5d:22:66), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
Internet Protocol, Src: 0.0.0.0 (0.0.0.0), Dst: 255.255.255.255 (255.255.255.255)
User Datagram Protocol, Src Port: bootpc (68), Dst Port: bootps (67)
Bootstrap Protocol
0000 ff ff ff ff ff ff 95 62 f5 5d 22 66 08 00 45 00 .....b .]"f..E.
0010 01 22 00 01 00 00 40 11 79 cb 00 00 00 00 ff ff ."....@. y.....
0020 ff ff 00 44 00 43 01 0e ae 4b 01 01 06 00 00 00 ...D.C.. .K.....
0030 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
eth0: <live capture in progress> Fi... Packets: 1320 Displayed: 1320 Marked: 0
Profile: Default

NAK Message

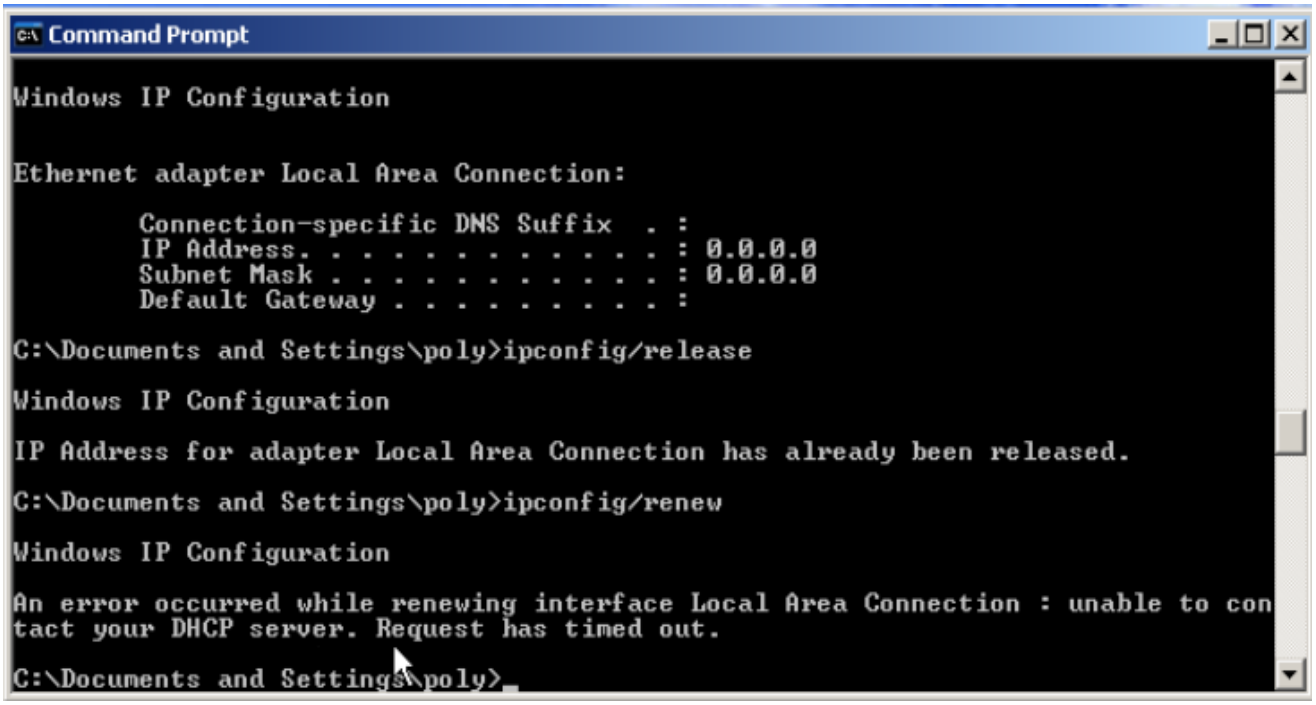

Applications Places System
Thu Oct 6, 4:17 PM
Capturing from eth0 - Wireshark
File Edit View Go Capture Analyze Statistics Telephony Tools Help
Filter:
Expression... Clear Apply
Add an expression to this filter string
No. Time Source Destination
708 1310.304014 0.0.0.0 255.255.255.255 DHCP DHCP Request - Transaction ID 0x0
709 1311.344911 0.0.0.0 255.255.255.255 DHCP DHCP Request - Transaction ID 0x0
710 1311.347207 10.10.111.1 255.255.255.255 DHCP DHCP NAK - Transaction ID 0x0
711 1312.395844 0.0.0.0 255.255.255.255 DHCP DHCP Request - Transaction ID 0x0
712 1312.398088 10.10.111.1 255.255.255.255 DHCP DHCP NAK - Transaction ID 0x0
713 1313.438713 0.0.0.0 255.255.255.255 DHCP DHCP Request - Transaction ID 0x0
714 1314.478744 0.0.0.0 255.255.255.255 DHCP DHCP Request - Transaction ID 0x0
715 1314.481423 10.10.111.1 255.255.255.255 DHCP DHCP NAK - Transaction ID 0x0
716 1315.515859 0.0.0.0 255.255.255.255 DHCP DHCP Request - Transaction ID 0x0
717 1315.518366 10.10.111.1 255.255.255.255 DHCP DHCP NAK - Transaction ID 0x0
718 1316.577017 0.0.0.0 255.255.255.255 DHCP DHCP Request - Transaction ID 0x0
Frame 56: 304 bytes on wire (2432 bits), 304 bytes captured (2432 bits)
Ethernet II, Src: 95:62:f5:5d:22:66 (95:62:f5:5d:22:66), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
Internet Protocol, Src: 0.0.0.0 (0.0.0.0), Dst: 255.255.255.255 (255.255.255.255)
User Datagram Protocol, Src Port: bootpc (68), Dst Port: bootps (67)
Bootstrap Protocol
0000 ff ff ff ff ff ff 95 62 f5 5d 22 66 08 00 45 00 .....b .]"f..E.
0010 01 22 00 01 00 00 40 11 79 cb 00 00 00 00 ff ff ."....@. y.....
0020 ff ff 00 44 00 43 01 0e ae 4b 01 01 06 00 00 00 ...D.C.. .K.....
0030 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
eth0: <live capture in progress> Fi... Packets: 1320 Displayed: 1320 Marked: 0
Profile: Default

Output for Cmd of XP



```
Command Prompt
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\poly>ipconfig/release

Windows IP Configuration

IP Address for adapter Local Area Connection has already been released.

C:\Documents and Settings\poly>ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection:

        Connection-specific DNS Suffix  . :
        IP Address. . . . . . . . . . . . : 0.0.0.0
        Subnet Mask . . . . . . . . . . . : 0.0.0.0
        Default Gateway . . . . . . . . . :

C:\Documents and Settings\poly>_
```

Request Timed-out.



```
Command Prompt

Windows IP Configuration


Ethernet adapter Local Area Connection:

        Connection-specific DNS Suffix  . :
        IP Address. . . . . . . . . . . . : 0.0.0.0
        Subnet Mask . . . . . . . . . . . : 0.0.0.0
        Default Gateway . . . . . . . . . :

C:\Documents and Settings\poly>ipconfig/release

Windows IP Configuration

IP Address for adapter Local Area Connection has already been released.

C:\Documents and Settings\poly>ipconfig/renew

Windows IP Configuration

An error occurred while renewing interface Local Area Connection : unable to con
tact your DHCP server. Request has timed out.

C:\Documents and Settings\poly>_
```