How to monitor DHCP traffic from the command line on Linux

Author : Dan Nanni

Categories : Networking

Tagged as : cli, dhcpsniffing

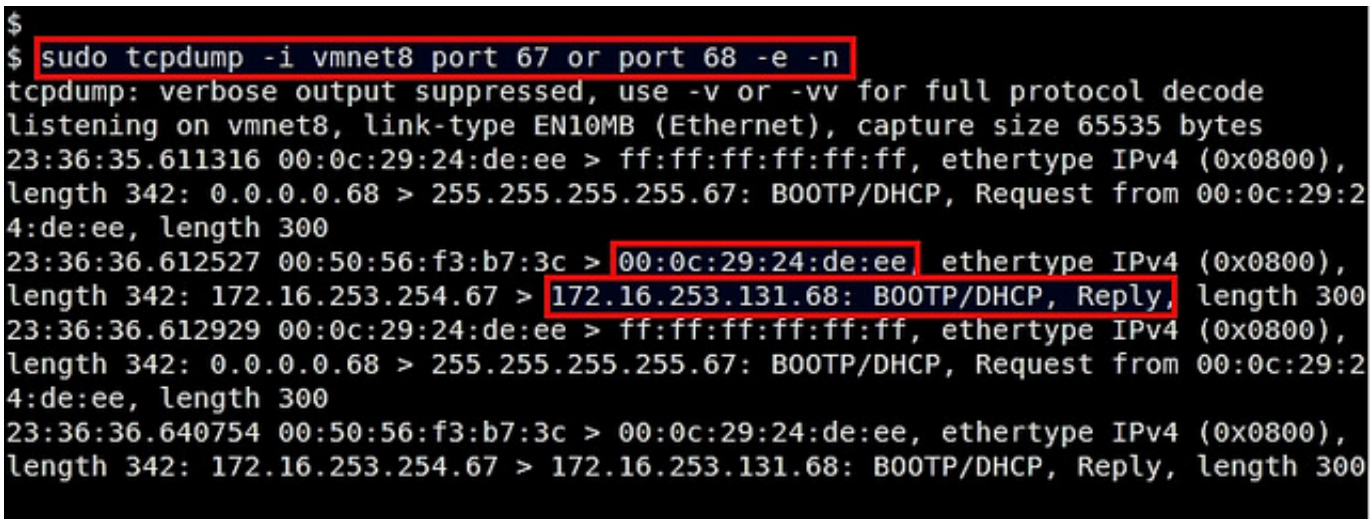
Question: I want to find out what IP address is assigned to a host via DHCP by monitoring DHCP request and response on the wire. How can I monitor DHCP traffic from the command line?

If you want to monitor DHCP communication between a DHCP server and a client, you can run a packet sniffing tool on the same local network, and capture DHCP traffic. There are a couple of sniffing tools you can use.

Method One

The first method to capture DHCP traffic is to use venerable `tcpdump` tool. In this case, you want to define a filter so that `tcpdump` dumps only DHCP related traffic. In DHCP, UDP port number 67 is used by a DHCP server, and UDP port number 68 is used by DHCP clients. Thus, you want to capture traffic with port number 67 or 68 as follows.

```
$ sudo tcpdump -i port 67 or port 68 -e -n
```



The above `tcpdump` output shows that IP address 172.16.253.131 is assigned to a client with hardware address 00:0c:29:24:de:ee.

Method Two

The second method to monitor DHCP requests and responses is to use `dhcpdump`, which is a command-line DHCP packet dumper program.

To install `dhcpdump` on Debian or Ubuntu:

```
$ sudo apt-get install dhcpdump
```

To install `dhcpdump` on CentOS, first enable Repoforge on your system, and then run:

```
$ sudo yum install dhcpdump
```

To install `dhcpdump` on Fedora:

```
$ sudo yum install dhcpdump
```

The following command will dump DHCP requests and responses in a human-readable format.

```
$ sudo dhcpdump -i
```

```
$
$ sudo dhcpdump -i vmnet8
  TIME: 2014-05-11 22:52:57.661
    IP: 0.0.0.0 (0:c:29:24:de:ee) > 255.255.255.255 (ff:ff:ff:ff:ff:ff)
    OP: 1 (BOOTPREQUEST)
 HTYPE: 1 (Ethernet)
  HLEN: 6
  HOPS: 0
   XID: 881f3411
  SECS: 0
 FLAGS: 0
CIADDR: 0.0.0.0
YIADDR: 0.0.0.0
SIADDR: 0.0.0.0
GIADDR: 0.0.0.0
CHADDR: 00:0c:29:24:de:ee:00:00:00:00:00:00:00:00:00:00
 SNAME: .
 FNAME: .
OPTION:  53 (  1) DHCP message type         1 (DHCPDISCOVER)
OPTION:  55 ( 17) Parameter Request List      1 (Subnet mask)
                                             28 (Broadcast address)
                                              2 (Time offset)
                                            121 (Classless Static Route)
                                             15 (Domainname)
                                              6 (DNS server)
                                             12 (Host name)
                                             40 (NIS domain)
                                             41 (NIS servers)
                                             42 (NTP servers)
                                             26 (Interface MTU)
                                            119 (Domain Search)
                                              3 (Routers)
                                            121 (Classless Static Route)
                                            249 (MSFT - Classless route)
                                             33 (Static route)
                                             42 (NTP servers)

--------------------------------------------------------------------------------

  TIME: 2014-05-11 22:52:58.655
    IP: 172.16.253.254 (0:50:56:f3:b7:3c) > 172.16.253.131 (0:c:29:24:de:ee)
    OP: 2 (BOOTPREPLY)
 HTYPE: 1 (Ethernet)
  HLEN: 6
  HOPS: 0
   XID: 881f3411
  SECS: 0
 FLAGS: 0
CIADDR: 0.0.0.0
YIADDR: 172.16.253.131
SIADDR: 172.16.253.254
GIADDR: 0.0.0.0
CHADDR: 00:0c:29:24:de:ee:00:00:00:00:00:00:00:00:00:00
 SNAME: .
 FNAME: .
OPTION:  53 (  1) DHCP message type         2 (DHCPOFFER)
OPTION:  54 (  4) Server identifier         172.16.253.254
OPTION:  51 (  4) IP address leasetime      1800 (30m)
OPTION:   1 (  4) Subnet mask               255.255.255.0
OPTION:  28 (  4) Broadcast address         172.16.253.255
OPTION:  15 ( 11) Domainname                localdomain
OPTION:   6 (  4) DNS server                172.16.253.2
OPTION:   3 (  4) Routers                   172.16.253.2
--------------------------------------------------------------------------------
```

The output shown by `dhcpdump` is more detailed than that of `tcpdump`. "YIADDR" field is populated with the IP address offered by a DHCP server to a client, and "CHADDR" field is the hardware address of the requesting client. It also shows other information such as DHCP lease time, subnet mask, DNS server, etc.

`dhcpdump` can filter DHCP responses such that it captures only DHCP responses sent to a particular hardware address.

For example, the following command will capture DHCP response packets sent to client whose hardware address starts with "00:c1:b5".

```
$ sudo dhcpdump -i eth0 -h ^00:c1:b5
```