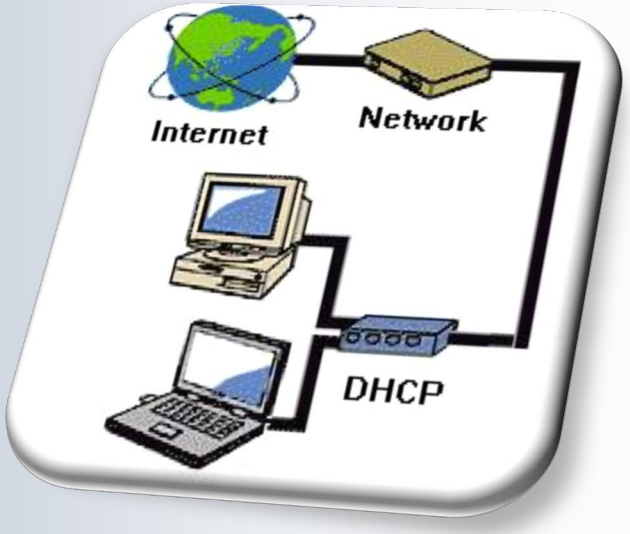
COMP 175

System Administration and Security

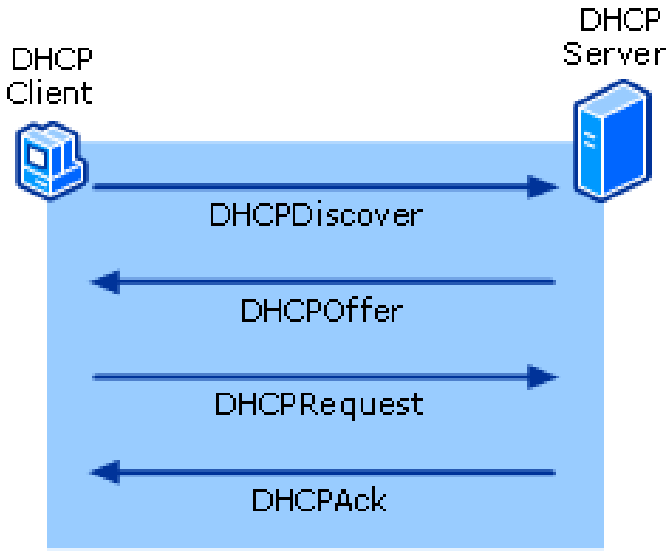


DHCP

Dynamic Host Configuration Protocol

DHCP Configuration

- Objectives
- Upon completion you will be able to:
  - Know the types of information required by a system on boot-up
  - Know how DHCP operates
  - Know how to configure DHCP
- **Who's down with DHCP?**



BOOTP

Back in the olden days.....

- The client/server Bootstrap Protocol (BOOTP) can configure a diskless computer or other device at boot time. BOOTP provides the:
  - IP address
  - net mask
  - the address of a default router
  - the address of a name server.
- BOOTP is static. When a client workstation asks for the above info, it is retrieved from a fixed table. Same results every time.

DHCP

- Dynamic Host Configuration Protocol
- DHCP automates the process of issuing IP addresses and other network related information necessary to access a network and the Internet.
- Safe and reliable configuration
  - DHCP avoids configuration errors caused by manually entering values at each computer
  - DHCP helps prevent duplicate address conflicts

DHCP

- Reduced configuration management
  - Using DHCP servers can greatly decrease time spent configuring and reconfiguring computers on the network
  - TCP/IP configuration is centralized and automated
  - Network administrators can centrally define global and sub-net specific TCP/IP configurations
  - Mobile users can travel anywhere on the intranet and automatically receive IP addresses when they reconnect to the network

Admins

Users

DHCP

DHCP Protocol
0100101 0100101 01001010

Dynamic Host Configuration Protocol

- DHCP provides
  - IP address
  - a lease time
  - routing (gateway) ip
  - subnet mask
  - dns server(s) ip information
  - optional parameters (cool stuff)

IP Address Allocation

- Automatic allocation
  - DHCP assigns a permanent IP address to a client
- Dynamic allocation
  - DHCP assigns an IP address to a client for a limited period of time (or until the client explicitly relinquishes the address)
- Manual allocation
  - a client's IP address is assigned by the network administrator, and DHCP is used simply to convey the assigned address to the client

History of DHCP

- DHCP is defined by RFC 2131
- Several other Internet protocols that address some parts of the host configuration problem:
  - Reverse Address Resolution Protocol (RARP) and Dynamic RARP (DRARP) for network address discovery
  - Trivial File Transfer Protocol (TFTP) provides for transport of a boot image from a boot server
  - Internet Control Message Protocol (ICMP) provides for informing hosts of additional routers including the subnet mask information.
  - BOOTP (predecessor of DHCP) an extensible transport mechanism for a collection of configuration information

BOOTP vs. DHCP

- DHCP is backwards compatible with BOOTP (was designed to be)
- DHCP includes a flags fields (unused field in BOOTP).
- Options are now 312 bytes (was 64)
- The DHCP “Message Type” option identifies DHCP messages
- sname and file fields can be used to hold additional options in DHCP

DHCP Is Not

What DHCP is not:

- DHCP allows but does not require the configuration of client parameters not directly related to the IP protocol
- DHCP does not address registration of newly configured clients with the Domain Name System (DNS)
- DHCP is not intended for use in configuring routers

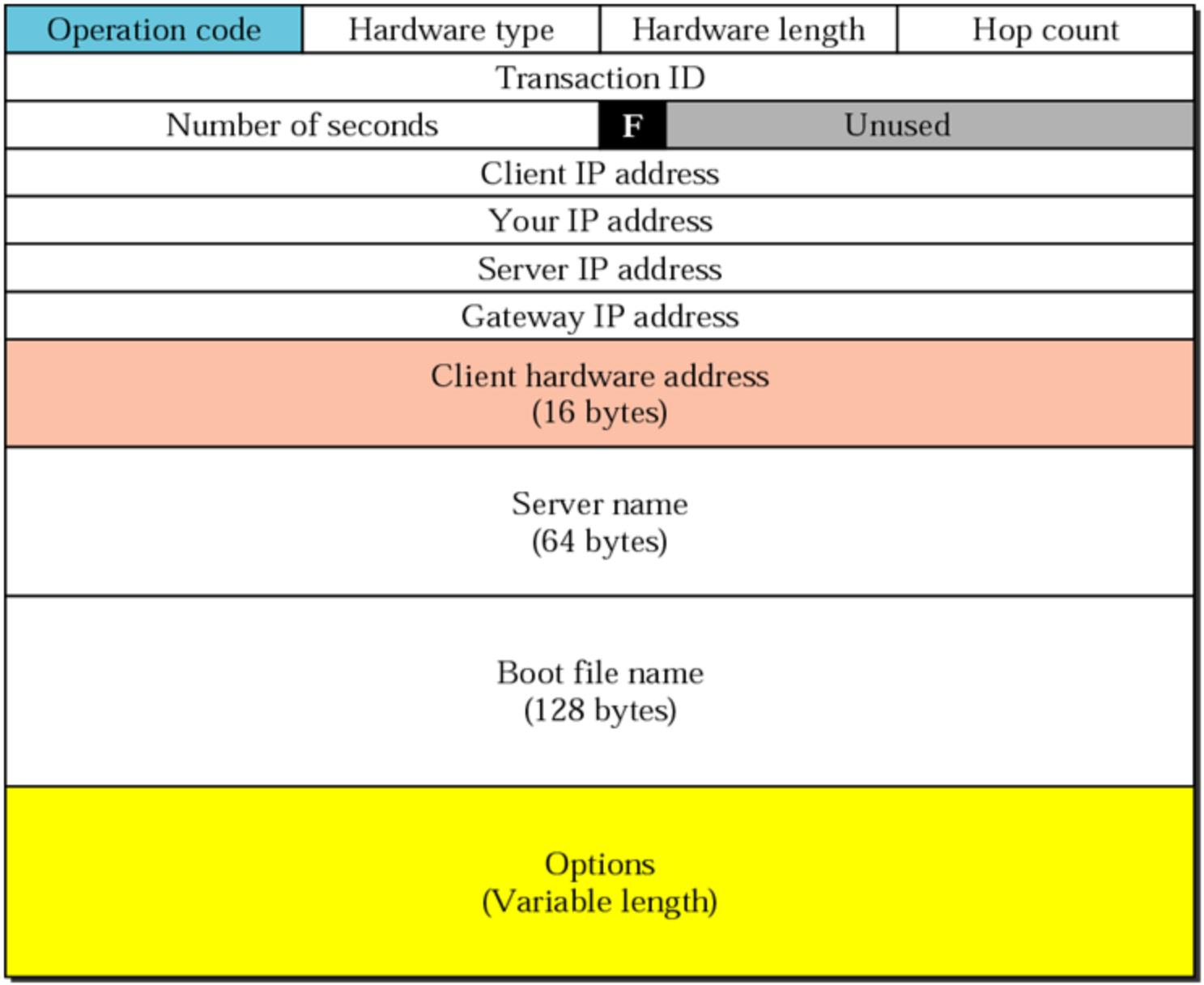
DHCP Terminology

- DHCP Server
  - Host running a DHCP Deamon (DHCPD) that provides and manages the configuration parameters for client hosts using UDP Transport (port 67)
- DHCP Client
  - Host that requests configuration parameters from a DHCP Server, uses the UDP transport (port 68)
- Relay agent
  - A host or router that passes DHCP messages between DHCP clients and DHCP servers
- Binding
  - Collection of configuration parameters, including at least an IP address, bound to a DHCP client

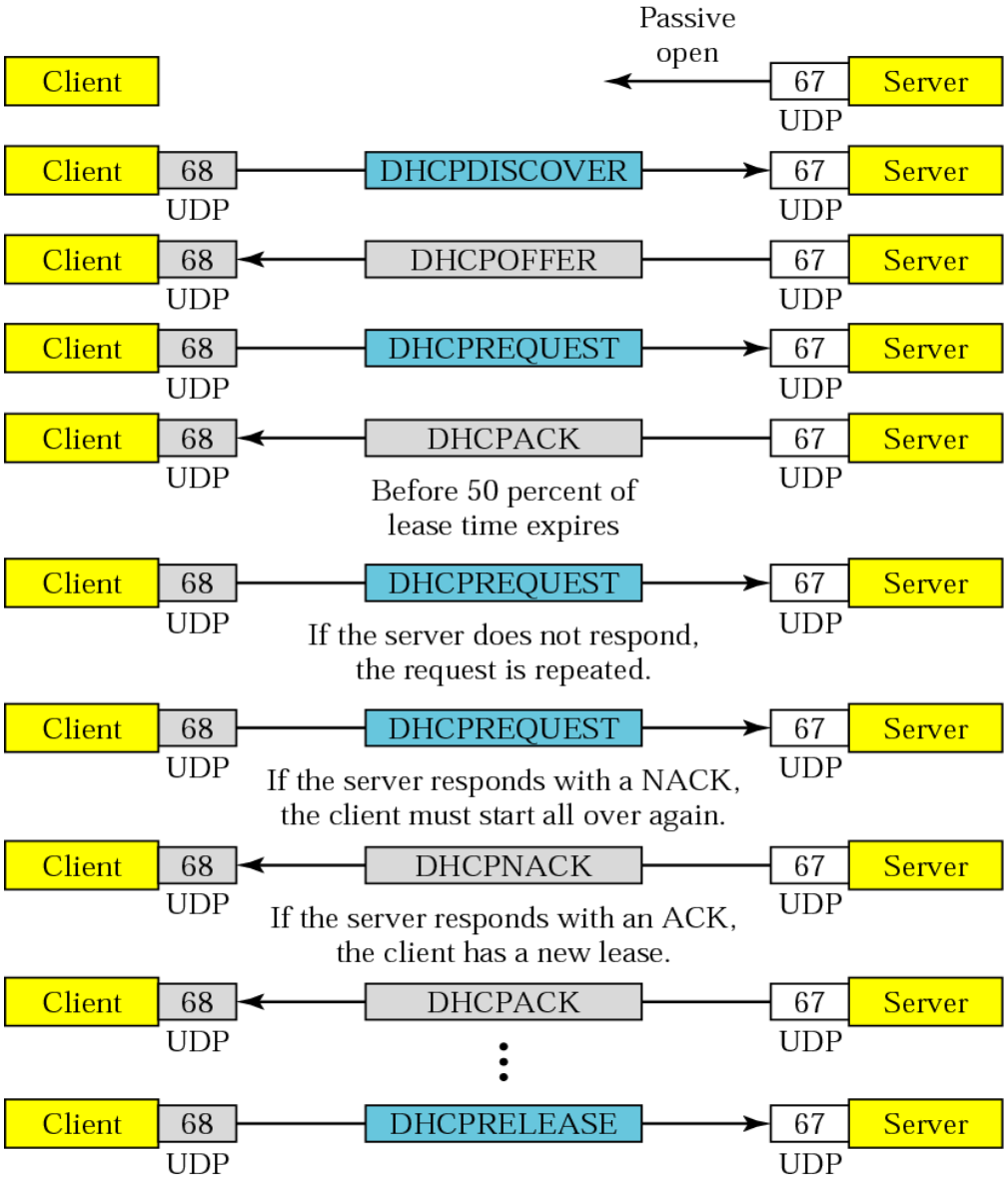
DHCP Workings

- DHCP has a pool of available addresses. When a request arrives, DHCP pulls out the next available address and assigns it to the client for a negotiable time period.
- When a request comes in from a client, the DHCP server first consults the static table.
- DHCP is great when devices and IP addresses change
- The DHCP packet format is almost identical to the BOOTP packet format (in order to be compatible with BOOTP).
- Only difference is 1-bit flag.

Packet Format



DHCP Exchange



Discover: client tries to find out what servers are out there.

Offer: those servers that can provide this service respond

Request: client selects one offer and makes a request

ACK: server acks the request

When 50% of the lease period is expired, client asks for a renewal.

If ACK received, reset timer. If NAK, go back to intializing state.

DHCP Options

- DHCP Options are defined in RFC 2132
- One option (option 53) is the “Message Type” option that in turn defines 8 types of messages:
  1. DHCPDISCOVER
  2. DHCPOFFER
  3. DHCPREQUEST
  4. DHCPDECLINE
  5. DHCPACK
  6. DHCPNAK
  7. DHCPRELEASE
  8. DHCPINFORM

Sample Message Exchange

Sample Client Broadcast:

```
Frame:  dst: ff:ff:ff:ff:ff:ff
        src: cc:ll:ii:ee:nn:tt
IP:     dst: 255.255.255.255
        src: 0.0.0.0
UDP:    dst: 67
        src: 68
DHCP:   chaddr: cc:ll:ii:ee:nn:tt
        ci addr: 0.0.0.0
        gi addr: 0.0.0.0
        yi addr: 0.0.0.0
        flags = 0
        transaction id = 1476309821
        Options:
          Message Type = DISCOVER
        (additional options follow)
```

Sample Server Response:

```
Frame:  dst: cc:ll:ii:ee:nn:tt
        src: ss:ee:rr:vv:ee:rr
IP:     dst: 255.255.255.255
        src: 192.168.0.1
UDP:    dst: 68
        src: 67
DHCP:   chaddr: cc:ll:ii:ee:nn:tt
        ci addr: 0.0.0.0
        gi addr: 0.0.0.0
        yi addr: 192.168.0.2
        flags = 0
        transaction id = 1476309821
        Options:
          Message Type = OFFER
        (additional options follow)
```

DHCP

DHCP Protocol

DORA

- Discover
- Offer
- Request
- Acknowledge

And

- Release, Decline, NAck

DHCP Messages

- DHCPDISCOVER
  - The client broadcasts message in search of available DHCP servers.
- DHCPOFFER
  - The server response to the client DHCPDISCOVER with offer of configuration parameters .

DHCP Messages

- DHCPREQUEST
  - The client broadcasts to the server, requesting offered parameters from one server specifically.
  - Confirms correctness of previously allocated address after, e.g., system reboot.
  - Extends the lease on a particular network address.
- DHCPRELEASE
  - The client-to-server communication, relinquishing network address and canceling remaining lease.

DHCP Messages

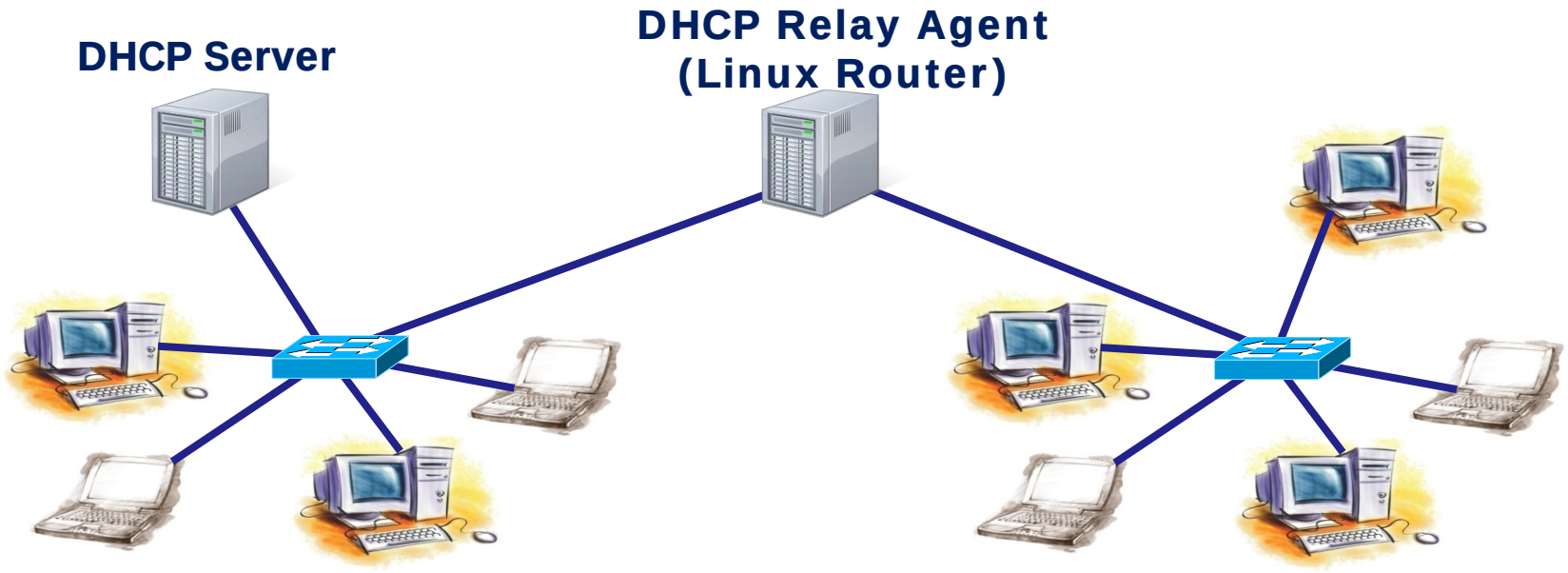
- DHCPACK
  - The server-to-client communication with configuration parameters, including committed network address.
- DHCPNAK
  - Server to client indicating client's notion of network address is incorrect (e.g., client has moved to new subnet) or client's lease as expired

DHCP Process

- DHCPDECLINE
  - The client-to-server communication, indicating that the network address is already in use.
- DHCPINFORM
  - The client-to-server communication, asking for only local configuration parameters that the client already has externally configured as an address.

DHCP Process

- All interactions are initiated by a client
- Server only replies
- Obtain an IP address automatically
- Configuring the host to the network is done by a simple handshake



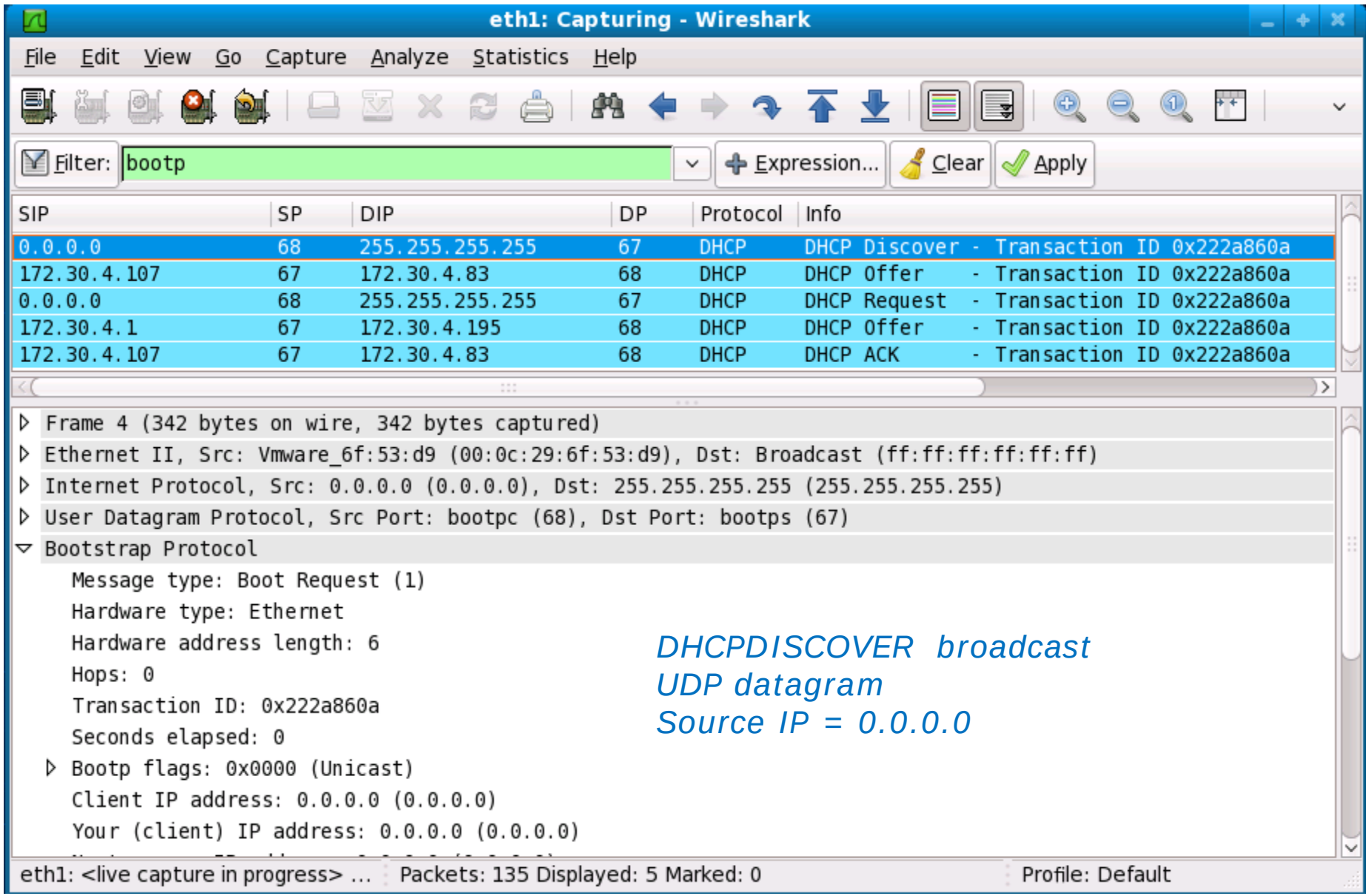
DHCP Process

- Client broadcasts DHCPDISCOVER
- One or more servers return DHCPOFFER with available address and network information
- Client chooses one offer that it likes best
- Broadcasts DHCPREQUEST to identify chosen Server/lease
- DHCPREQUEST also to renew lease

DHCP Process

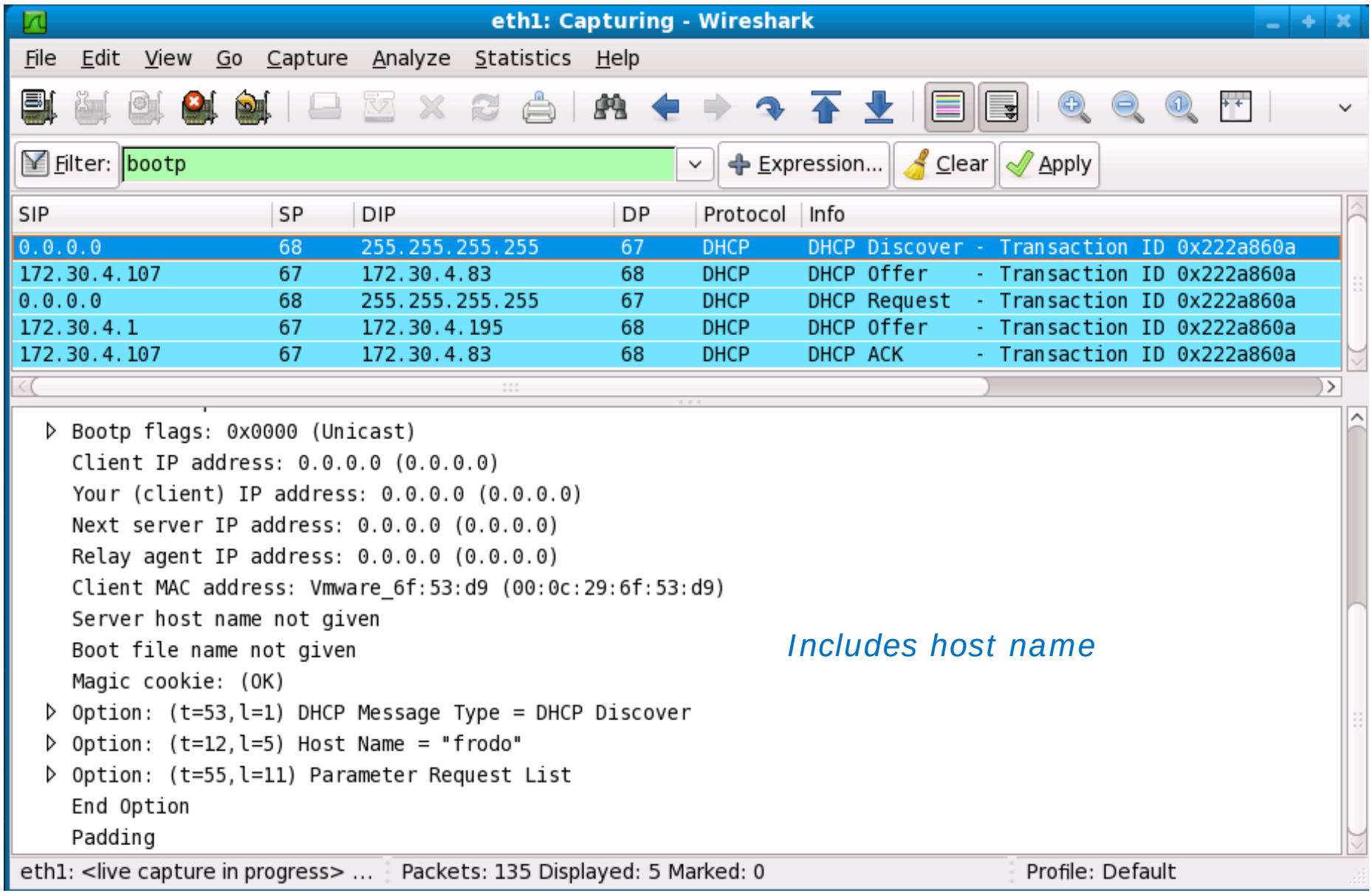
- Server sends
  - DHCPACK
    - Lease is finalized
    - Client starts using IP
  - DHCPNAK
    - Client resumes from DHCPDISCOVER point
- If client doesn’t want IP - DHCPDECLINE is sent
- DHCPRELEASE gives IP back into pool

DHCPDISCOVER



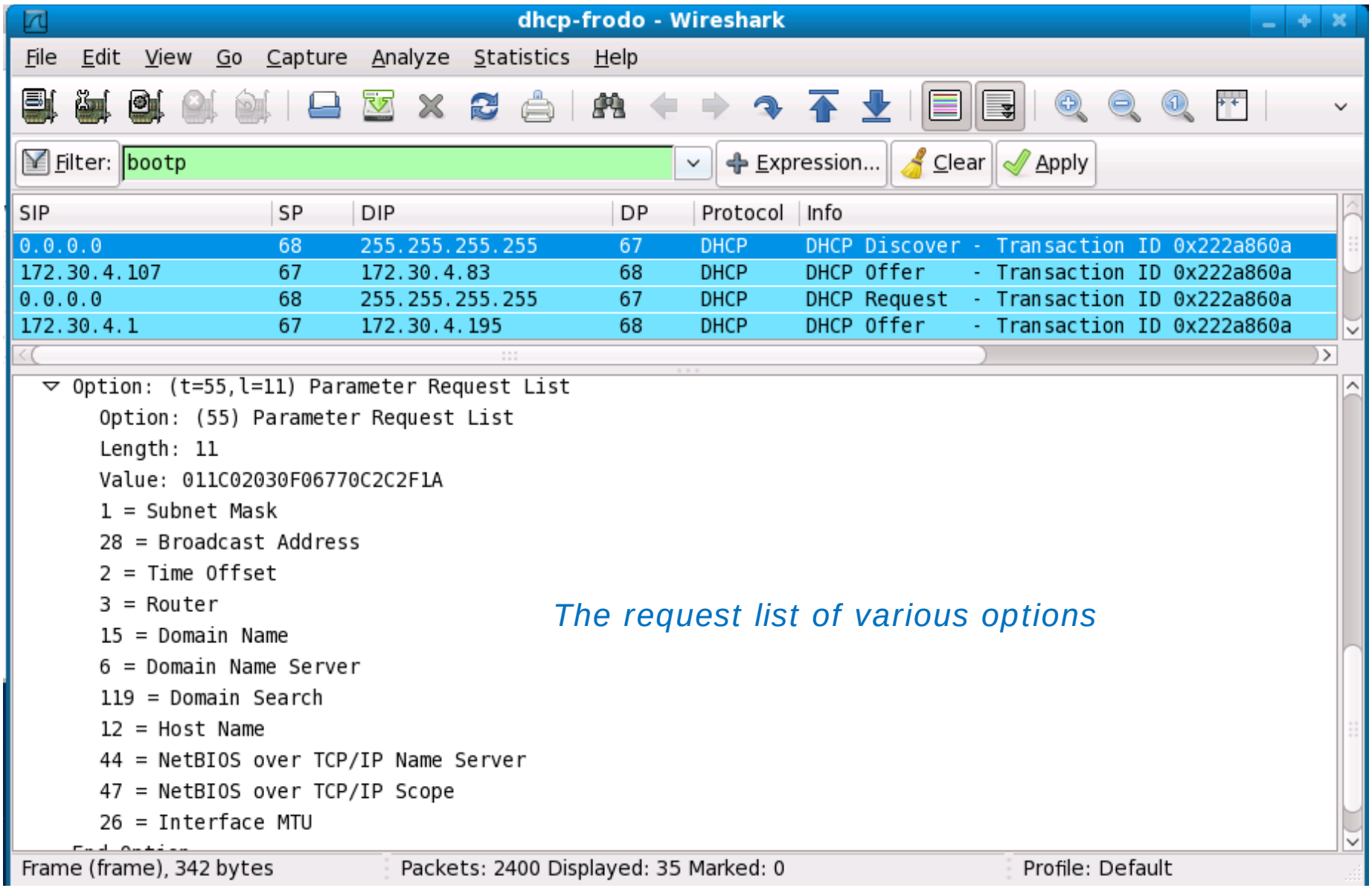
DHCPDISCOVER broadcast
UDP datagram
Source IP = 0.0.0.0

DHCPDISCOVER



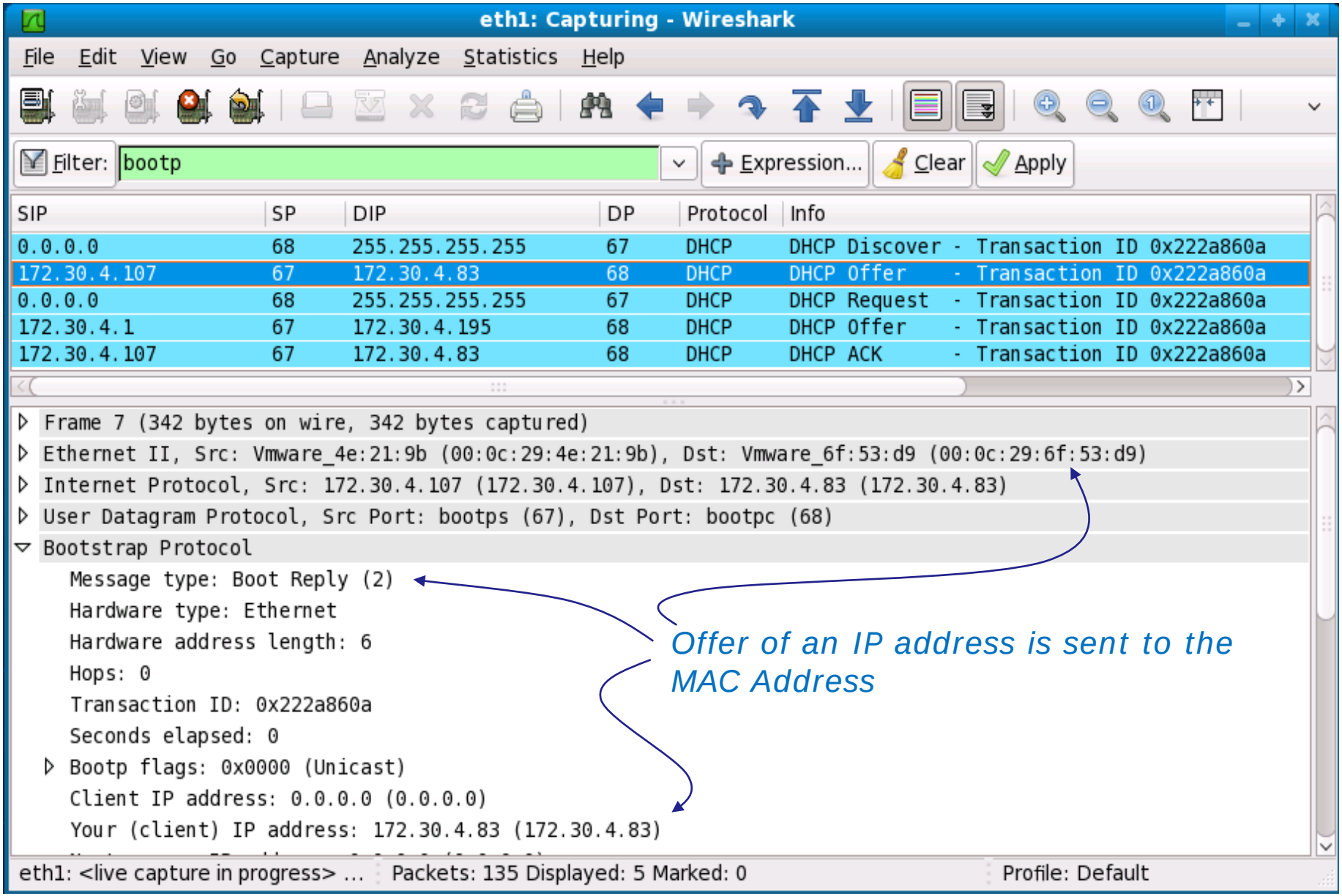
Includes host name

DHCP



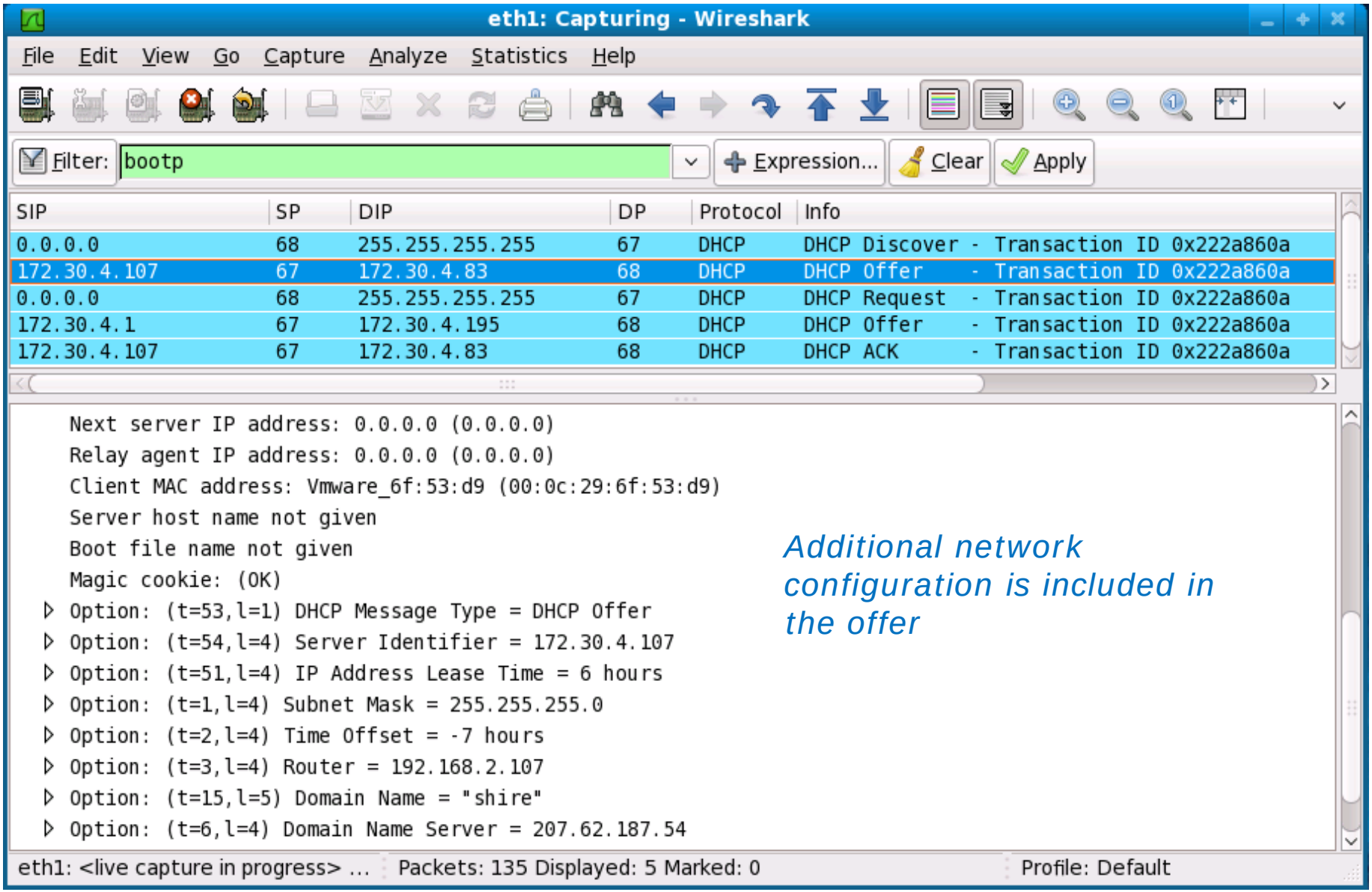
The request list of various options

DHCPOFFER



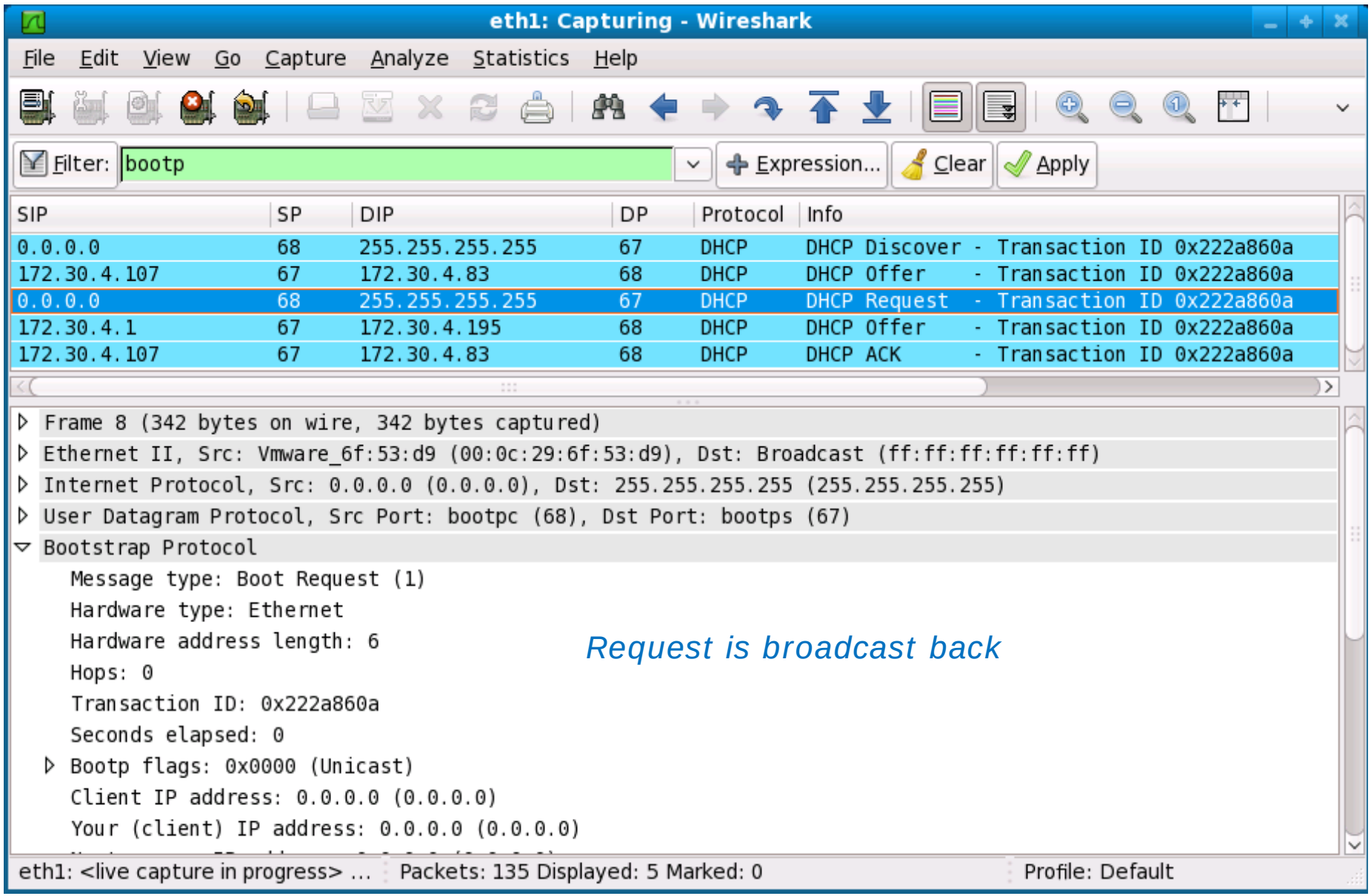
Offer of an IP address is sent to the MAC Address

DHCPOFFER



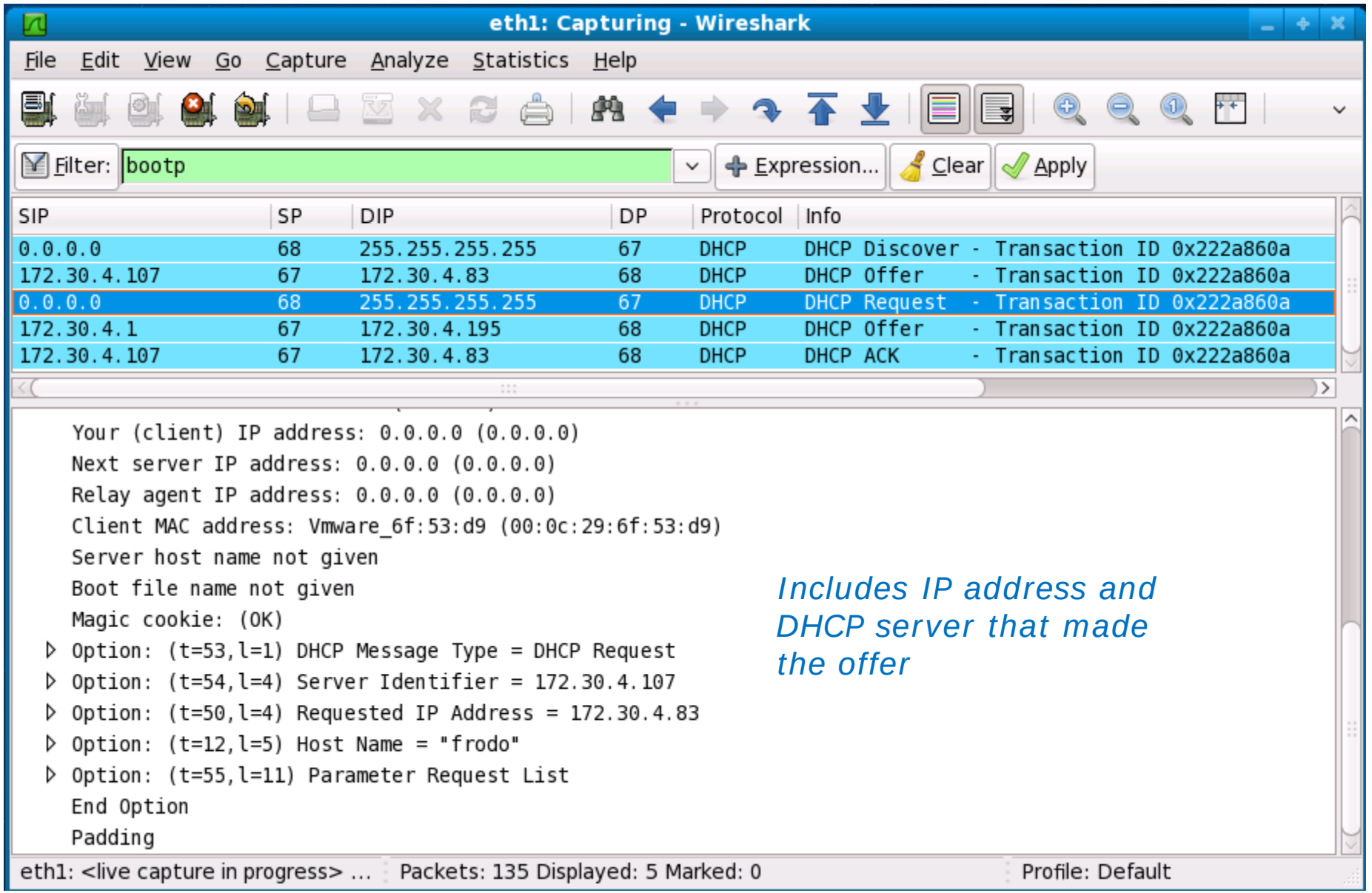
Additional network configuration is included in the offer

DHCPREQUEST



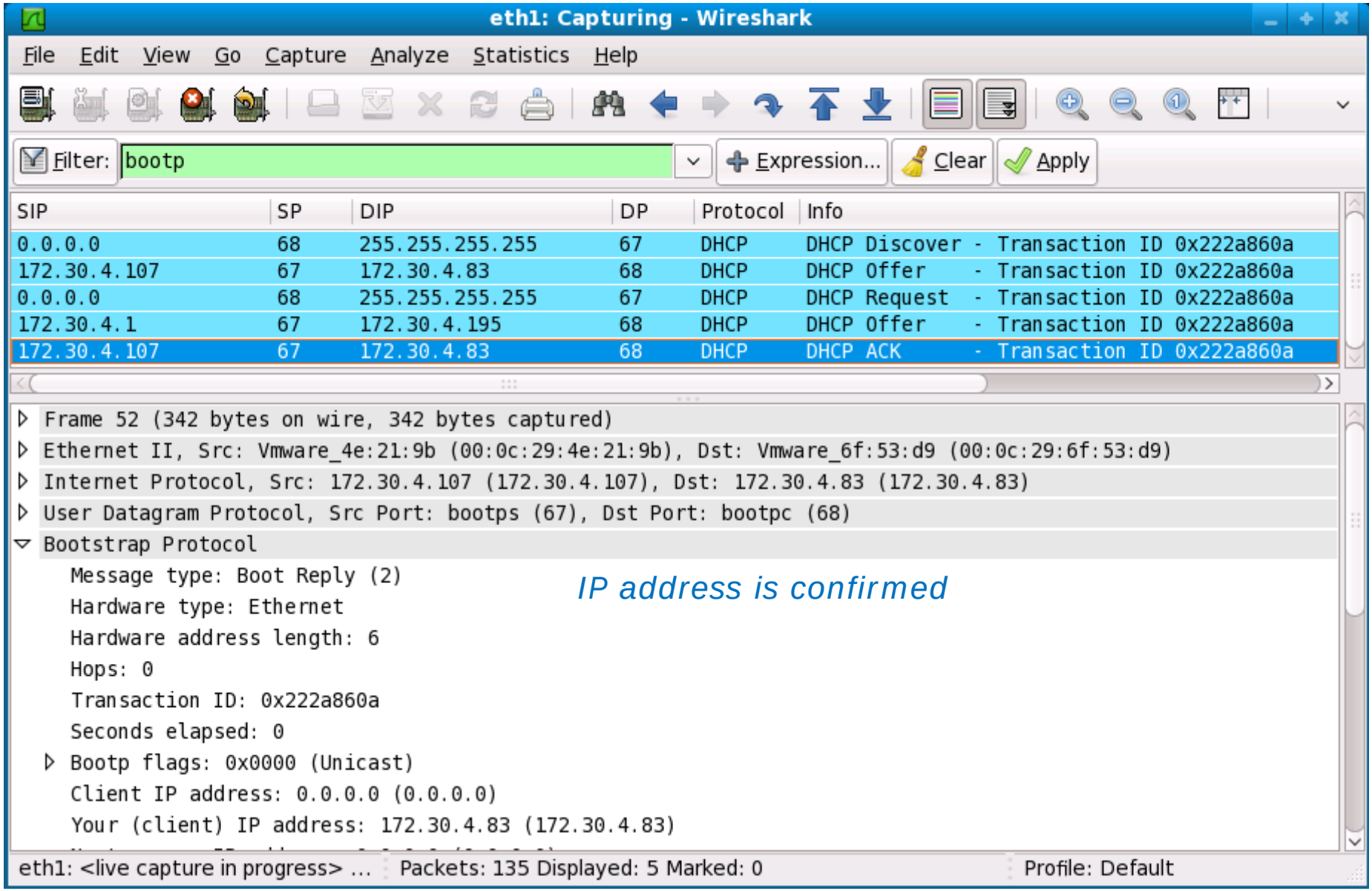
Request is broadcast back

DHCPREQUEST

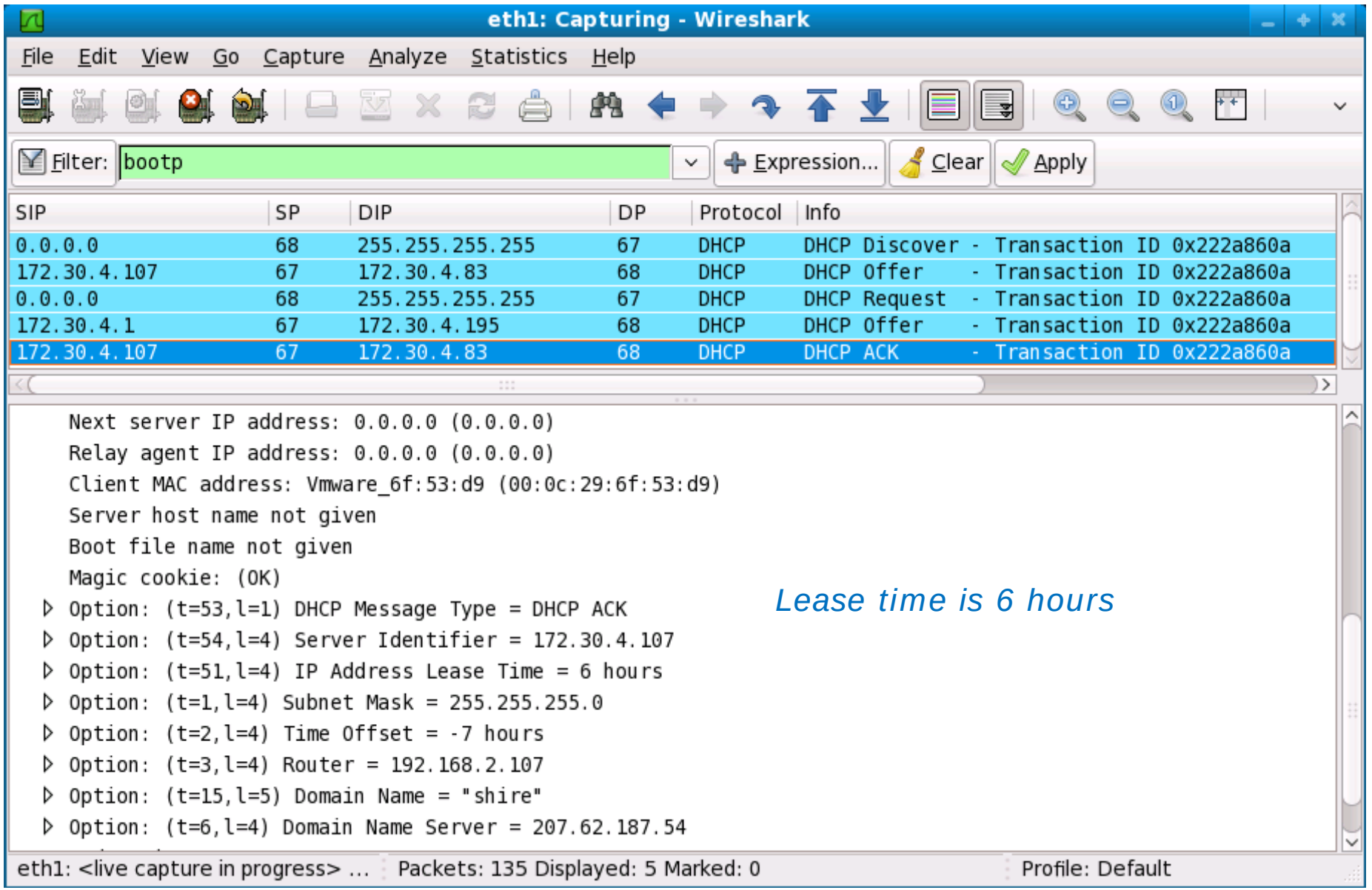


Includes IP address and DHCP server that made the offer

DHCPACK

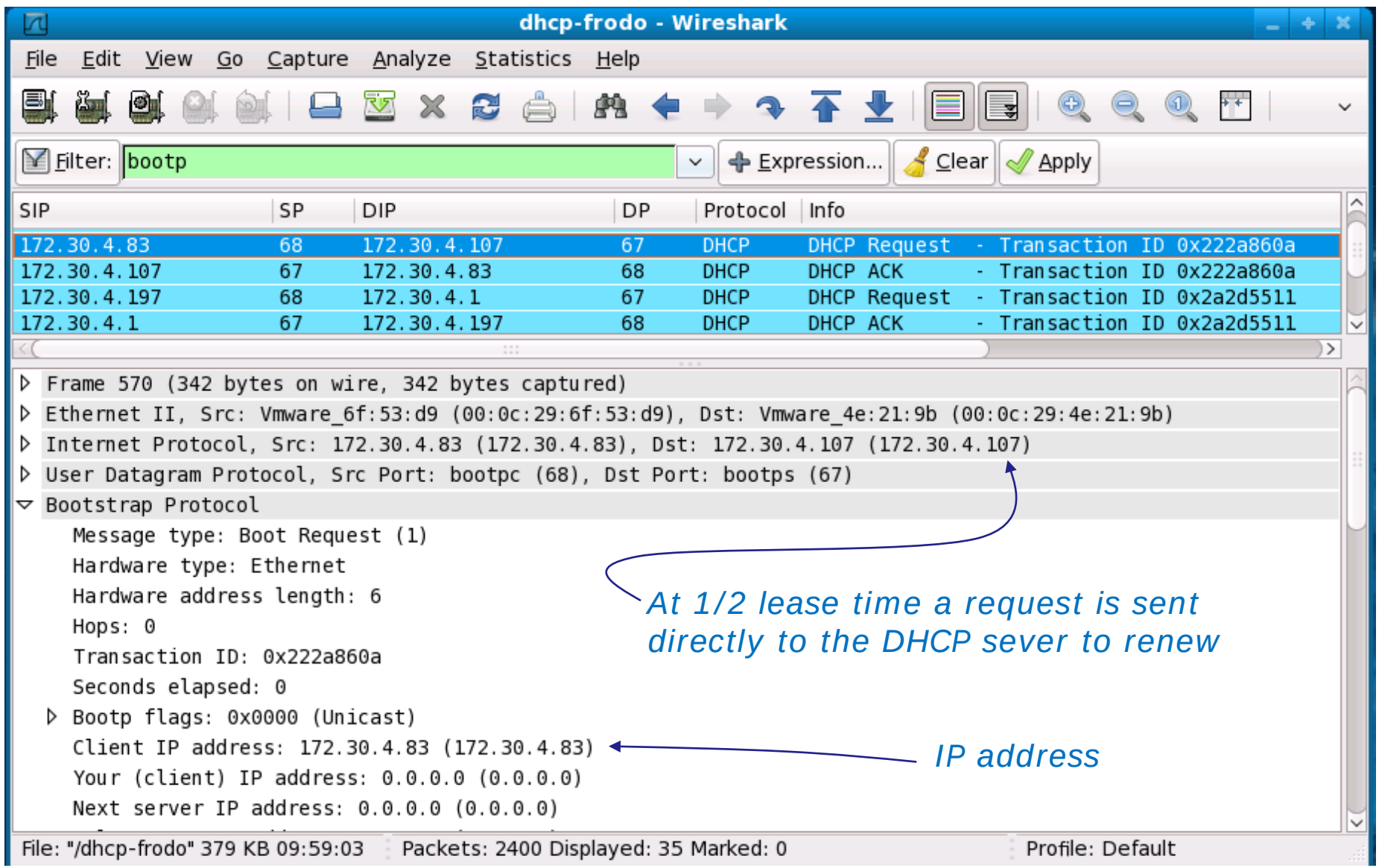

eth1: Capturing - Wireshark
File Edit View Go Capture Analyze Statistics Help
Filter: bootp
Expression... Clear Apply
SIP SP DIP DP Protocol Info
0.0.0.0 68 255.255.255.255 67 DHCP DHCP Discover - Transaction ID 0x222a860a
172.30.4.107 67 172.30.4.83 68 DHCP DHCP Offer - Transaction ID 0x222a860a
0.0.0.0 68 255.255.255.255 67 DHCP DHCP Request - Transaction ID 0x222a860a
172.30.4.1 67 172.30.4.195 68 DHCP DHCP Offer - Transaction ID 0x222a860a
172.30.4.107 67 172.30.4.83 68 DHCP DHCP ACK - Transaction ID 0x222a860a
Frame 52 (342 bytes on wire, 342 bytes captured)
Ethernet II, Src: Vmware_4e:21:9b (00:0c:29:4e:21:9b), Dst: Vmware_6f:53:d9 (00:0c:29:6f:53:d9)
Internet Protocol, Src: 172.30.4.107 (172.30.4.107), Dst: 172.30.4.83 (172.30.4.83)
User Datagram Protocol, Src Port: bootps (67), Dst Port: bootpc (68)
Bootstrap Protocol
Message type: Boot Reply (2)
Hardware type: Ethernet
Hardware address length: 6
Hops: 0
Transaction ID: 0x222a860a
Seconds elapsed: 0
Bootp flags: 0x0000 (Unicast)
Client IP address: 0.0.0.0 (0.0.0.0)
Your (client) IP address: 172.30.4.83 (172.30.4.83)
IP address is confirmed
eth1: <live capture in progress> ... Packets: 135 Displayed: 5 Marked: 0 Profile: Default

DHCPACK

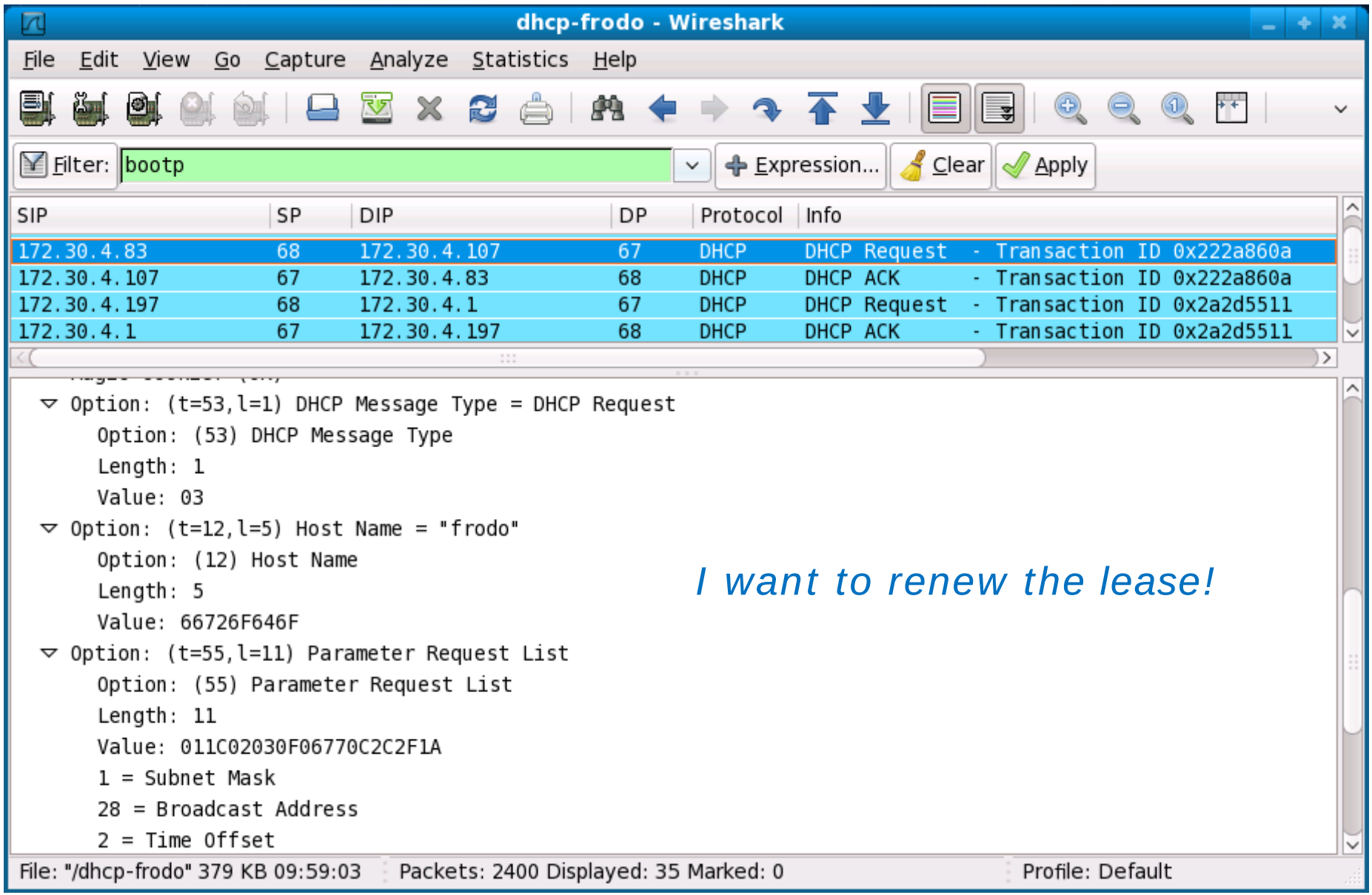


Lease time is 6 hours

DHCPREQUEST - Timer

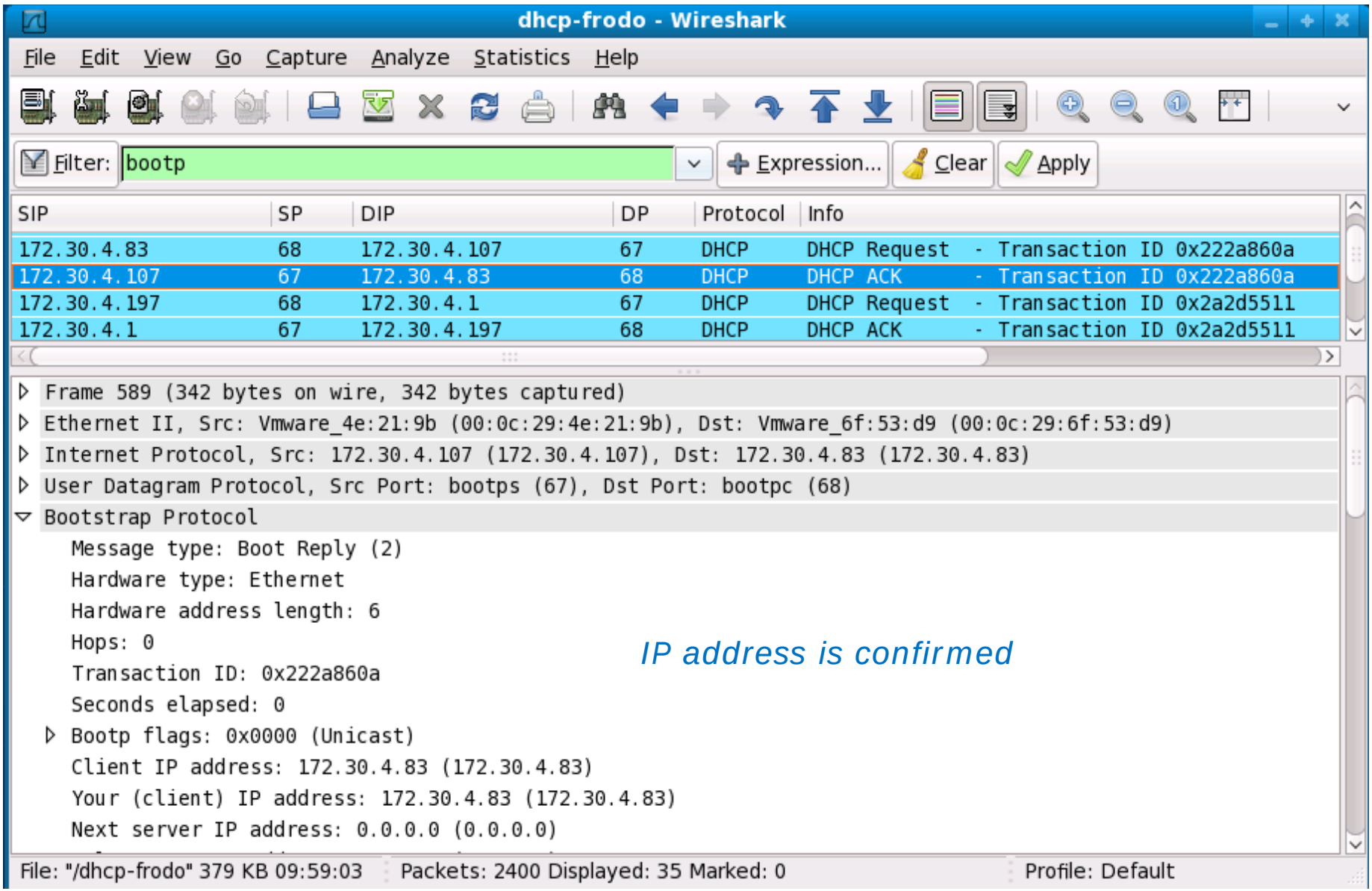


DHCPREQUEST



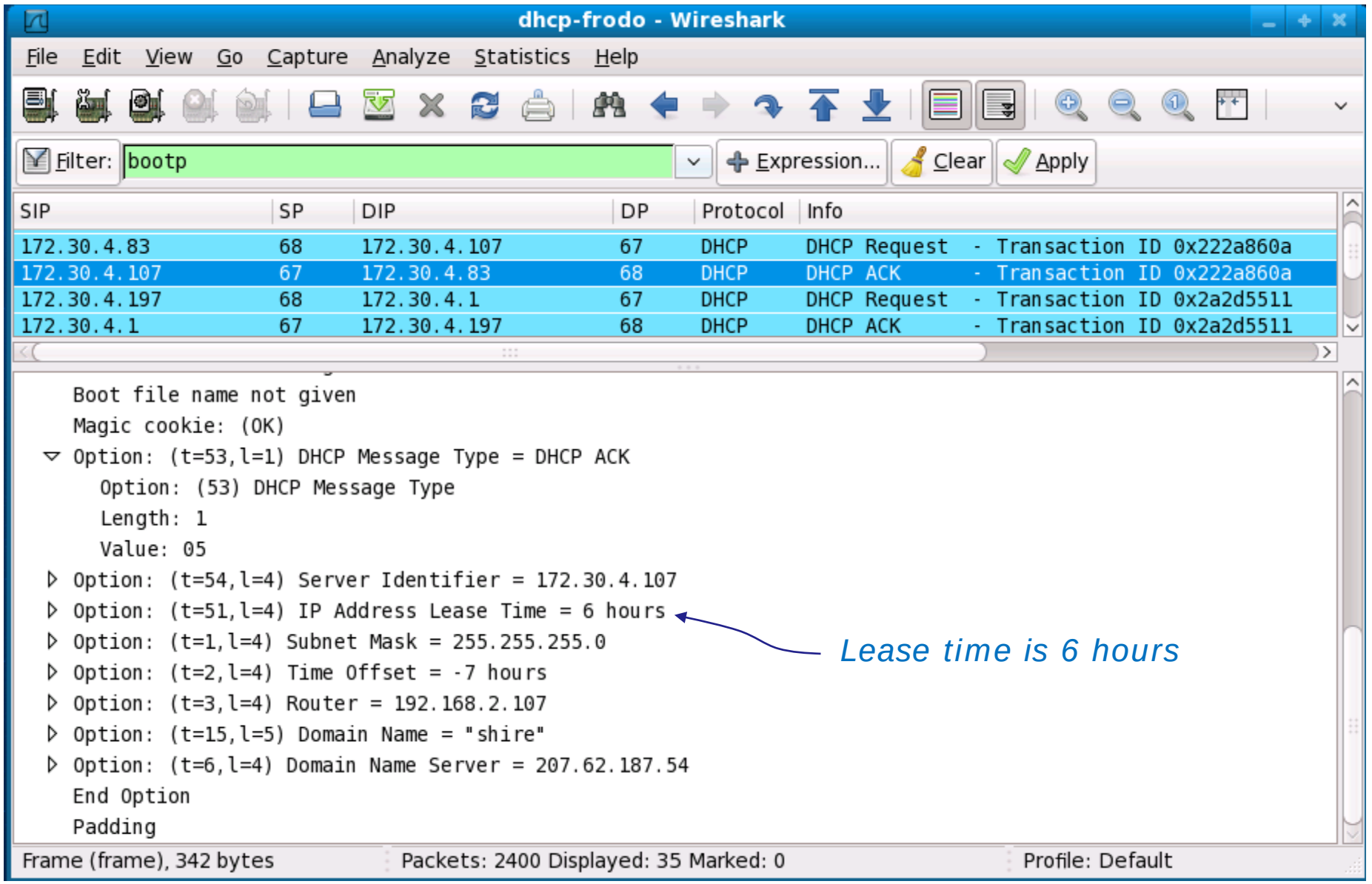
I want to renew the lease!

DHCPACK



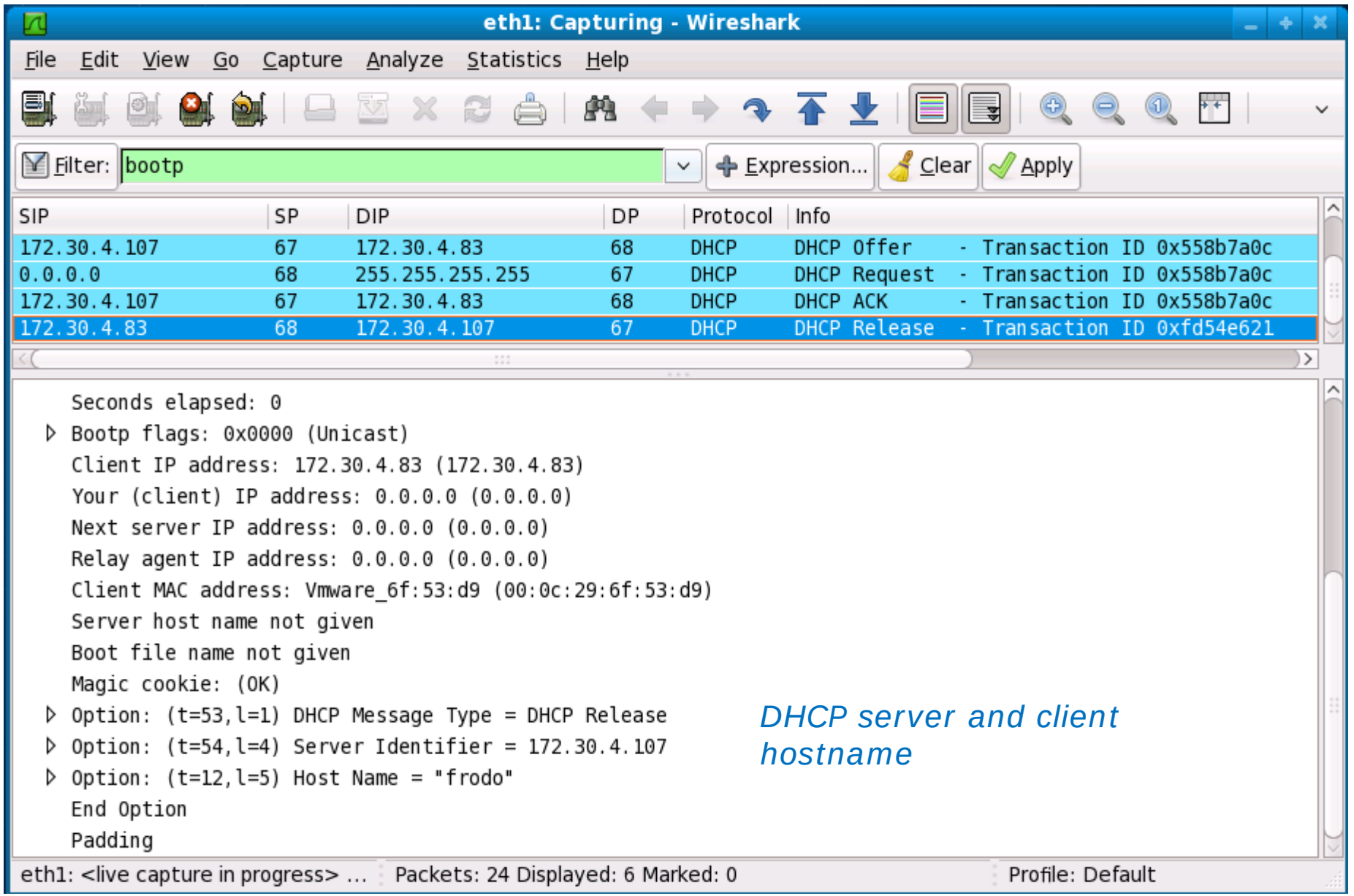
IP address is confirmed

DHCPACK



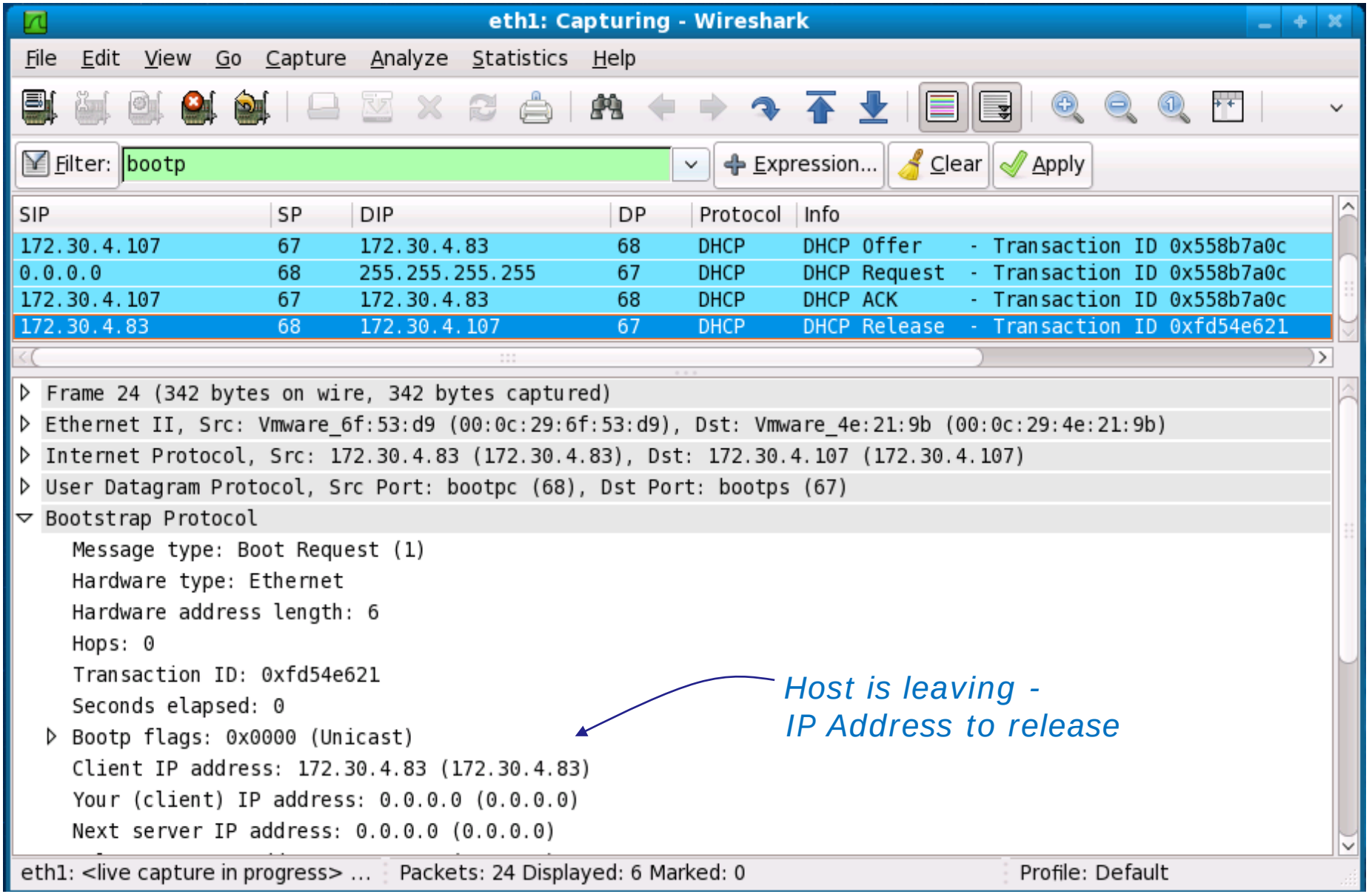
Lease time is 6 hours

DHCPRELEASE



DHCP server and client hostname

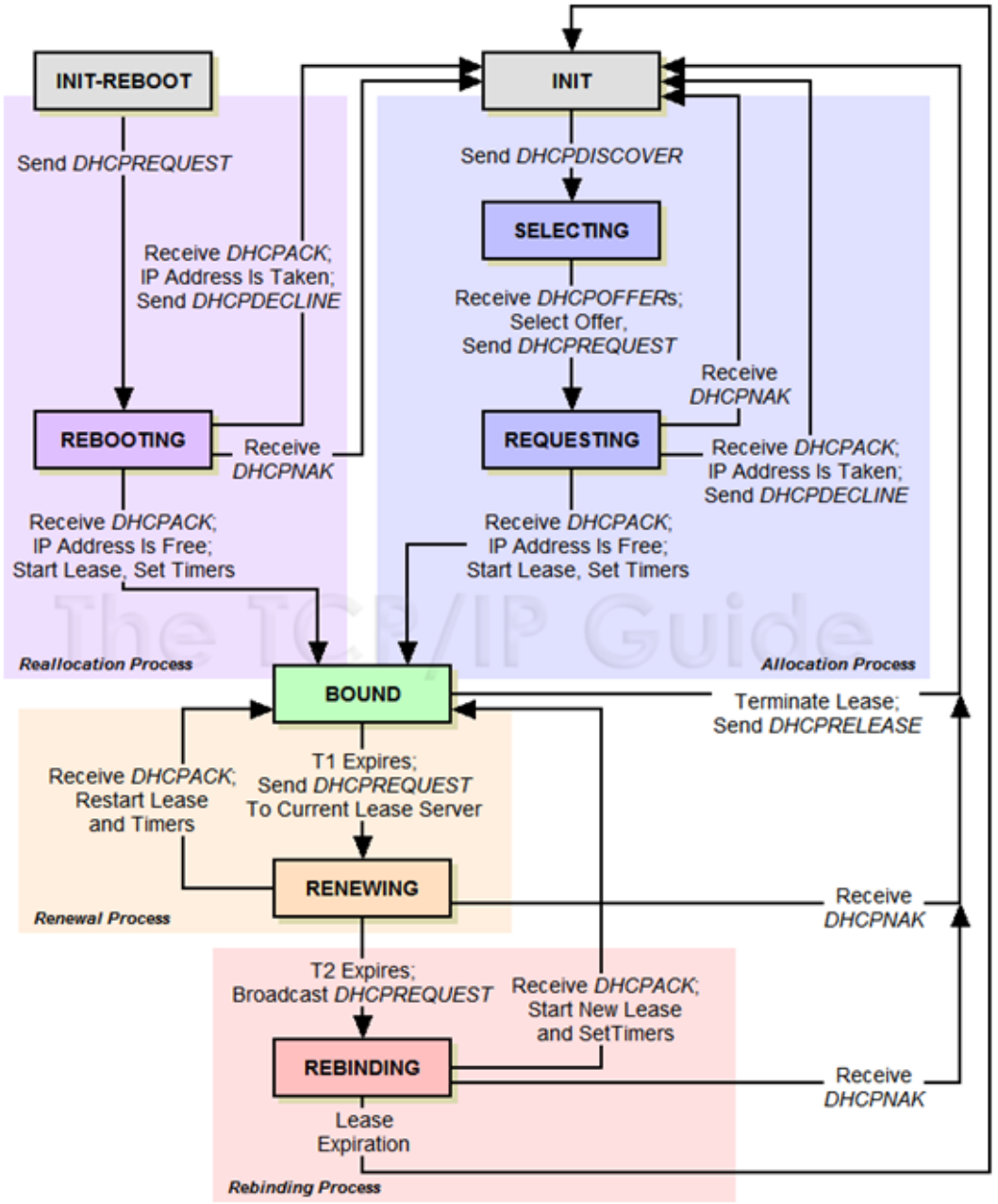
DHCPRELEASE



DHCP Process

States

Client driven



DHCP Process

- Client is responsible to renew/release IP
- Lease timestamps:
  - Total lease duration
  - T1 (0.5 * duration_of_lease)
    - client enters the RENEWING state
    - contacts the server that originally issued network address
  - T2 (0.875 * duration_of_lease)
    - client enters the REBINDING state
    - attempts to contact any server

DHCP as UDP Application

- DHCP server - port 67, client - port 68
- Reliability is not provided by UDP
- Client is responsible for reliability
  - Client implements timer to measure timeout for messages not responded to
  - Client adopts a retransmission strategy uses a randomized exponential backoff algorithm to determine the delay between retransmissions
  - Every next message acts as an acknowledgment for the previous step
    - For example, DHCPREQUEST is an ACK for DHCPOFFER

DHCP Process

- Lease duration
  - Client holds IP when not connected
  - Clients retire
  - Servers/Databases should have constant IP´s
- Analyze The Network
  - Sufficient addresses available?
  - Performance?
  - Servers?
  - Redundancy is available
  - Failover is available
  - DHCP must be up before clients – use a UPS

DHCP Terms

- Scopes and exclusions
  - A pool of IP addresses that can be assigned to clients
- Reservations
  - IP addresses can be reserved for specific computers using MAC addresses
- Leases
  - Clients no longer own their own IP address and instead lease one from a DHCP server
  - The lease has a time limit but can be renewed

Sample.conf

```
# dhcpd.conf  - SOHO configuration file
# last edit 07/04/2011 m2
#           08/14/2011 m2 added option hostname
# restart with: /usr/sbin/dhcpd -q eth0
# check leases with:  cat /var/state/dhcp/dhcpd.leases
# global options
# lease times in seconds - renews attempted at 50%
default-lease-time 86400;
max-lease-time 691200;
option interface-mtu 1500;
ddns-update-style none;
option domain-name "treacle.com";
option domain-name-servers 10.0.0.2;
option ntp-servers 10.0.0.2;
```

Sample.conf (continued)

```
# network declaration
#
subnet 10.0.0.0 netmask 255.255.255.0 {
     range 10.0.0.112  10.0.0.127;
     option subnet-mask 255.255.255.0;
     option broadcast-address 10.0.0.255;
     option routers 10.0.0.2;
     option ip-forwarding off;
     authoritative;
     option netbios-node-type 8;}
host MarchHare {
    hardware ethernet bc:ae:c5:01:1d:3e;
    option host-name "MarchHare";
    fixed-address 10.0.0.5; }
```

leases

- cat /var/state/dhcp/dhcpd.leases
- The header as in V3.0pl2

```
# All times in this file are in UTC (GMT), not your local
# timezone. This is not a bug, so please don't ask about it.
# There is no portable way to store leases in the local
# timezone, so please don't request this as a feature.
# If this is inconvenient or confusing to you, we sincerely
# apologize.  Seriously, though - don't ask.
```

leases

```
lease 10.0.0.126 {
  starts 2 2011/10/11 01:37:56;
  ends 3 2011/10/12 01:37:56;
  tstp 3 2011/10/12 01:37:56;
  binding state free;
  hardware ethernet 68:a3:c4:3c:b1:9d;
  uid "\001h\243\304<\261\235";
  client-hostname "GMLaptop";
}
lease 10.0.0.118 {
  starts 4 2011/10/13 19:55:07;
  ends 5 2011/10/14 19:55:07;
  binding state active;
  next binding state free;
  hardware ethernet 00:1c:c3:9e:ee:ae;
  uid "\001\000\034\303\236\356\256";
  client-hostname "DIRECTV-HR23-C39EEEAE";
}
```

DHCP syslog Entries

Oct 15 15:19:43 tea dhcpd:

DHCPDISCOVER from 28:ef:01:aa:1c:44 via eth0

DHCPOFFER on 10.0.0.114 to 28:ef:01:aa:1c:44 via eth0

DHCPREQUEST for 10.0.0.114 (10.0.0.2) from 28:ef:01:aa:1c:44 via eth0

DHCPACK on 10.0.0.114 to 28:ef:01:aa:1c:44 via eth0

Wrote 0 deleted host decls to leases file.

Wrote 0 new dynamic host decls to leases file.

Wrote 14 leases to leases file.

DHCP Issues

- Watch out for DHCP conflicts
  - DSL/Cable box
  - Wireless
    - Use strong passphrase
    - Limit 'guest' lease access
    - Don't carelessly leave wide open
- You are the network administrator
- You are the security administrator

Ubuntu Desktop

- sudo apt install net-tools

```
root@Jammy:/etc# ifconfig
eno1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.0.0.126  netmask 255.255.255.0  broadcast 10.0.0.255
        inet6 fe80::362e:7d83:2ce8:ac77  prefixlen 64  scopeid 0x20<link>
        ether 2c:41:38:61:86:e7  txqueuelen 1000  (Ethernet)
        RX packets 289261  bytes 107146400 (107.1 MB)
        RX errors 0  dropped 12517  overruns 0  frame 0
        TX packets 101738  bytes 12010312 (12.0 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 17966  bytes 4419278 (4.4 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 17966  bytes 4419278 (4.4 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

wlo1: flags=4099<UP,BROADCAST,MULTICAST>  mtu 1500
        ether 40:25:c2:7c:cb:60  txqueuelen 1000  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

root@Jammy:/etc#
```

DHCP Security

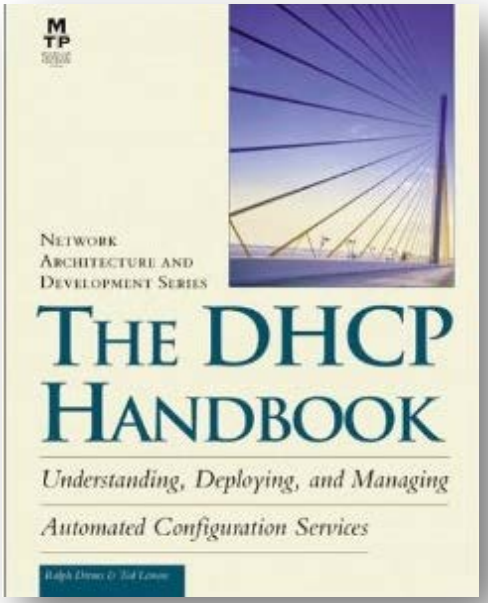
- The DHCP protocol does not include any mechanism for authentication
  - Unauthorized clients can gain access to resources
  - Unauthorized (Rogue) DHCP servers can provide false information to clients
    - Man-In-The-Middle attacks
  - Malicious DHCP clients can launch resource exhaustion attacks

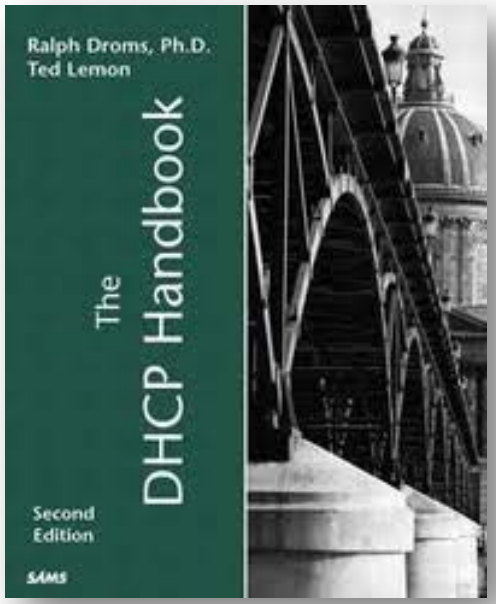
OS Fingerprinting via DHCP

- OS disclosed by IP TTL on DHCP Packets
  - Linux TTL 64
  - Windows TTL 128
  - OS X TTL 255
  - See www.fingerbank.org

Resources

- http://www.isc.org/software/dhcp
- The DHCP Handbook – 1st and 2nd Editions





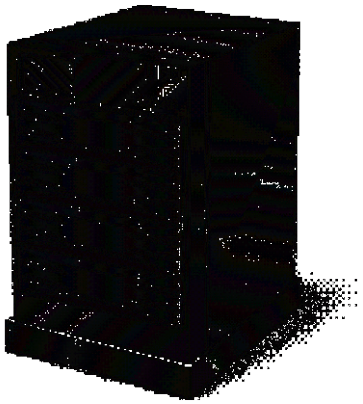
Failover

- Optional Discussion
- Redundancy, High Availability, Maintenance
- Primary - Secondary pairs
- Experimental in ISC BIND
- Use similar hardware, OS version, same DHCP
- Time sync is critical
- Address pool is split and balanced
- Watch the logs

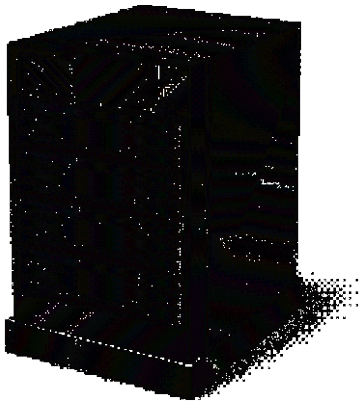
Nov 6 19:50:51 secondary dhcpd: failover peer dhcp-failover: I move from normal to communications-interrupted

Symmetrical Failover

A

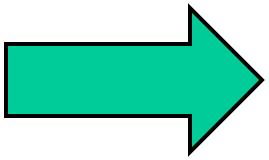


B



Main server for

Scope 1
Scope 2
Scope 3

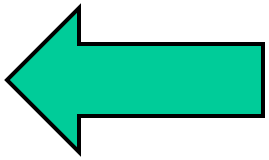


Backup server for

Scope 1
Scope 2
Scope 3

Backup server for

Scope 4
Scope 5
Scope 6

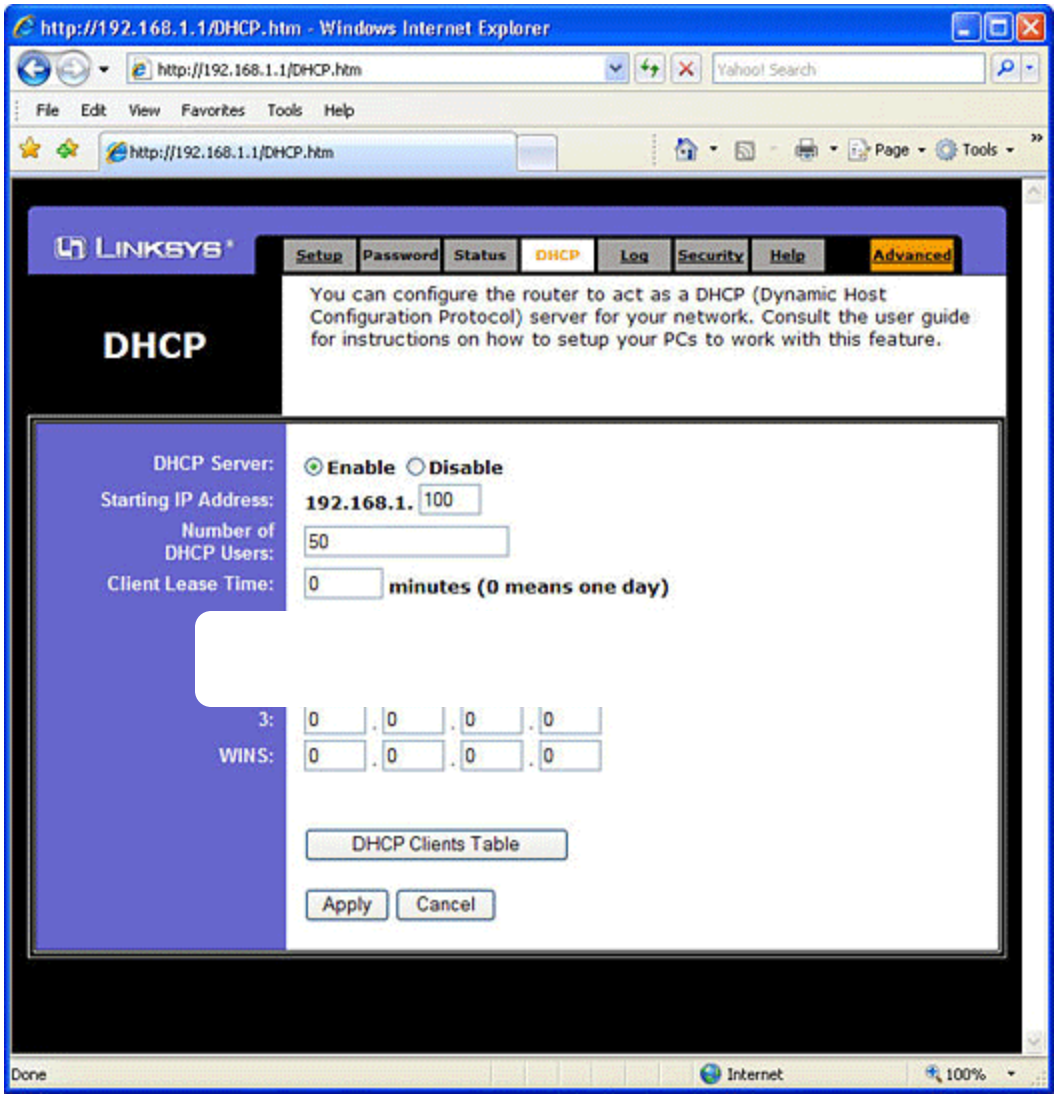


Main server for

Scope 4
Scope 5
Scope 6

SOHO DHCP Server

- Caveats?



Microsoft DHCP Exercise

- Install Wireshark - www.wireshark.org
- Start a packet capture
- Open a command prompt
  - Start menu or Run: cmd
- Renew your DHCP lease
  - Type ipconfig /release and press Enter
  - Type ipconfig /renew and press Enter
- Stop the packet capture
- Analyze the results

Remember

- The two basic mechanisms in DHCP are IP address allocation and configuration parameters delivery.
- Relay agents avoid the need for a DHCP/BOOTP server on each subnet (broadcast space).
- DHCP provides: IP address, lease time, routing (gateway) IP, subnet mask, DNS server(s) IP, optional parameters (cool stuff)
- DHCP Messages DORA: Discover, Offer, Request, Acknowledge (and Release, Decline, Nack)
- All interactions are initiated by a client
  - Server only replies
- Server listens on UDP port 67
- Client listens on UDP port: 68