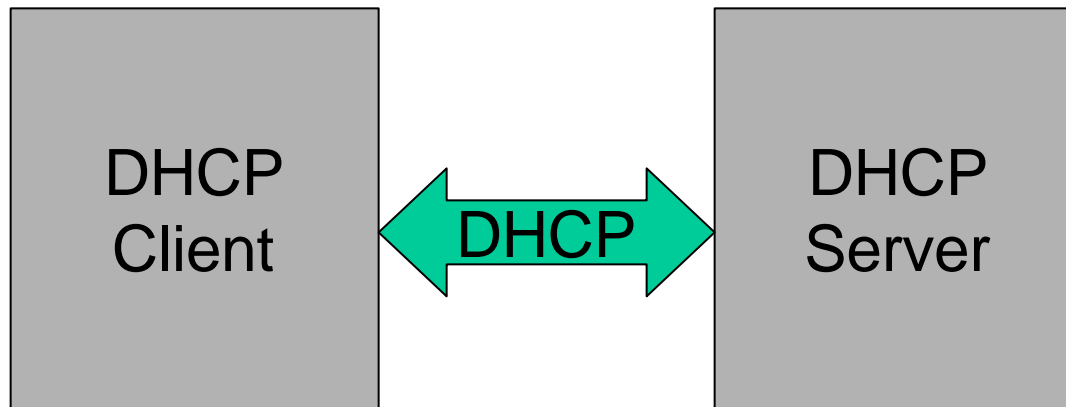


nyc**wireless**

A DHCP Primer

Dario Laverde,
dario@mediatracker.com

Dynamic Host Configuration Protocol



- Dynamic Host Configuration consists of at least an IP address in addition to a lease time, routing (gateway) ip, subnet mask, dns server(s) ip information and many optional parameters.

What is DHCP?

- The Dynamic Host Configuration Protocol (DHCP) provides configuration parameters to Internet hosts.
- DHCP consists of two components:
 - A protocol for delivering host-specific configuration parameters to a host
 - A mechanism for allocation of network addresses to hosts

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*) addresses 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* (**the predecessor of DHCP**) is 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

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

TCP/IP Layers

- Physical
 - Frame (mac address)
- Data Link
 - ARP
- Internet
 - IP datagram [subnet # | Host ID]
- Transport
 - UDP
 - TCP
- Application
 - DHCP

DHCP Terminology

- **DHCP Server**
 - Host that provides and manages the configuration parameters for many “clients” hosts using UDP Transport (port 67)
- **DHCP Client**
 - Host that requests configuration parameters from a DHCP Server, also known as a DHCP Daemon (DHCPD). It also uses the UDP transport (port 68)
- **BOOTP relay agent**
 - A host or router that passes DHCP messages between DHCP clients and DHCP servers
- **Binding**
 - A binding is a collection of configuration parameters, including at least an IP address, associated with or "bound to" a DHCP client

DHCP Message Format

op (1)	htype (1)	hlen (1)	hops (1)
xid (4)			
secs (2)		flags (2)	
ciaddr (4)			
yiaddr (4)			
siaddr (4)			
giaddr (4)			
chaddr (16)			
sname (64)			
file (128)			
options (312)			

The DHCP Message Fields

- **op** Message op code / message type.
1 = BOOTREQUEST, 2 = BOOTREPLY
- **htype** Hardware address type
- **hlen** Hardware address length
- **hops** Client sets to zero, optionally used by relay agents.
- **xid** Transaction ID, a random number chosen by the client, used to associate messages and responses between a client and a server.
- **secs** Filled in by client, seconds elapsed since client began the address acquisition or renewal process.
- **flags** Flags used by server and/or client

The DHCP Message Fields (cont.)

- ciaddr Client IP address; filled if client in BOUND, RENEW or REBINDING state and can respond to ARP requests.
- yiaddr 'your' (client) IP address.
- siaddr IP address of next server to use in bootstrap; returned in DHCPOFFER, DHCPACK by server.
- giaddr Relay agent IP addr when booting via a relay agent.
- chaddr Client hardware address.
- sname Optional server host name, null terminated string.
- file Boot file name, null terminated string; "generic" name or null in DHCPDISCOVER, fully qualified directory-path name in DHCPOFFER.
- options List of options (option 255 terminates list)
Format of each : option code, length, data

DHCP Options

- DHCP Options are defined in RFC 2132
- One such 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

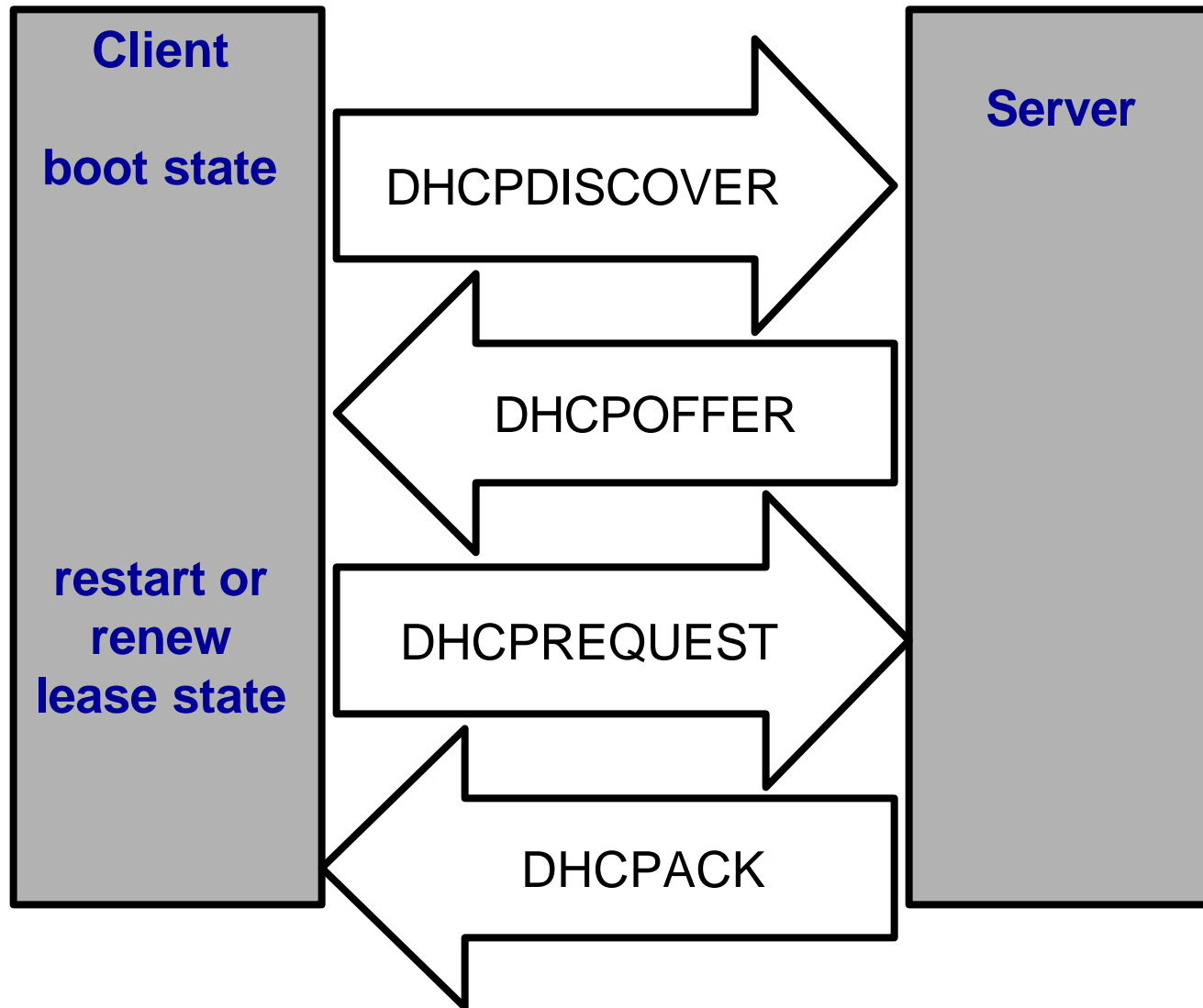
Sample Client Broadcast:

```
Frame: dst: ff:ff:ff:ff:ff:ff
      src: cc:11:ii:ee:nn:tt
IP:   dst: 255.255.255.255
      src: 0.0.0.0
UDP:  dst: 67
      src: 68
DHCP: chaddr: cc:11: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)
```

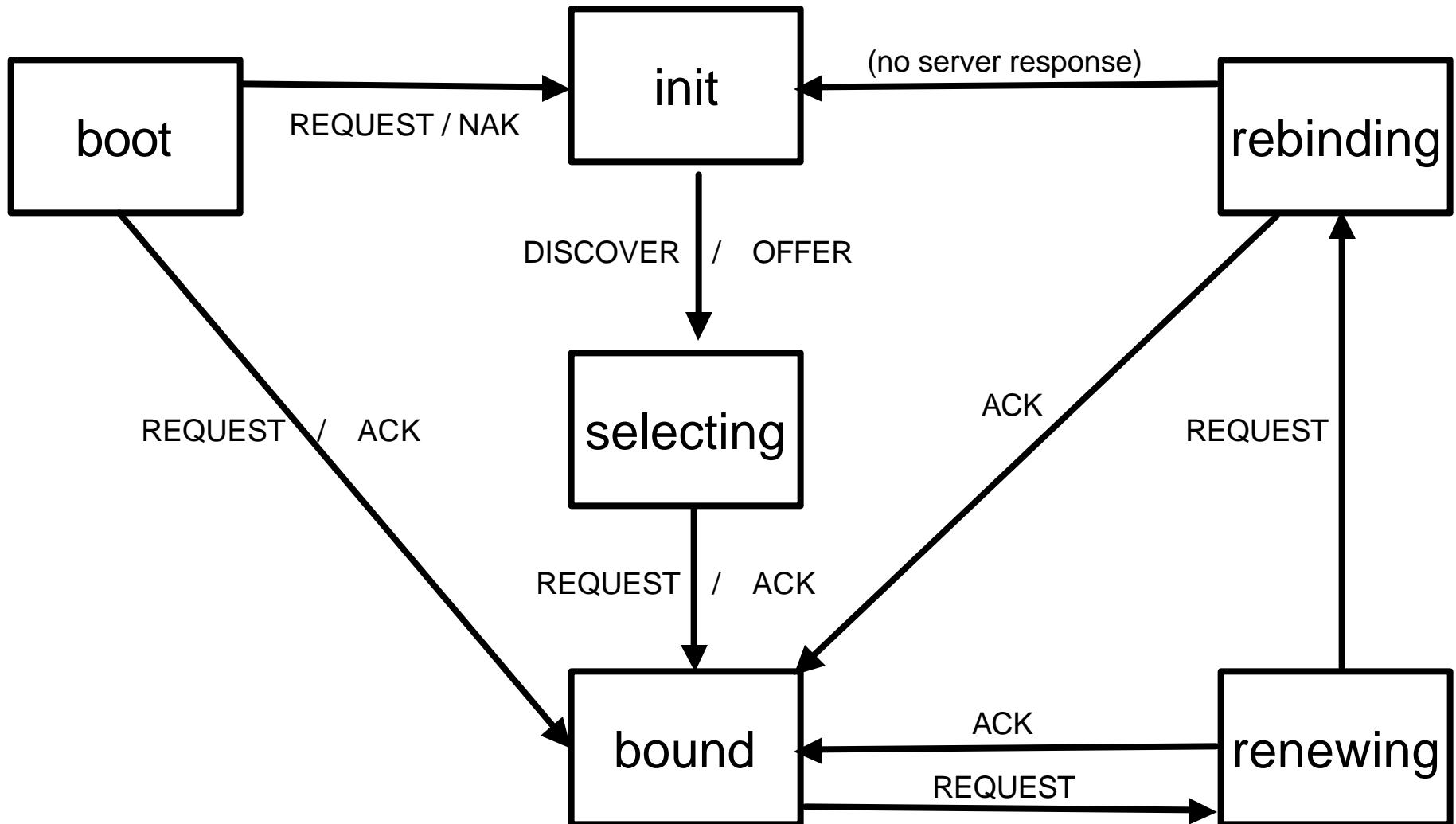
Sample Server Response:

```
Frame: dst: cc:11: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:11: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)
```

Initial State Diagram



DHCP Client States



DHCP Server Strategy

- IP Address Allocation
 - A new request for an IP address is taken from a pool of IP addresses or a prearranged static assignment.
 - IP Address is checked to see if not in use.
 - If in use it is marked as abandoned and reused when the address pool is depleted. Abandoned addresses can be periodically cleaned up.
 - If not in use, the requested IP is either accepted (ACK) or not (NAK) or the message may be ignored.
- Lease Management
 - The server maintains a persistent database of leases
 - A lease is not confirmed until it is written to the database.

Firewall Issues

- On some systems with a packet filter, if a firewall is set to block UDP port 67 and 68 entirely, broadcast packets sent through the packet filter will not be blocked resulting in a strange behavior with DHCP clients.
 - The initial packet exchange is broadcast, but renewals are unicast. The client will appear to be unable to renew until it starts broadcasting its renewals, and then suddenly it'll work.

Firewall Solution

- Firewall rules **_must_** allow packets from IP address 0.0.0.0 to IP address 255.255.255.255 from UDP port 68 to UDP port 67 through.
- They must also allow packets from your local firewall's IP address and UDP port 67 through to any address your DHCP server might serve on UDP port 68.
- Finally, packets from relay agents on port 67 to the DHCP server on port 67, and vice versa, must be permitted.

Debugging DHCP with a Network Analyzer:

The screenshot shows the Wireshark interface with a capture of network traffic. The packet list pane at the top shows several packets, with packet 109 highlighted in blue. This packet is a BOOTP Boot Request from 0. The packet details pane below shows the structure of the DHCP message, including the magic cookie, message type (DHCP Inform), client identifier, host name ('nightowl'), and a list of requested parameters (Subnet Mask, Domain Name, Router, Domain Name Server, NetBIOS over TCP/IP Name Server, NetBIOS over TCP/IP Node Type, NetBIOS over TCP/IP Scope, Vendor-specific Information, and User Class Information). The packet bytes pane at the bottom shows the raw hex and ASCII data of the packet.

No. .	Time	Source	Destination	Protocol	Info
104	113.964432	NIGHTOWL	192.168.0.255	BROWSER	Local Master Announ
105	114.863914	NIGHTOWL	ff:ff:ff:ff:ff:ff	ARP	who has 192.168.0.1
106	117284.090730	localhost	NIGHTOWL	ARP	192.168.0.1 is at 0
107	117284.090758	NIGHTOWL	localhost	BOOTP	Boot Request from 0
108	116.028631	localhost	255.255.255.255	BOOTP	Boot Request from 0
109	116.364533	NIGHTOWL	localhost	BOOTP	Boot Request from 0
110	121.871506	NIGHTOWL	localhost	DNS	Standard query A wp
111	123.376267	NIGHTOWL	localhost	DNS	Standard query A wp

```

Magic cookie: (OK)
Option 53: DHCP Message Type = DHCP Inform
Option 61: Client identifier
Option 12: Host Name = "nightowl"
Option 55: Parameter Request List
  1 = Subnet Mask
  15 = Domain Name
  3 = Router
  6 = Domain Name Server
  44 = NetBIOS over TCP/IP Name Server
  46 = NetBIOS over TCP/IP Node Type
  47 = NetBIOS over TCP/IP Scope
  43 = Vendor-specific Information
  77 = User Class Information
Unknown option code: 252
End option
  
```

0000	00 a0 cc 63 fa 6e 00 d0	59 08 07 e3 08 00 45 00	...c.n.. Y.....E.
0010	01 48 00 6f 00 00 80 11	b7 e2 c0 a8 00 02 c0 a8	.H.o....
0020	00 01 00 44 00 43 01 34	64 81 01 01 06 00 23 48	...D.C.4 d.....#H
0030	29 00 01 00 00 00 c0 a8	00 02 00 00 00 00 00 00).....
0040	00 00 00 00 00 00 00 d0	59 08 07 e3 00 00 00 00 Y.....

Filter: Reset Apply File: <capture> Drops: 0

Current and Future Developments

- Procedure for defining new DHCP Options: RFC 2489
- *A new DHCP Option (option code 252):*
 - *WPAD (Web Proxy Automatic Discovery)*
This feature is already implemented in Internet Explorer and allows for automatic setting of web proxy information.
- Proposal for a DHCP server to server protocol (DHCP failover protocol)

For More Information

Links:

- <http://www.dhcp.org>
- <http://www.ietf.org/html.charters/dhc-charter.html>
- <http://www.ics.org/dhcp.html>

Book:

The DHCP Handbook

by Ralph Droms and Ted Lemon

MacMillan Technical Publications