Systems and Network Management

DHCP and tcpdump

1 Background

The format of DHCP packets was established with RFC 951 for the *bootstrap protocol*, or *bootp*. DHCP was made to be backwardly compatible with the bootp protocol so that the infrastructure of bootp relay agents on routers would not need to be replaced. The DHCP extensions to bootp are bootp *options*. Table 1 on the following page shows the names of the fields in the fixed-format part of a DHCP message.

2 tcpdump and DHCP

The manual page for thge current version of **tcpdump** (version 3.7.1; an RPM is available from our server) unfortunately does not explain the detail of all the fields in the DHCP protocol. To understand them all, it is necessary to look at the source. Here is my summary after reading ~/RPM/BUILD/tcpdump-3.7.1/tcpdump-3.7.1/print-bootp.c.

Field	Description
op	Message operation code: 1 in message from client, 2 in message from server
htype	Link-layer address type from RFC 1700. For Ethernet, htype is 1.
hlen	Link-layer address length, in bytes. (number of bytes in chaddr field)
hops	Number of relay agents that have forwarded this message.
xid	*Transaction identifier*; used by clients to match responses from servers with previously transmitted requests.
secs	Number of seconds since client began DHCP transaction
flags	Least significant bit is set to 1 to indicate messages to client must be broadcast
ciaddr	Client's IP address, set by client after reaches BOUND state (i.e., address is valid)
yiaddr	Client's IP address, set by server to inform client of its address ("your" IP addresss)
siaddr	IP address of the next server for the client to use (i.e., for the client to download an operating system kernel using tftp)
giaddr	Relay agent (or "gateway") IP address: relay agent fills this in with the address of the interface through which it received the DHCP message
chaddr	Client's link layer address (i.e., on our LAN, the Ethernet address)
sname	Name of the next server for client to use in the configuration process
file	filename the client should request from the next server (i.e., an operating system kernel, or kickstart file)

Table 1: DHCP Message fields

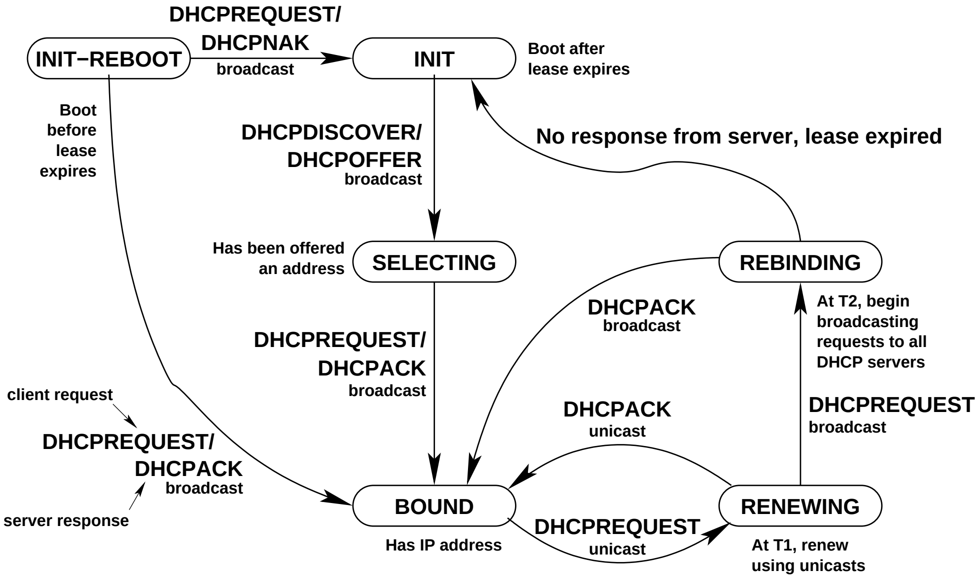

Figure 1: A state diagram showing states of a DHCP client. Note that T is the lease time, $T1 = \frac{T}{2}$, $T2 = \frac{7T}{8}$. See also table 3 on page 5 from the DHCP RFC 2131 (available in full at `/home/nfs/ietf/rcf/rfc2131.txt`), which sumarises DHCP messages.

Field	printf() format in tcpdump	short desc.
htype	" htype-#%d"	length of link-layer address
hops	" hops:%d"	number of relay agents
xid	" xid:0x%x"	transaction ID
secs	" secs:%d"	seconds since sesssion started
flags	" flags:0x%x"	LSb is broadcast flag
ciaddr	" C:%s"	Client's ip address
yiaddr	" Y:%s"	'your' ip address (bootp client)
siaddr	" S:%s"	Server's ip address
giaddr	" G:%s"	Gateway's ip address
chaddr	" ether %s"	Ethernet address
sname	sname "⟨*servername*⟩"	name of next server
file	file "⟨*filename*⟩"	file name to download
	SM	Subnet mask
	DG	Default gateway
	TS	Time server
	NS	Name servers
	HN	Host name
	DN	Domain name

Table 2: How tcpdump represents various DHCP fields.

Message		Use
DHCPDISCOVER	—	Client broadcast to locate available servers.
DHCPOFFER	—	Server to client in response to DHCPDISCOVER with offer of configuration parameters.
DHCPREQUEST	—	Client message to servers either (a) requesting offered parameters from one server and implicitly declining offers from all others, (b) confirming correctness of previously allocated address after, e.g., system reboot, or (c) extending the lease on a particular network address.
DHCPACK	—	Server to client 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
DHCPDECLINE	—	Client to server indicating network address is already in use.
DHCPRELEASE	—	Client to server relinquishing network address and cancelling remaining lease.
DHCPINFORM	—	Client to server, asking only for local configuration parameters; client already has externally configured network address.

Table 3: DHCP Messages: this is "table 2" from RFC 2131; the RFC is available in full from `ictlab` at `/home/nfs/ietf/rcf/rfc2131.txt`.