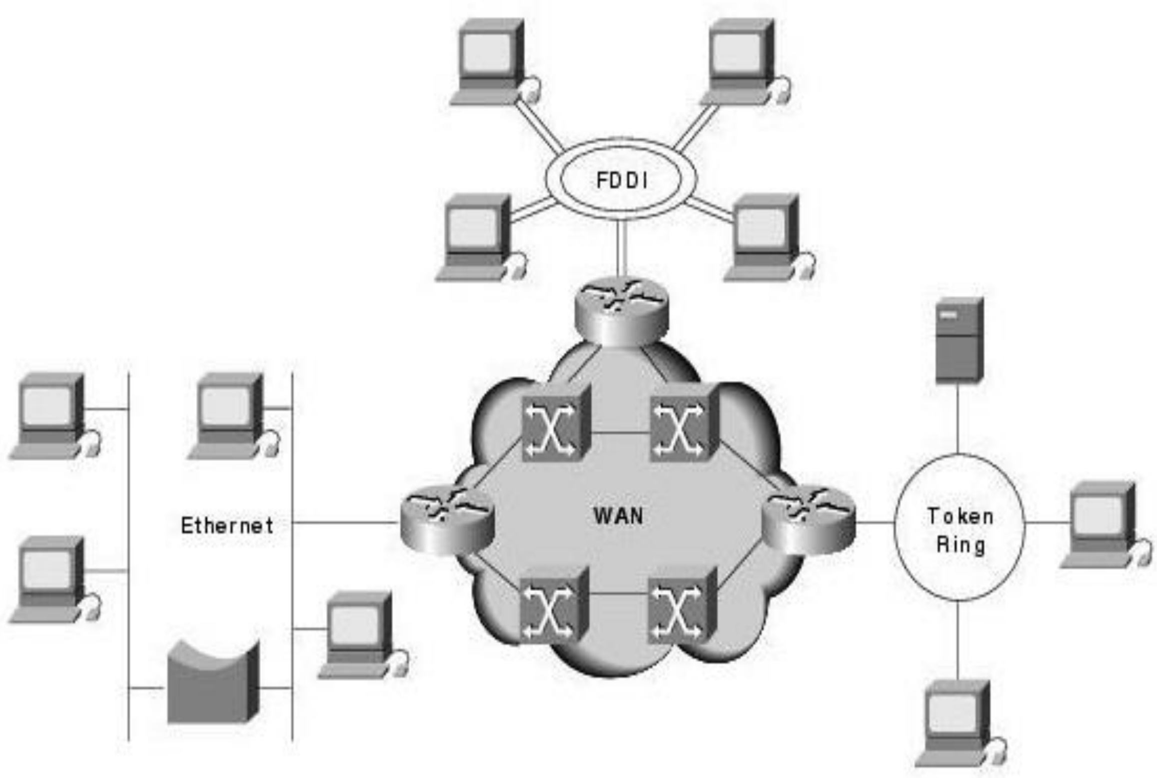
Basic Internetworking (IP, CIDR, ARP, BOOTP DHCP, ICMP)

Internetworking is a collection of individual networks, connected by intermediate networking devices, that functions as a single large network. It refers to the industry, products, and procedures that meet the challenge of creating and administering internetworks.



Internetworking is the practice of interconnecting multiple computer networks, such that any pair of hosts in the connected networks can exchange messages irrespective of their hardware-level networking technology.

Challenges faced by internetworking are:

- Connectivity
- Reliability
- Network Management
- Flexibility

Protocols present in Internetworking:

- **DHCP(Dynamic Host Configuration Protocol)**

Dynamic Host Configuration Protocol (DHCP) is a standardized network protocol used on Internet Protocol (IP) networks.The DHCP is controlled by a DHCP server that dynamically distributes network configuration parameters for interfaces and services. Networks ranging in size from small home networks to campus networks frequently use DHCP.

Working of DHCP:

A DHCP server dynamically assigns an IP address and other network configuration parameters to each device on a network so they can communicate with other IP networks. DHCP is an enhancement of an older protocol called BOOTP.

With respect to the DHCP protocol, the DHCP server goes through an initializing, selecting, requesting, binding, renewal, rebinding, and expiration cycle when negotiating for an IP address, as shown in the below diagram. The process is basically as follows:

1. The client just added or relocated on the network requests an IP address by broadcasting a DHCPDISCOVER message to the local subnet over the well-known BOOTP server port. (The client can also go through a BOOTP router or relay agent to forward the DHCPDISCOVER to additional remote DHCP servers.) This is the *initializing* state.

2. The participating DHCP servers respond with a DHCPOFFER message if they have a valid configuration for the client. The client may get many of these messages, which contain the IP address and configuration data. (The servers make sure to reserve the addresses so as not to accidentally offer them to another client.) At this point the client enters the *selecting* state.

3. After selecting an address, the client broadcasts the selected address and name of the "winning" server (Server 1) using a DHCPREQUEST message. This is the *requesting* state. All the other servers can now safely unreserve their addresses.

4. Server 1 sends the client a DHCPACK (acknowledgment) message with the negotiated IP address, the lease, and the network configuration parameters. The client now enters the *binding* state and can fully use the assigned IP address.

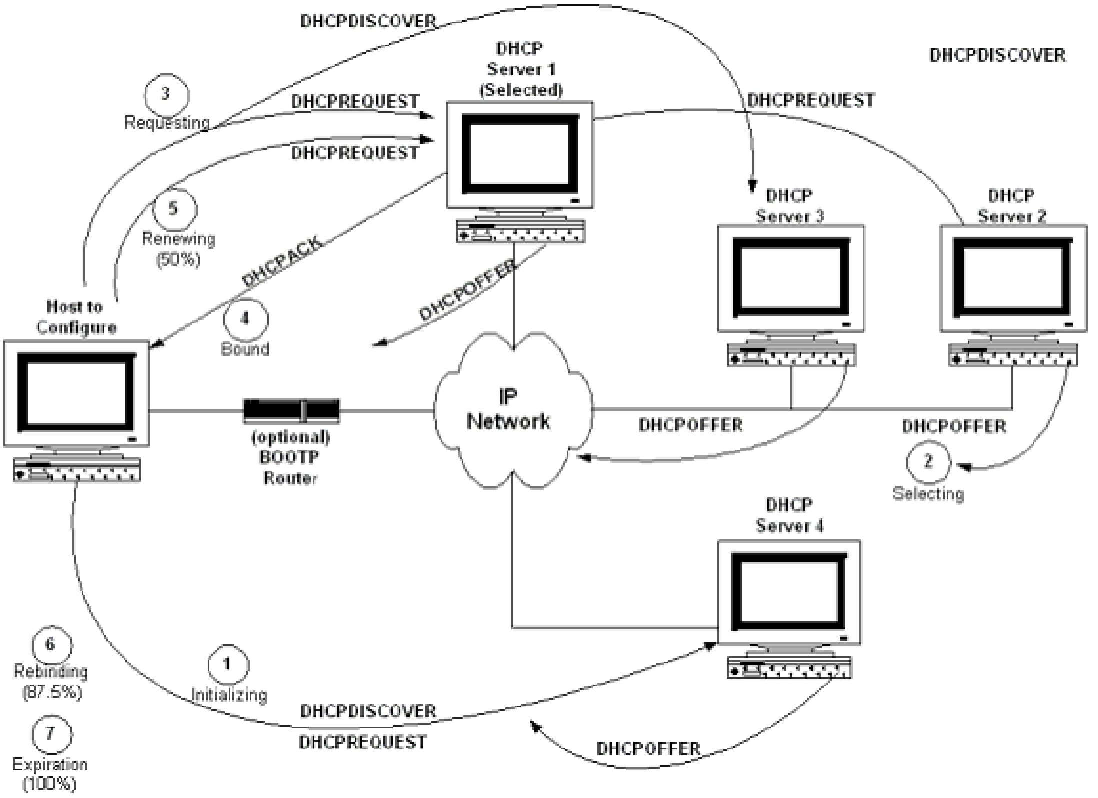
5. About halfway through the lease, the client sends Server 1 another DHCPREQUEST for a lease renewal and enters the *renewal* state. If the server deems the lease renewable, it sends back another DHCPACK to update the lease (including any new parameters). The client now returns to the *binding* state, as in Step 4.

6. If the client cannot renew the lease (such as if Server 1 is down), the client waits until about 87.5% of the way through the lease and broadcasts another DHCPREQUEST to all DHCP servers. Any server can now return a DHCPACK containing the extended lease and updated parameters. This is the *rebinding* state.

7. When the lease reaches 100% expired, or a server sends back a DHCPNAK negative acknowledgment message, the client must give up the IP address. It then returns to the *initializing* state and must start the address negotiation over again.

DHCP is defined in RFC 2131 and RFC 2132. Refer to them for more information.

Two DHCP servers are recommended for a network. The benefit of having more than one server is if one fails another is available to continue processing requests, ensuring that all hosts (old and new) are serviced continuously.



- **ICMP(Internet Control Message Protocol)**

The Internet Control Message Protocol (ICMP) is a protocol that devices within a network use to communicate problems with data transmission. In this ICMP definition, one of the primary ways in which ICMP is used is to determine if data is getting to its destination and at the right time. This makes ICMP an important aspect of the error reporting process and testing to see how well a network is transmitting data.

Working of ICMP:

ICMP will take source IP from the discarded packet and inform the source by sending a source quench message.

Then the source will reduce the speed of transmission so that the router will free itself from congestion.

Since IP does not have an inbuilt mechanism for sending error and control messages. It depends on Internet Control Message Protocol(ICMP) to provide an error control. It is used for reporting errors and management queries. It is a supporting protocol and is used by networks devices like routers for sending error messages and operations information., e.g. the requested service is not available or that a host or router could not be reached.

ICMPv4 Packet Format :

Type(8 bit)	Code(8 bit)	CheckSum(16 bit)
Extended Header(32 bit)		
Data/Payload(Variable Length)		

BOOTP: Bootstrap Protocol

Knowledge of its IP address, can determine its IP address using RARP when it is bootstrapped. There are two problems with RARP: (1) the only thing returned is the IP address, and (2) since RARP uses a link-layer broadcast, RARP requests are not forwarded by routers (necessitating an RARP server on every physical network). This chapter describes an alternative method for a diskless system to bootstrap itself, called the Bootstrap Protocol, or BOOTP.

BOOTP Packet Format

BOOTP requests and replies are encapsulated in UDP datagrams, as shown in Figure 16.1.

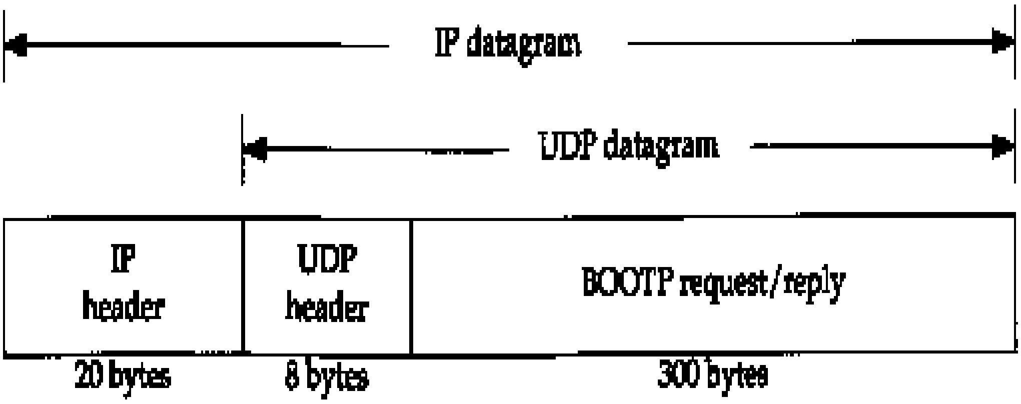


Figure 16.1 Encapsulation of BOOTP requests and replies within a UDP datagram.

Format of the 300-byte BOOTP request and reply.

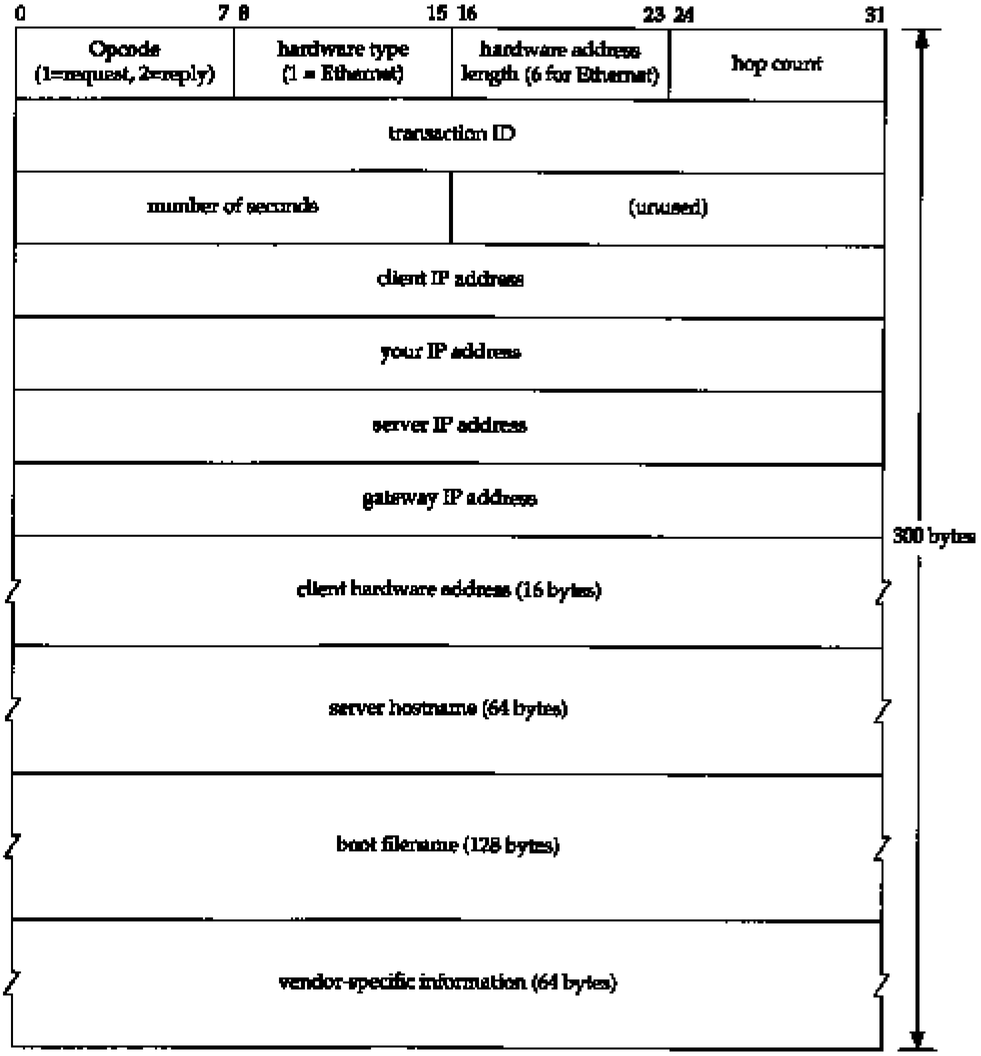

0
7 8
15 16
23 24
31
Opcode (1=request, 2=reply)
hardware type (1 = Ethernet)
hardware address length (6 for Ethernet)
hop count
transaction ID
number of seconds
(unused)
client IP address
your IP address
server IP address
gateway IP address
client hardware address (16 bytes)
server hostname (64 bytes)
boot filename (128 bytes)
vendor-specific information (64 bytes)
300 bytes

Figure 16.2 Format of BOOTP request and reply.