18CSC302J- Computer Networks

Unit-3

Syllabus

1. DNS- DNS in the Internet, DNS Resolution, DNS Messages
2. TELNET – SSH
3. FTP- TFTP
4. WWW Architecture, Documents
5. HTTP, HTTP Request and Reply,
6. **DHCP Operation, DHCP Configuration**
7. SMTP, POP3, IMAP, MIME

Learning Resources

1. Douglas E. Comer, Internetworking with TCP/IP, Principles, protocols, and architecture,Vol 1 5th Edition,2006 ISBN: 0131876716, ISBN: 978-0131876712

Host Configuration: DHCP

Why DHCP

- It is a first client/server application program, Dynamic Host Configuration Protocol (DHCP).
- This application is discussed first because it is the first client/server application program that is used after a host is booted.
- In other words, it serves as a bootstrap when a host is booted and supposed to be connected to the Internet, but the host does not know its IP address.
- Every computer that utilizes TCP/IP protocol should know its IP address.

Introduction

- Each computer that uses the TCP/IP protocol suite needs to know its IP address.
- If the computer uses classless addressing or member of a subnet, it also needs to know its subnet mask.
- Most computers today need two other pieces of information: the address of a default router to be able to communicate with other networks and the address of a name server to be able to use names instead of addresses
- **In other words, four pieces of information are normally needed:**

1. The IP address of the computer
2. The subnet mask of the computer
3. The IP address of a router
4. The IP address of a name server

Introduction

- These four pieces of information can be stored in a configuration file and accessed by the computer during the bootstrap process.
- But what about a diskless workstation or a computer with a disk that is booted for the first time?
- In the case of a diskless computer, the OS and the networking software could be stored in read-only memory (ROM).
- However, the above information is not known to the manufacturer and thus cannot be stored in ROM.
- The information is dependent on the individual configuration of the machine and defines the network to which the machine is connected.

Previous Protocols

- Before DHCP became the formal protocol for host configuration, some other protocols were used for this propose.

a) Reverse Address Resolution Protocol (RARP)

- At the beginning of the Internet era, a protocol called RARP was designed to provide the IP address for a booted computer.
- RARP was actually a version of ARP; ARP maps an IP address to a physical address: RARP maps a physical address to an IP address.
- However, RARP is deprecated today for two reasons.
- First, RARP used the broadcast service of the data link layer, which means that a RARP server must be present in each network.
- Second, RARP can provide only the IP address of the computer, but a computer today needs all four pieces of information mentioned above.

Previous Protocols

b) Bootstrap Protocol (BOOTP)

- The BOOTP is the prerunner of DHCP.
- It is a client/server protocol designed to overcome the two deficiencies of the RARP protocol.
- First, since it is a client/server program, the BOOTP server can be anywhere in the Internet.
- Second, it can provide all pieces of information we mentioned above, including the IP address.
- To provide the four pieces of information described above, it removes all restriction about the RARP protocol.
- BOOTP, however, is a static configuration protocol.
- When a client requests its IP address, the BOOTP server consults a table that matches the physical address of the client with its IP address.
- This implies that the binding between the physical address and the IP address of the client already exists.

Previous Protocols

Bootstrap Protocol (BOOTP)

- There are some situations in which we need a dynamic configuration protocol.
- For example, when a host moves from one physical network to another, its physical address changes.
- As another example, there are occasions when a host wants a temporary IP address to be used for a period of time.
- BOOTP cannot handle these situations because the binding between the physical and IP addresses is static and fixed in a table until changed by the administrator.
- For Solving these problems, DHCP has been devised to handle these shortcomings.

DHCP (Definition)

- It is a Client/server protocol to provide the four required parameters to a diskless machine to enable the machine communicate with other networks
- DHCP is a successor to BOOTP and is backward compatible with it.
- Although BOOTP is considered deprecated, there may be some systems that may still use BOOTP for host configuration.

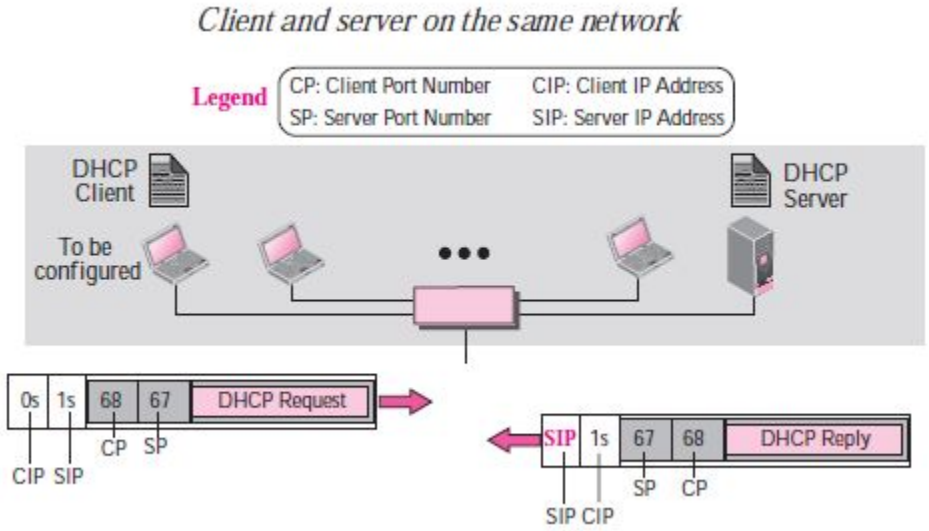
DHCP Operation

- The operation is initiated with a broadcasting request by the client depending upon the client and server's location, which could be any one of the following
- Same network - Client and server are present on the same network
- Different network - Client and server are present on different network

  A client can be in one network and the server in another, separated by several other networks.

Same Network with Operation

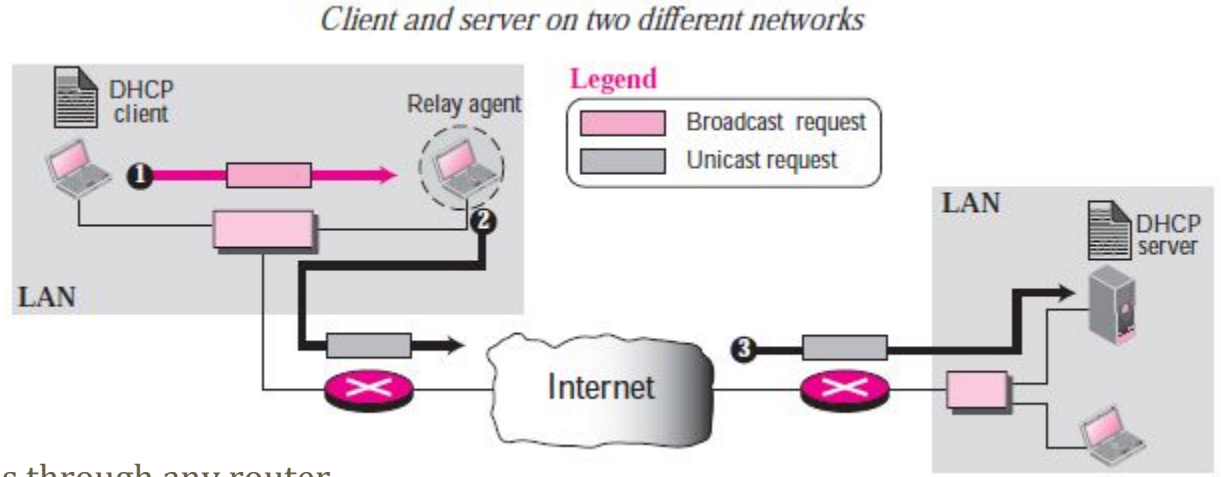
- A open command is provided by the server on UDP port number 67.
- Server waits for the client to respond
- The server gets the response from the booted client on port number 68
- A connection is now established between the source port 67 and destination port 68 by the server acknowledging with either a broadcast or unicast message.



- The response can be unicast because the server knows the IP address of the client.
- It also knows the physical address of the client, which means it does not need the services of ARP for logical to physical address mapping. However, some systems do not allow the bypassing of ARP, resulting in the use of the broadcast address.

Different network Operation

- There is one problem that must be solved.
- The DHCP request is broadcast because the client does not know the IP address of the server.

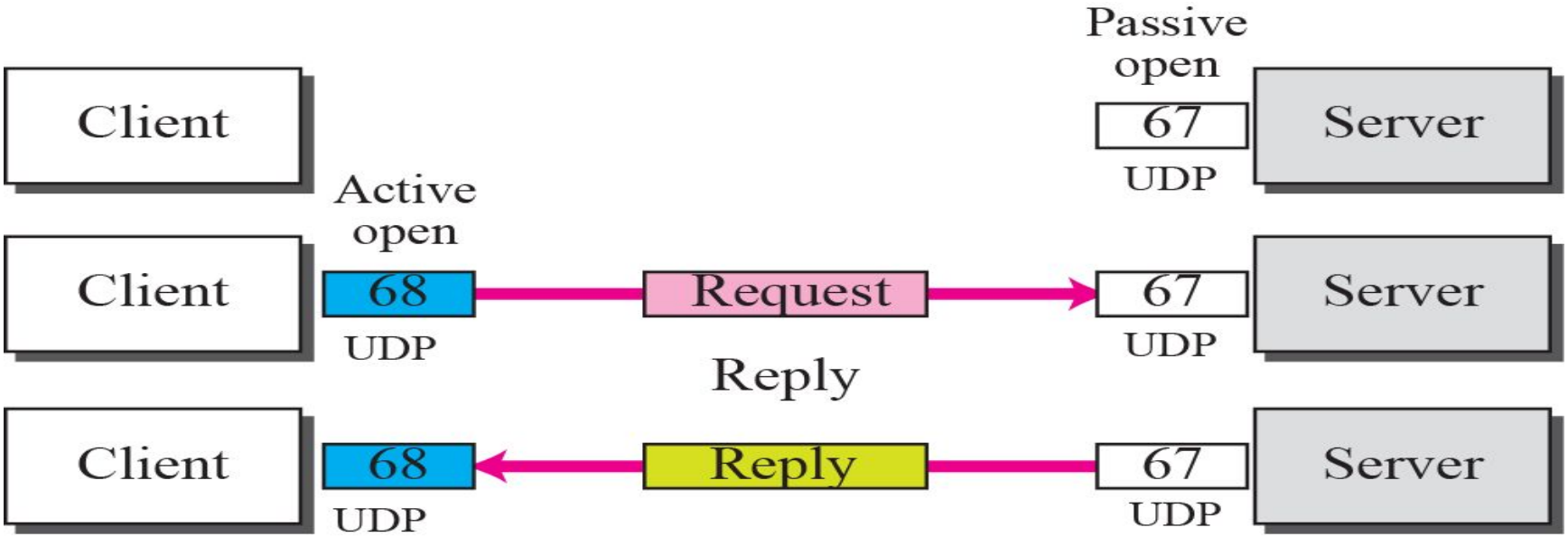


- A broadcast IP datagram cannot pass through any router.
- A router receiving such a packet discards it.
- Recall that an IP address of all 1s is a limited broadcast address.
- To solve the problem, there is a need for an intermediary.
- One of the hosts (or a router that can be configured to operate at the Application Layer) can be used as a

Different network Operation

- The host, in this case is called a relay agent.
- The relay agent knows the unicast address of a DHCP server and listens for broadcast messages on port 67.
- When it receives this type of packet, it encapsulates the message in a unicast datagram and sends the request to the DHCP server.
- The packet, carrying a unicast destination address, is routed by any router and reaches the DHCP server.
- The DHCP server knows the message comes from a relay agent because one of the fields in the request message defines the IP address of the relay agent.
- The relay agent, after receiving the reply, sends it to the DHCP client.

UDP ports


Passive
open
Client
67
Server
UDP
Active
open
Client
68
Request
67
Server
UDP
UDP
Reply
Client
68
Reply
67
Server
UDP
UDP

UDP Ports

- Port 67 - used by server (Common)
- Port 68 - used by client (to overcome the demultiplexing issue)
- Consider the below scenario
  - Host A uses DHCP client
  - Host B uses DAYTIME client
  - (both are in the same network and uses ephermal port 2017)
  - A broadcast message is sent from the server as an acknowledgement
  - This message contains the destination port 2017 and broadcast IP address FFFFFFFF16
  - Host A finds a message from application program on 2017
  - A correct message and incorrect message is delivered to DHCP and DAYTIME clients respectively
  - Transaction ID is also used to identify the clients which avoids the confusion created.

TFTP

- The server does not send all of the information that a client may need for booting.
- It is an acknowledgement from the server, In the reply message, the server defines the pathname of a file in which the client can find complete booting information.
- The client can then use a TFTP message which is encapsulated in a UDP user datagram, to obtain the rest of the needed information.

Error control

What if a request is lost or damaged? What if the response is damaged?

- There is a need for error control when using DHCP.
- DHCP uses UDP, which does not provide error control.
- Therefore, DHCP must provide error control.
- Error control is accomplished through two strategies:
  1. DHCP requires that UDP uses the **checksum**; the use of the checksum in UDP is optional.
  2. The DHCP client uses **timers** and a **retransmission policy** if it does not receive the DHCP reply to a request.
- To prevent a traffic jam when several hosts need to retransmit a request (for example, after a power failure), DHCP forces the client to use a random number to set its timers.

Packet Format

Operation code (8 bit) – Variant of DHCP

Hardware type (8 bit) - variant of physical network

Hardware length (8 bit) - length of PA in bytes

Hop count (8 bit) - Maximum number of hops

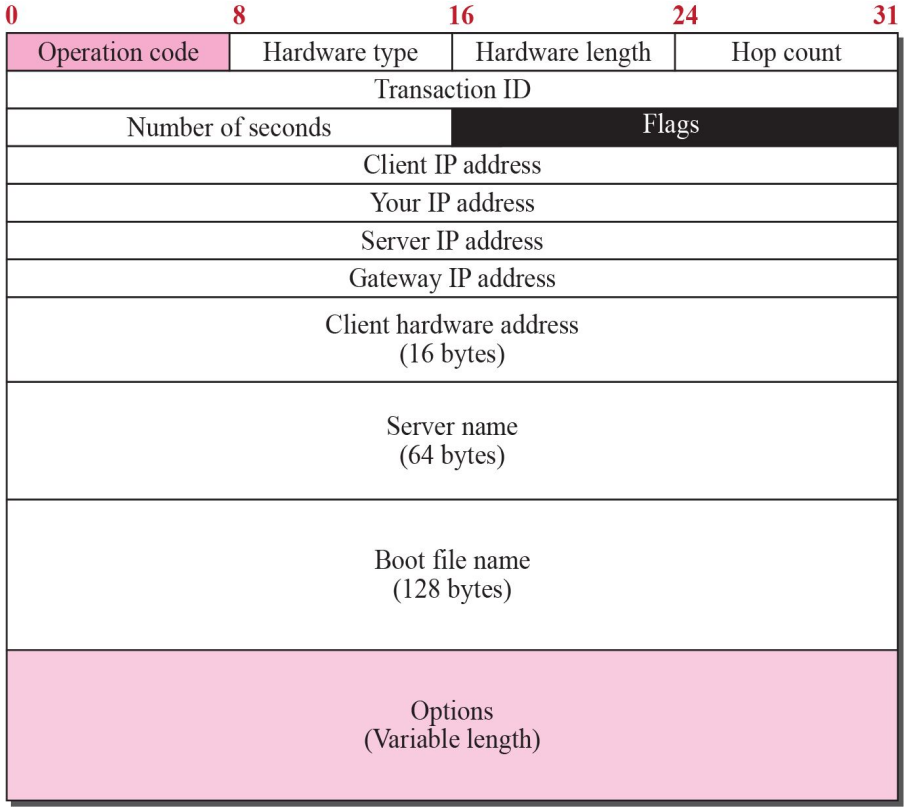
Transaction ID (4 byte)-To match a reply with the request

Number of seconds (16 bit) – Time elapsed to boot the client

Flag (16 bit)– left-most bit is used leaving the remaining bits to be zero.

Client IP address (4 byte) – holds client's IP address

Server IP address (4 byte) - holds server's IP address



Packet Format

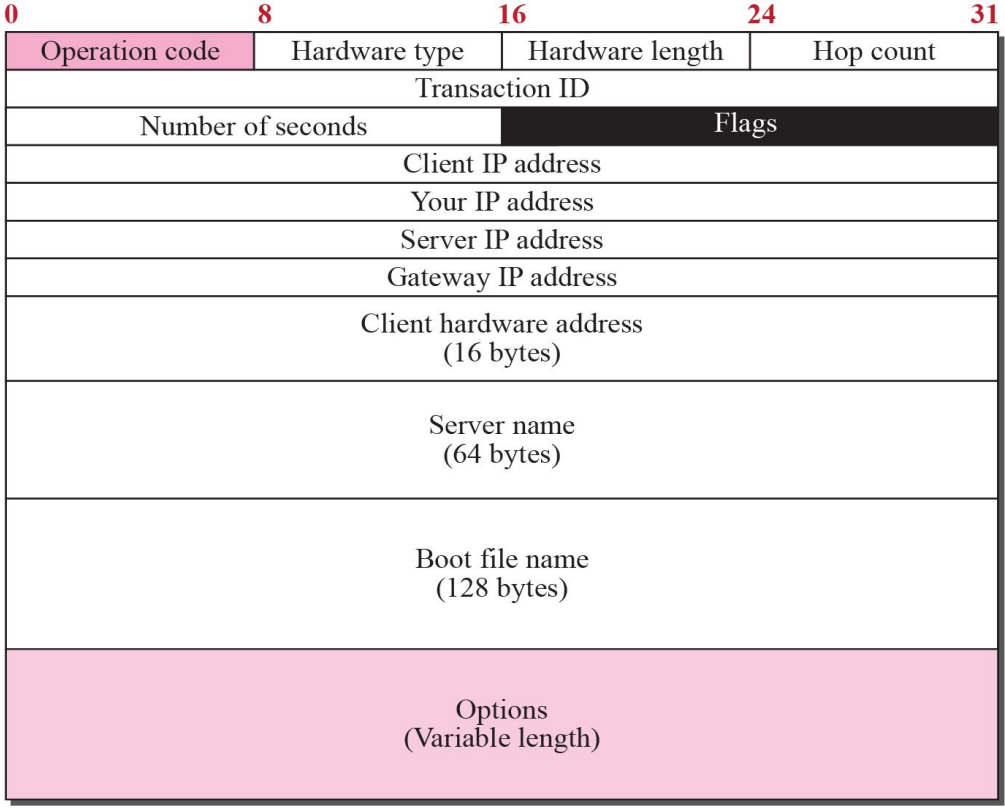
Gateway IP address (4 byte)– holds router's IP address

Client Hardware address– Client's physical address

Server name (64 byte)– holds server's domain name

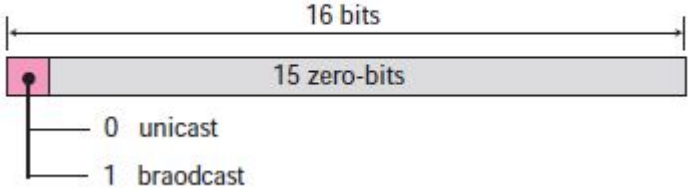
Boot file name (128 byte)– Holds path name

Options (64 byte)– carries either vendor information or other additional information.

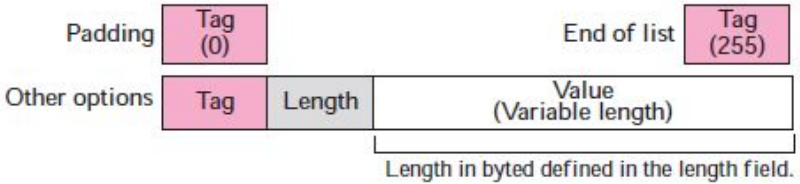


Packet Format

Flag format



Option format



Options for DHCP

Tag	*Length*	*Value*	*Description*
0			Padding
1	4	Subnet mask	Subnet mask
2	4	Time of the day	Time offset
3	Variable	IP addresses	Default router
4	Variable	IP addresses	Time server
5	Variable	IP addresses	IEN 16 server
6	Variable	IP addresses	DNS server
7	Variable	IP addresses	Log server
8	Variable	IP addresses	Quote server
9	Variable	IP addresses	Print server
10	Variable	IP addresses	Impress
11	Variable	IP addresses	RLP server
12	Variable	DNS name	Host name
13	2	Integer	Boot file size
53	1	Discussed later	Used for dynamic configuration
128–254	Variable	Specific information	Vendor specific
255			End of list

CONFIGURATION

Static address allocation

- The DHCP has been devised to provide static and dynamic address allocation.
- A DHCP server has a database that statically binds physical addresses to IP addresses.
- When working in this way, DHCP is backward compatible with the deprecated protocol BOOTP

Dynamic address allocation

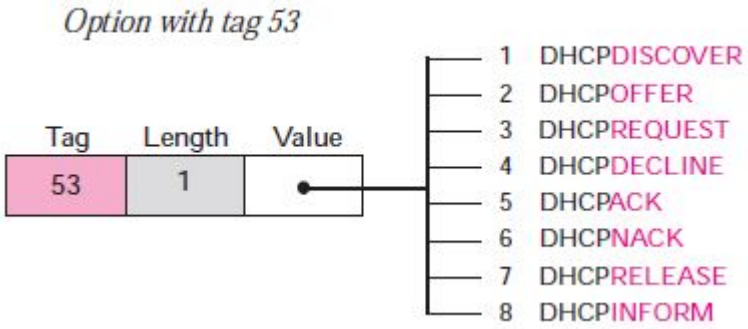
- DHCP has a second database with a pool of available IP addresses.
- This second database makes DHCP dynamic.
- When a DHCP client requests a temporary IP address, the DHCP server goes to the pool of available (unused) IP addresses and assigns an IP address for a negotiable period of time.
- When a DHCP client sends a request to a DHCP server, the server first checks its static database.
- If an entry with the requested physical address exists in the static database, the permanent IP address of the client is returned.
- On the other hand, if the entry does not exist in the static database, the server selects an IP address from the available pool, assigns the address to the client, and adds the entry to the dynamic database.

Dynamic address allocation

- The dynamic aspect of DHCP is needed when a host moves from network to network or is connected and disconnected from a network (for example, a subscriber to a service provider).
- DHCP provides temporary IP addresses for a limited period of time.
- **The addresses assigned from the pool are temporary addresses.**
- The **DHCP server issues a lease for a specific period of time**.
- When the lease expires, the client must either stop using the IP address or renew the lease.
- The server has the choice to agree or disagree with the renewal.
- If the server disagrees, the client stops using the address.

Transition states

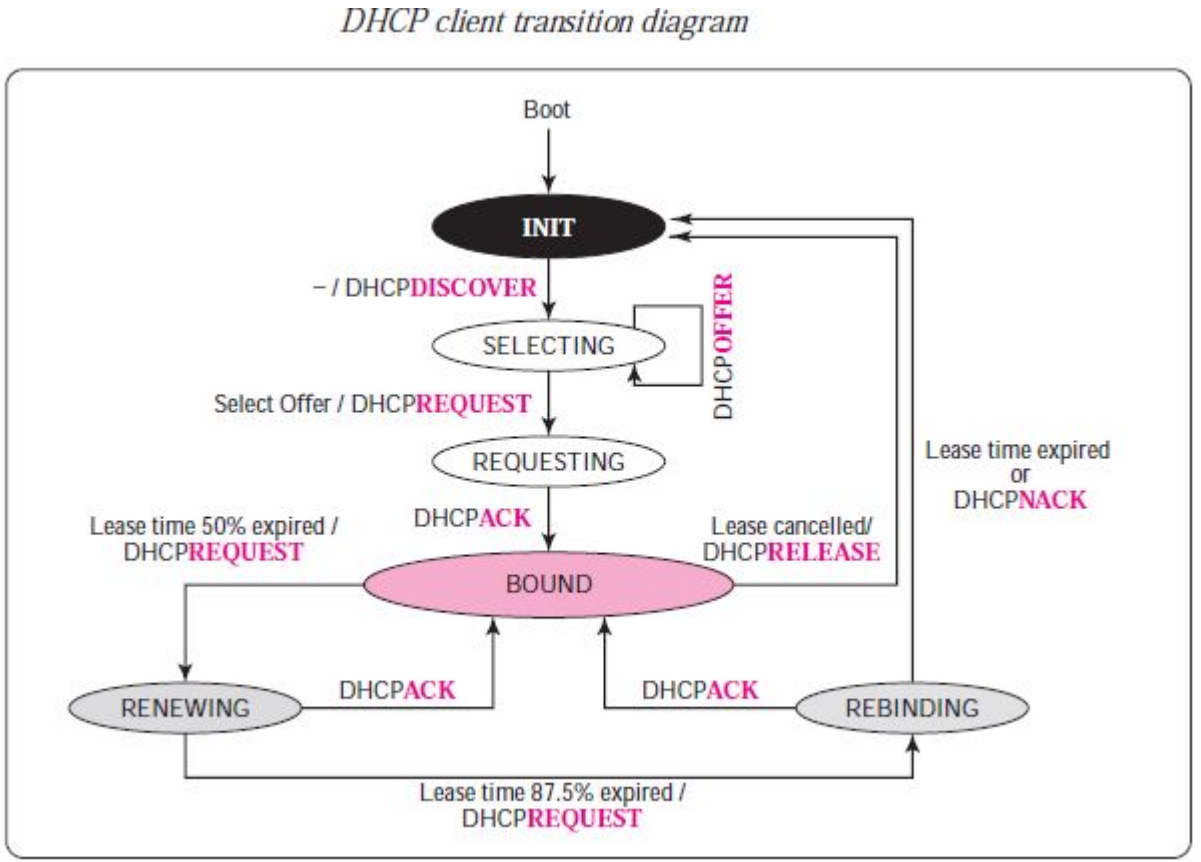
- To enable dynamic address allocation, the machine passes through several transitions
- The type of the transition is indicated tag 53.



States

- INIT state – Client initiates by sending DHCPDISCOVER message
- SELECTING STATE – SERVERS offers DHCPOFFER message. Client has to select one among the offers. Client sends DHCPREQUEST message to the selected server.
- REQUESTING STATE – Until the client receives DHCPACK message, it stays in the same state
- BOUND STATE – Client uses the IP address until the lease expires. DHCPREQUEST is again initiated by the client to renew the lease when 50% of the lease period is expired.
- RENEWING STATE – If DHCPACK is received, client gets back to BOUND state otherwise enters into the REBINDING state after 87.5% of time expires
- REBINDING STATE – The client does the following
    - DHCPNACK / lease expired – Client goes to the initializing state and gets new IP address.
    - DHCPACK – It goes to the bound state – resets timer.

States


DHCP client transition diagram
Boot
INIT
– / DHCPDISCOVER
SELECTING
DHCPOFFER
Select Offer / DHCPREQUEST
REQUESTING
Lease time expired
or
DHCPNACK
DHCPACK
Lease time 50% expired /
DHCPREQUEST
Lease cancelled/
DHCPRELEASE
BOUND
RENEWING
DHCPACK
DHCPACK
REBINDING
Lease time 87.5% expired /
DHCPREQUEST

Issues

- Issues related to the DHCP states.

Early Release

- A DHCP client that has been assigned an address for a period of time may release the address before the expiration time.
- The client may send a DHCPRELEASE message to tell the server that the address is no longer needed.
- This helps the server to assign the address to another client waiting for it.

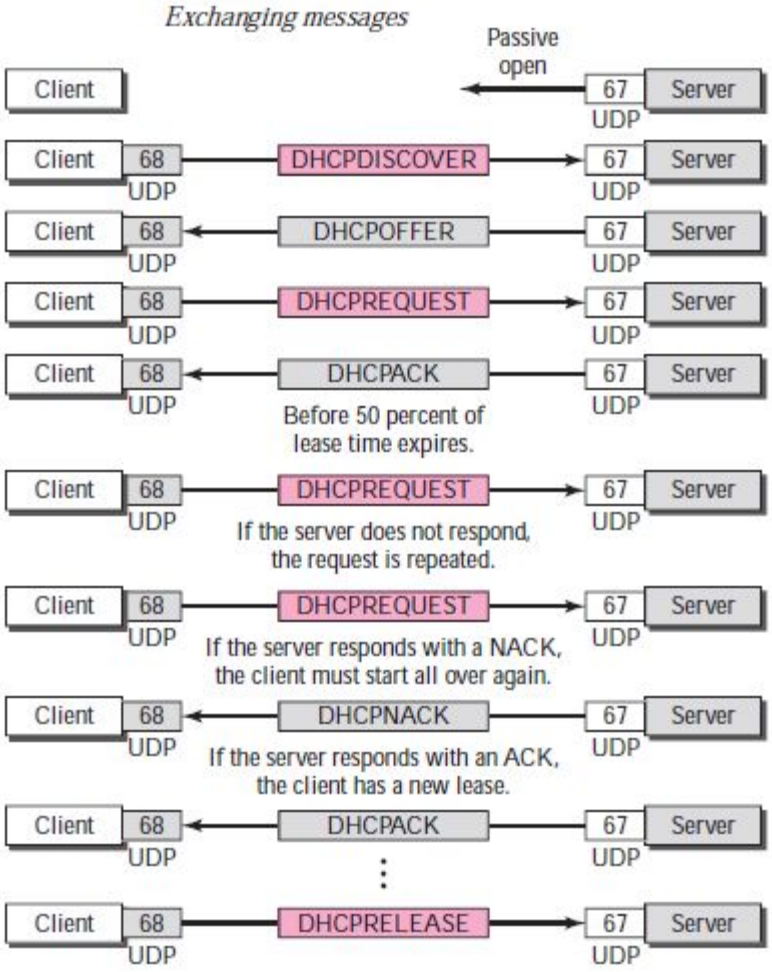
Timers

- The client uses three times: renewal timer, rebinding timer, and expiration timer.
- If the server does not specify the time-

Renewal timer:	→	50% of lease time
Rebinding timer:	→	87.5% of lease time
Expiration timer:	→	100% of lease time

ted, the client needs to use the default value.

Exchanging Messages



DHCP-SUMMARY

- Introduction
  - Previous protocols
    - RARP
    - BOOTP
  - DHCP
- DHCP Operation
  - Same Network
  - Different Networks
  - UDP Ports
  - Using TFTP
  - Error Control
  - Packet Format
- Configuration
  - Static Address Allocation
  - Dynamic Address Allocation
  - Transition States
  - Other Issues
    - Early Release
    - Timers
  - Exchanging Messages

References (finishing slides covering references for all the topics)

1. Douglas E. Comer, Internetworking with TCP/IP, Principles, protocols, and architecture,Vol 1 5th Edition,2006 ISBN: 0131876716, ISBN: 978-0131876712 **(Ref 2 in syllabus)**
2. https://slideplayer.com/slide/13911208/
3. http://www.csun.edu/~jeffw/Semesters/2006Fall/COMP429/Presentations/Ch25-FTP.pdf
4. https://study.com/academy/lesson/testing-an-ftp-connection.html
5. www.afternerd.com/blog/smtp