(DEEMED TO BE UNIVERSITY)

Complex

Experiential Learning (site visits)

Forum Theater

Jigsaw Discussion

Inquiry Learning

Role Playing

Active Review Sessions (Games or Simulations)

Interactive Lecture

Hands-on Technology

Case Studies

Brainstorming

Groups Evaluations

Peer Review

Informal Groups

Triad Groups

Large Group Discussion

Think-Pair-Share

Writing (Minute Paper)

Self-assessment

Pause for reflection

Simple

NETWORK PROTOCOLS & SECURITY
23EC2210 R/A/E

Topic:

ARP, DHCP

Session - 19

AIM OF THE SESSION

To familiarize students with the ARP and DHCP Protocols.

INSTRUCTIONAL OBJECTIVES

This Session is designed to:

1. Describe the functionality of ARP Protocol.
2. Describe the functionality of DHCP Protocol.

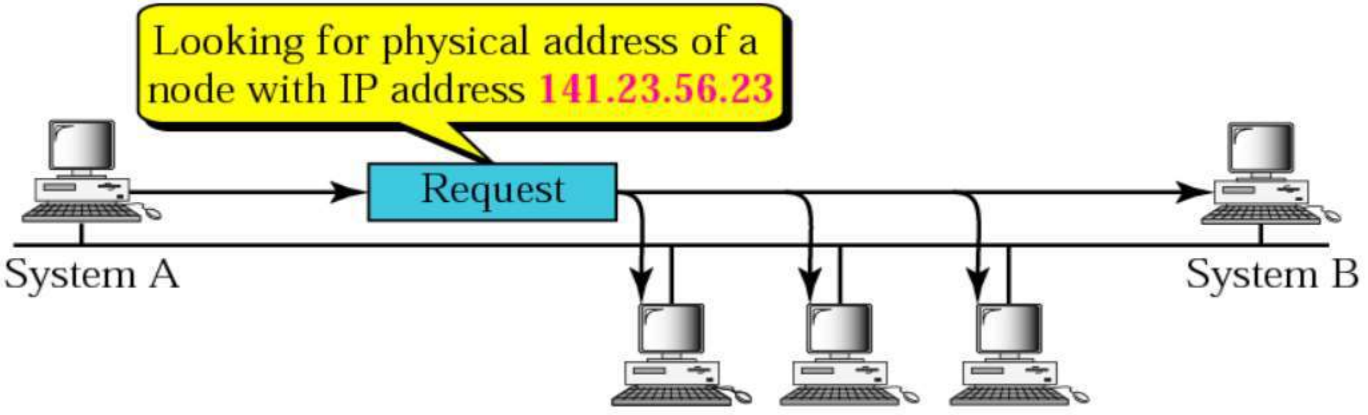
LEARNING OUTCOMES

At the end of this session, you should be able to:

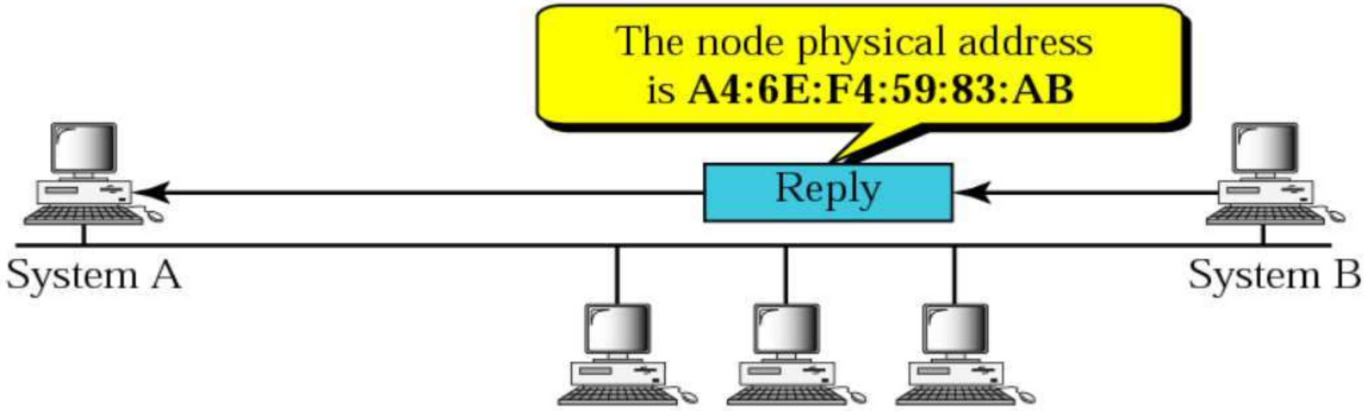
1. Illustrate the importance of ARP and DHCP protocols.
2. Demonstrate the functionality of ARP process.
3. Demonstrate the functionality of DHCP process.

ARP

ARP OPERATION


Looking for physical address of a node with IP address 141.23.56.23
Request
System A
System B

a. ARP request is broadcast

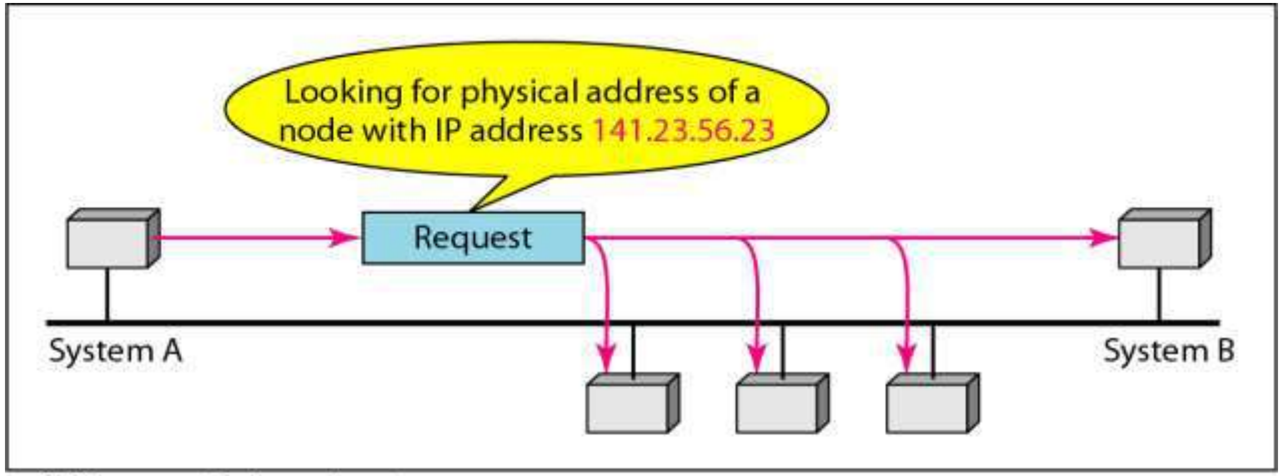


b. ARP reply is unicast

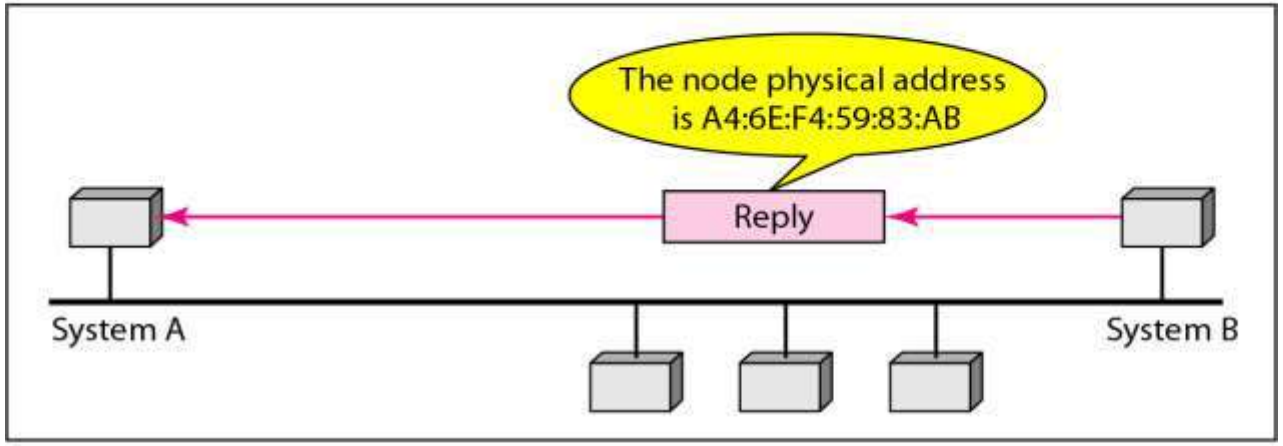
ARP (ADDRESS RESOLUTION PROTOCOL)

ARP OPERATION

ARP stands for **Address Resolution Protocol**, which is used to find the MAC address of the device from its known IP address.

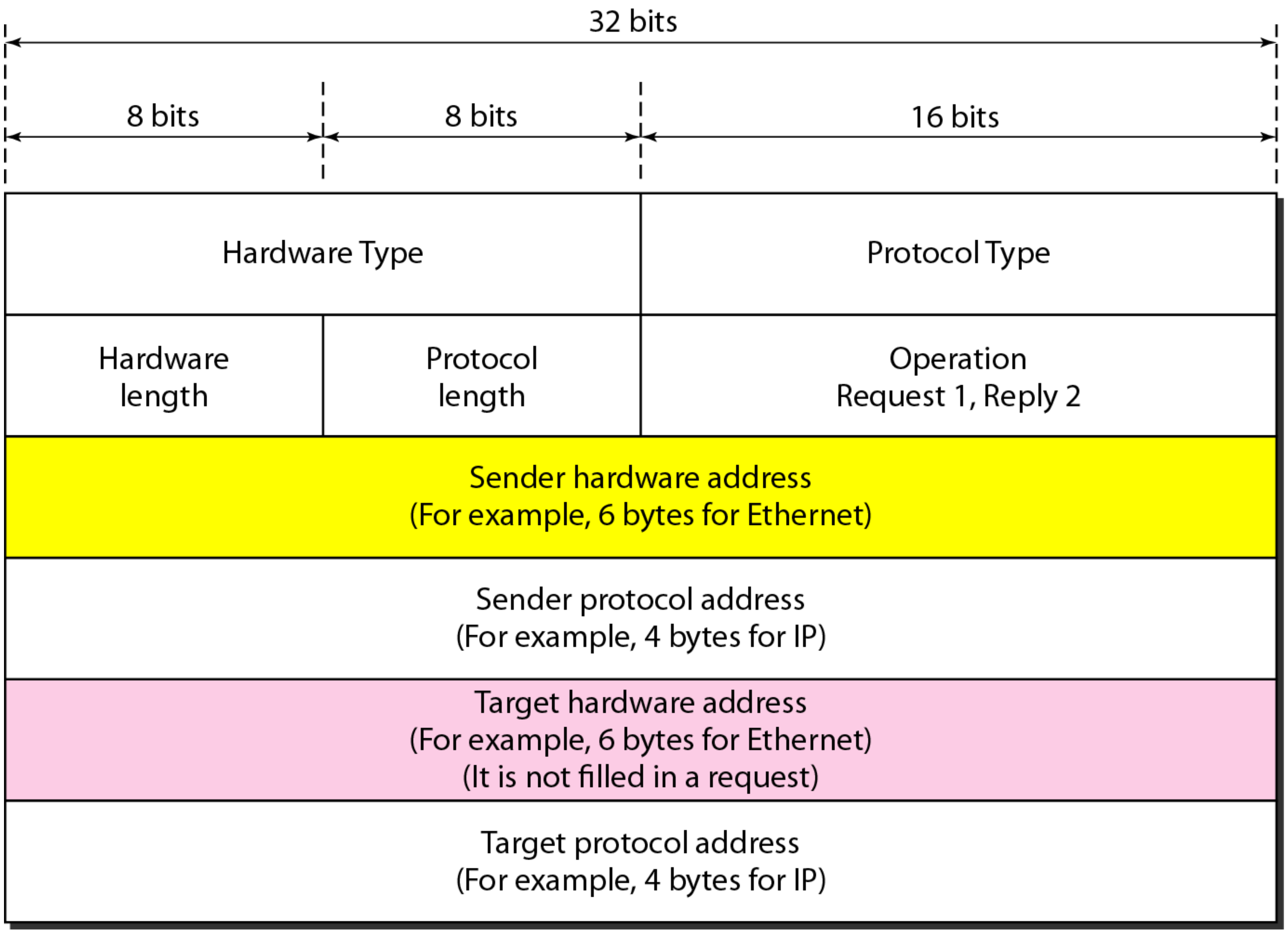

Looking for physical address of a node with IP address 141.23.56.23
Request
System A
System B

a. ARP request is broadcast



b. ARP reply is unicast

ARP PACKET FORMAT



32 bits

8 bits

8 bits

16 bits

Hardware Type

Protocol Type

Hardware length

Protocol length

Operation
Request 1, Reply 2

Sender hardware address
(For example, 6 bytes for Ethernet)

Sender protocol address
(For example, 4 bytes for IP)

Target hardware address
(For example, 6 bytes for Ethernet)
(It is not filled in a request)

Target protocol address
(For example, 4 bytes for IP)

Fields of ARP packet

- **Hardware type:** It is a 16-bit field that defines the type of network on which address resolution protocol is running.

- **Protocol type:** It is a 16-bit field that defines the type of protocol. Eg. IPV4

- **Hardware length:** It is an 8-bit field that defines the physical address length in bytes.

- **Protocol length:** It is an 8-bit field that defines the logical address length in bytes.

- **Operations:** It is a 16-bit field that defines the types of packets.
  There are two types of packets ARP request (1) and ARP reply (2).

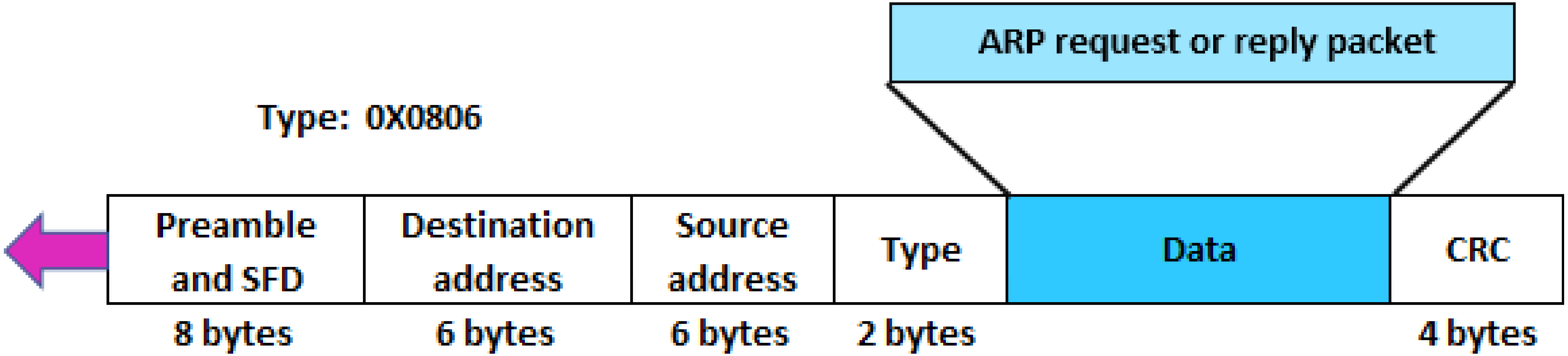
- **Sender hardware address:** It is a variable-length field that defines the physical address of the sender.

- **Sender protocol address:** It is a variable-length field that defines the logical address of the sender.

- **Target hardware address:** It is a variable-length field that defines the physical address of the receiver.

- **Target protocol address:** It is a variable-length field that defines the logical address of the receiver.

ARP ENCAPTULATION



ARP request or reply packet

Type: 0X0806

Preamble and SFD	Destination address	Source address	Type	Data	CRC
8 bytes	6 bytes	6 bytes	2 bytes		4 bytes

ARP Address Mapping Process

Below is a list of steps involved in the ARP process:

Step 1: The sender knows the IP address of the receiver.

Step 2: The IP asks ARP to create an ARP request message that contains information like sender physical address, receiver physical address field is filled with 0s, the sender IP address and receiver IP address.

Step 3: ARP request message is sent to the data link layer where the message is encapsulated in the frame using the sender's physical address as a source address and broadcast address as a destination address.

Step 4: Each and every host receives the frame because the frame contains a broadcast destination address. All hosts check the address with their address. If the match founds, the packet is dropped to that host; otherwise, it passes to the address resolution protocol.

Step 5: After receiving the packet, target host will reply with an ARP reply message that contains the target physical address. The message in this step is unicast.

Step 6: When the sender receives a reply message from the target, it knows the target's physical address.

Step 7: Now, the IP Datagram carries data for the target machine encapsulated and sent in the unicast form to the destination.

DHCP

Dynamic Host Configuration Protocol (DHCP)

- The Dynamic Host Configuration Protocol (DHCP) is a network management protocol used on Internet Protocol (IP) networks.

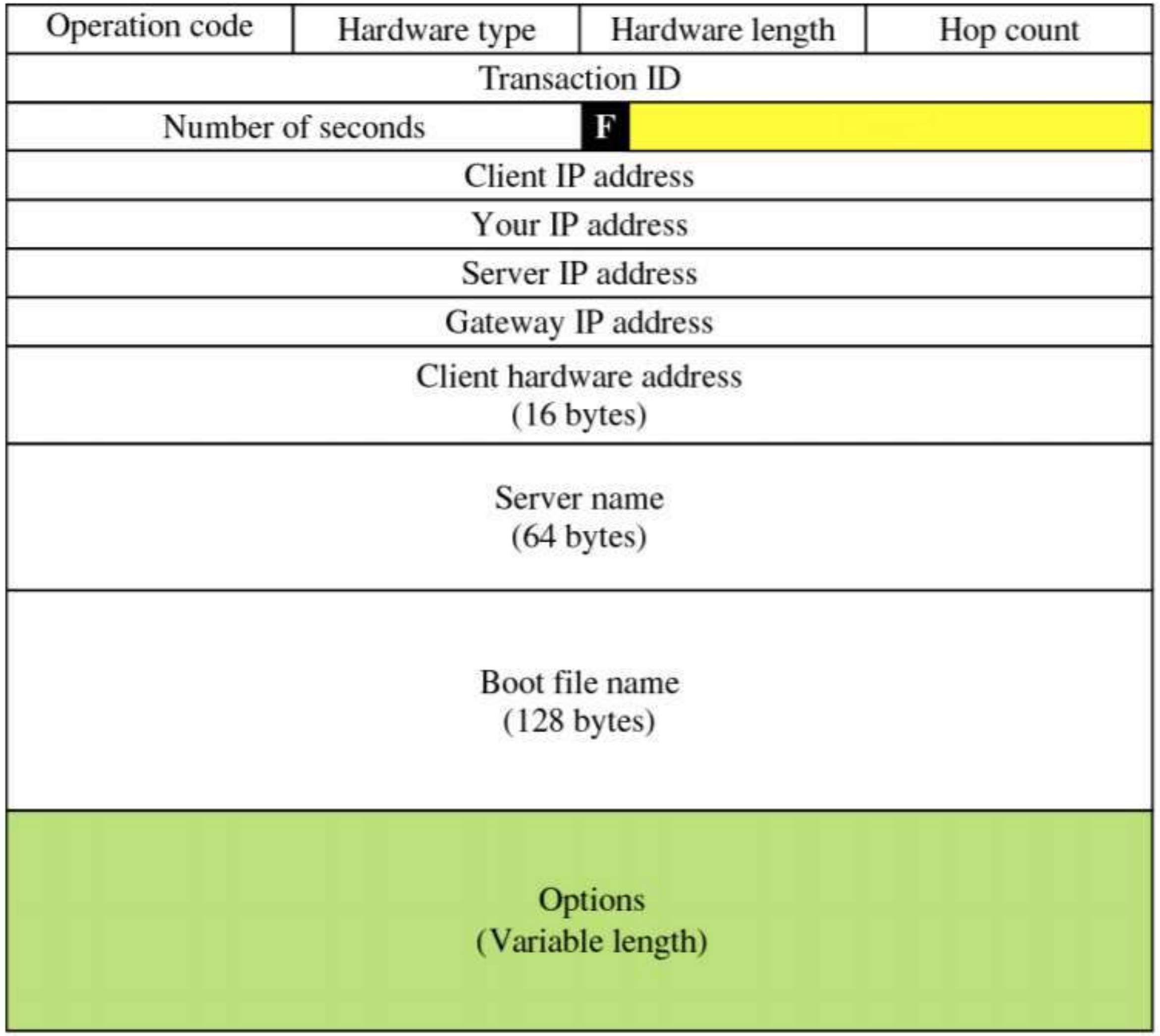
- DHCP server dynamically assigns an IP address and other network configuration parameters to each device on the network, so they can communicate with other IP networks.

- A DHCP server enables computers to request IP addresses and networking parameters automatically from the Internet service provider (ISP).

- This reduces the need for a network administrator or a user to manually assign IP addresses to all network devices.

- In the absence of a DHCP server, a computer or other device on the network needs to be manually assigned an IP address.

DHCP Message Format



Operation code | Hardware type | Hardware length | Hop count

Transaction ID

Number of seconds | F

Client IP address

Your IP address

Server IP address

Gateway IP address

Client hardware address
(16 bytes)

Server name
(64 bytes)

Boot file name
(128 bytes)

Options
(Variable length)

Operation Code: One byte field defines type of DHCP packet: Request = 1, Reply = 2

Hardware Type: One byte field defining physical network: Ethernet = 1

Hardware Length: One byte field specifying length of physical address: Ethernet = 6

Hop Count: One byte field maximum hops packet can go. Client sets this to 0

Transaction ID: Four Byte field used by client to make sure server is talking to this client and not another simultaneous request's response

Number of seconds: two byte field number of seconds since client became alive

Flag: One bit flag allows client to force server to broadcast reply instead of sending reply to a specific IP address. If client does not know its IP address yet, it wants a broadcast reply from server.

Client IP address: Four byte field of client's IP address. If unknown is zero.

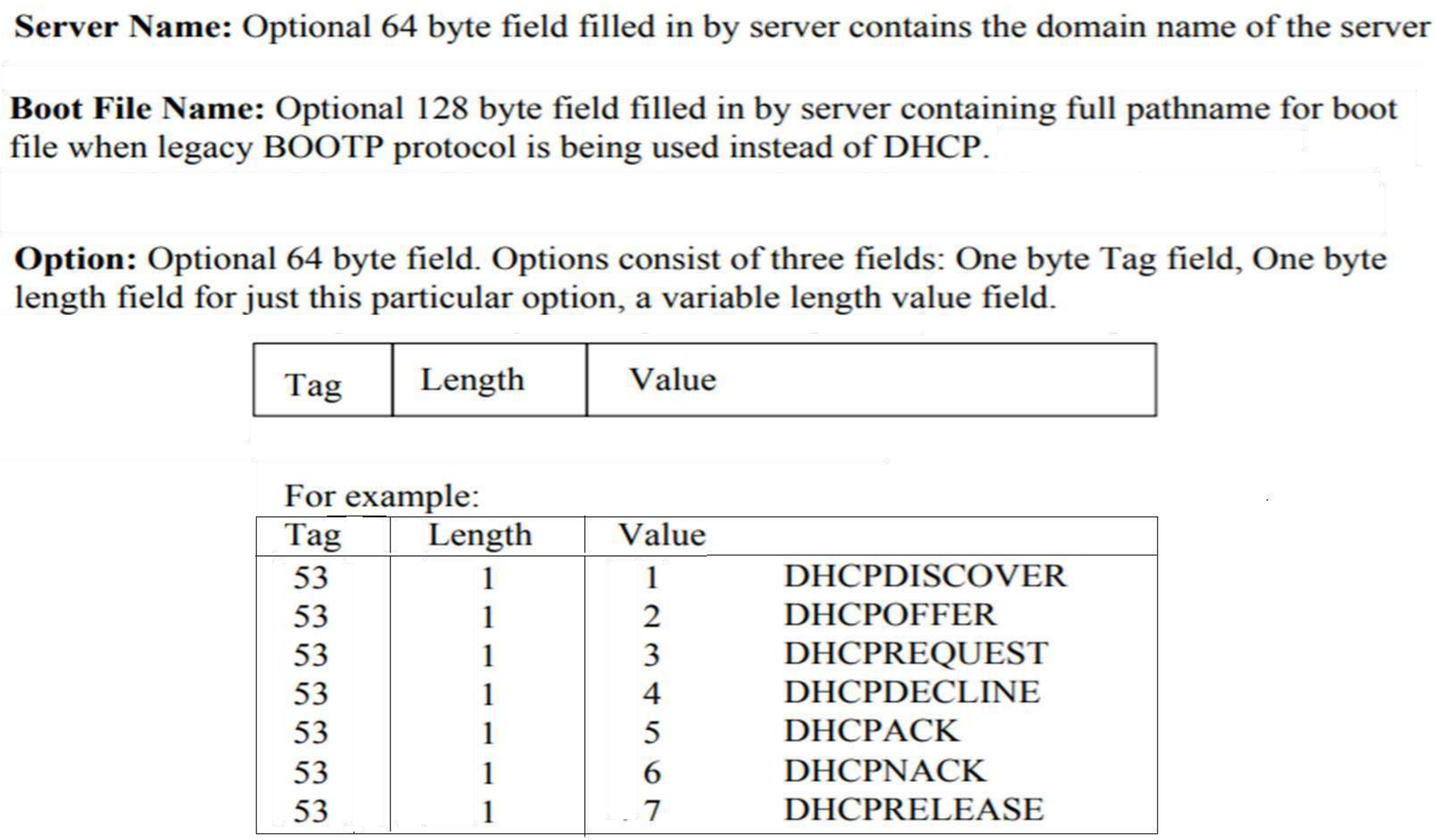
Your IP address: Four byte field server fills in to tell client the clients IP address

Server IP address: four byte field. Server responding fills in it's own IP

Gateway IP Address: Four byte field containing IP address of router (filled in by server)

Client Hardware Address: In our case 6 byte Ethernet MAC of client sending. Can get this from Ethernet frame source MAC but this makes life easy for lazy server

DHCP Message Format…



Server Name: Optional 64 byte field filled in by server contains the domain name of the server

Boot File Name: Optional 128 byte field filled in by server containing full pathname for boot file when legacy BOOTP protocol is being used instead of DHCP.

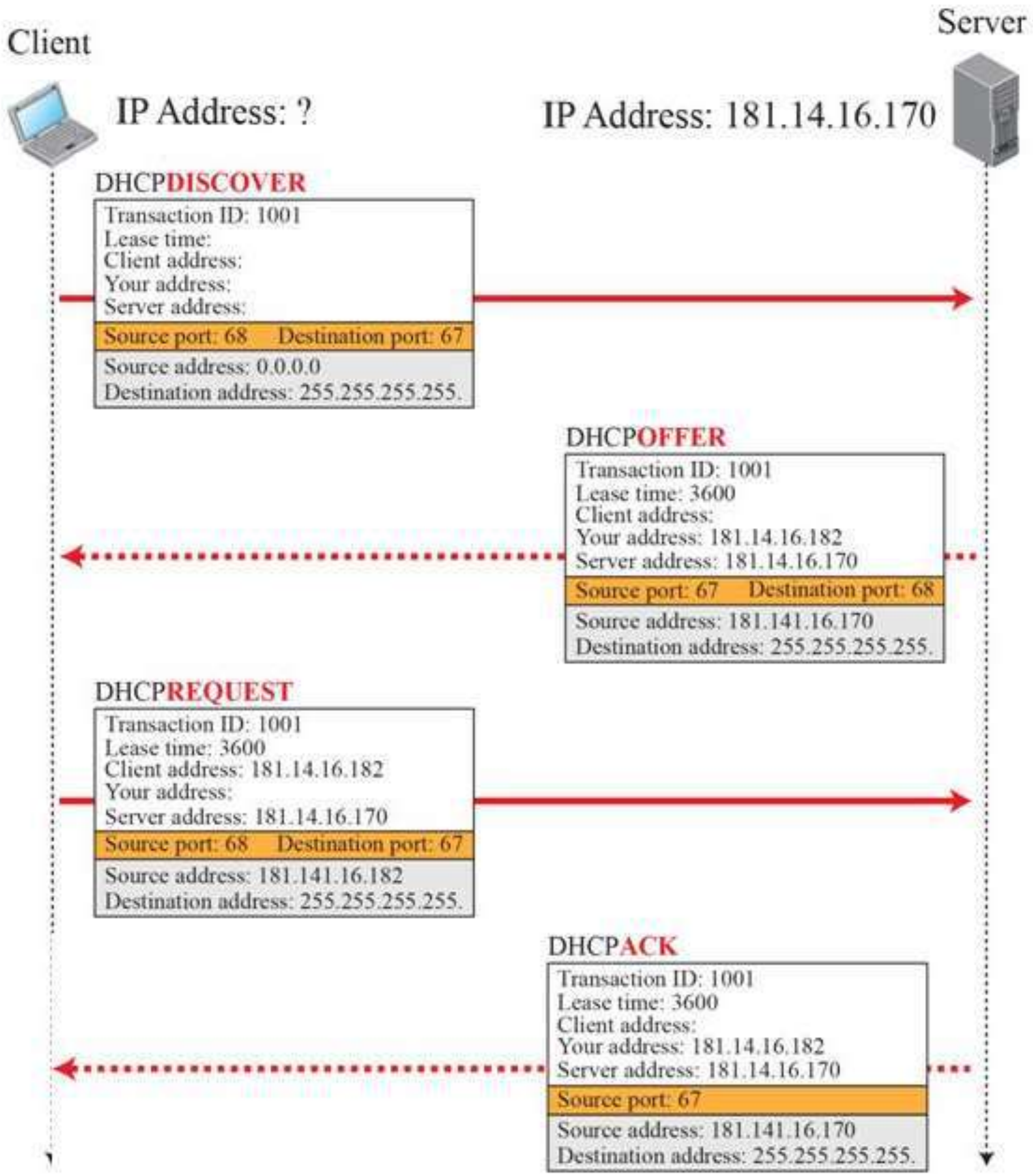
Option: Optional 64 byte field. Options consist of three fields: One byte Tag field, One byte length field for just this particular option, a variable length value field.

Tag	Length	Value

For example:

Tag	Length	Value	
53	1	1	DHCPDISCOVER
53	1	2	DHCPOFFER
53	1	3	DHCPREQUEST
53	1	4	DHCPDECLINE
53	1	5	DHCPACK
53	1	6	DHCPNACK
53	1	7	DHCPRELEASE

DHCP Operation



DHCP**DISCOVER**

Transaction ID: 1001
Lease time:
Client address:
Your address:
Server address:
Source port: 68 Destination port: 67
Source address: 0.0.0.0
Destination address: 255.255.255.255.

DHCP**OFFER**

Transaction ID: 1001
Lease time: 3600
Client address:
Your address: 181.14.16.182
Server address: 181.14.16.170
Source port: 67 Destination port: 68
Source address: 181.141.16.170
Destination address: 255.255.255.255.

DHCP**REQUEST**

Transaction ID: 1001
Lease time: 3600
Client address: 181.14.16.182
Your address:
Server address: 181.14.16.170
Source port: 68 Destination port: 67
Source address: 181.141.16.182
Destination address: 255.255.255.255.

DHCP**ACK**

Transaction ID: 1001
Lease time: 3600
Client address:
Your address: 181.14.16.182
Server address: 181.14.16.170
Source port: 67
Source address: 181.141.16.170
Destination address: 255.255.255.255.

Legend

Application
UDP
IP

Note:
Only partial information is given.

DHCP Messages

DHCPDISCOVER

- The first time a DHCP client computer attempts to log on to the network, it requests IP address information from a DHCP server by broadcasting a DHCP Discover packet.
- It is a broadcast message where the source IP address in the packet is 0.0.0.0 because the client does not yet have an IP address and the destination address is 255.255.255.255.

DHCPOFFER

- Each DHCP server that receives the client DHCP Discover packet responds with a DHCP Offer packet containing an unleased IP address and additional network configuration information, such as the subnet mask and default gateway.
- More than one DHCP server can respond with a DHCP Offer packet. The client will accept the first DHCP Offer packet it receives.

DHCPREQUEST

- When a DHCP client receives a DHCP Offer packet, it responds by sending a DHCP Request packet that contains the offered IP address, and shows acceptance of the offered IP address

DHCP Messages…

DHCP Acknowledge (DHCPAck)

The DHCPACK message is an acknowledgement by the DHCP server that authorizes the DHCP client to start using the network configuration it received from the DHCP server earlier.

DHCPNAK

- This message is the exact opposite to DHCPACK described above. This message is sent by the DHCP server when it is not able to satisfy the DHCPREQUEST message from the client.

DHCPDECLINE

- This message is sent from the DHCP client to the server in case the client finds that the IP address assigned by DHCP server is already in use.

DHCPRELEASE

- A DHCP client sends a DHCP Release packet to the server to release the IP address and cancel any remaining lease.

SUMMARY

- ARP Protocol
- DHCP Protocol

TERMINAL QUESTIONS

1. With a neat sketch demonstrate the functioning of ARP and RARP protocols.

2. With a neat sketch demonstrate the functioning of DHCP protocol.

3. Discuss in detail the messages communication in DHCP process.

REFERENCES FOR FURTHER LEARNING OF THE SESSION

Reference Books:

1. Behrouz A. Forouzan , “Data Communication and Networking”, TMH, 5th Edition, 2012.
2. A.S. Tanenbaum, David J. Wetheral “Computer Networks” Pearson, 5th Edition.

THANK YOU

KL

(DEEMED TO BE UNIVERSITY)

Team – Network Protocols & Security