Internet Protocol

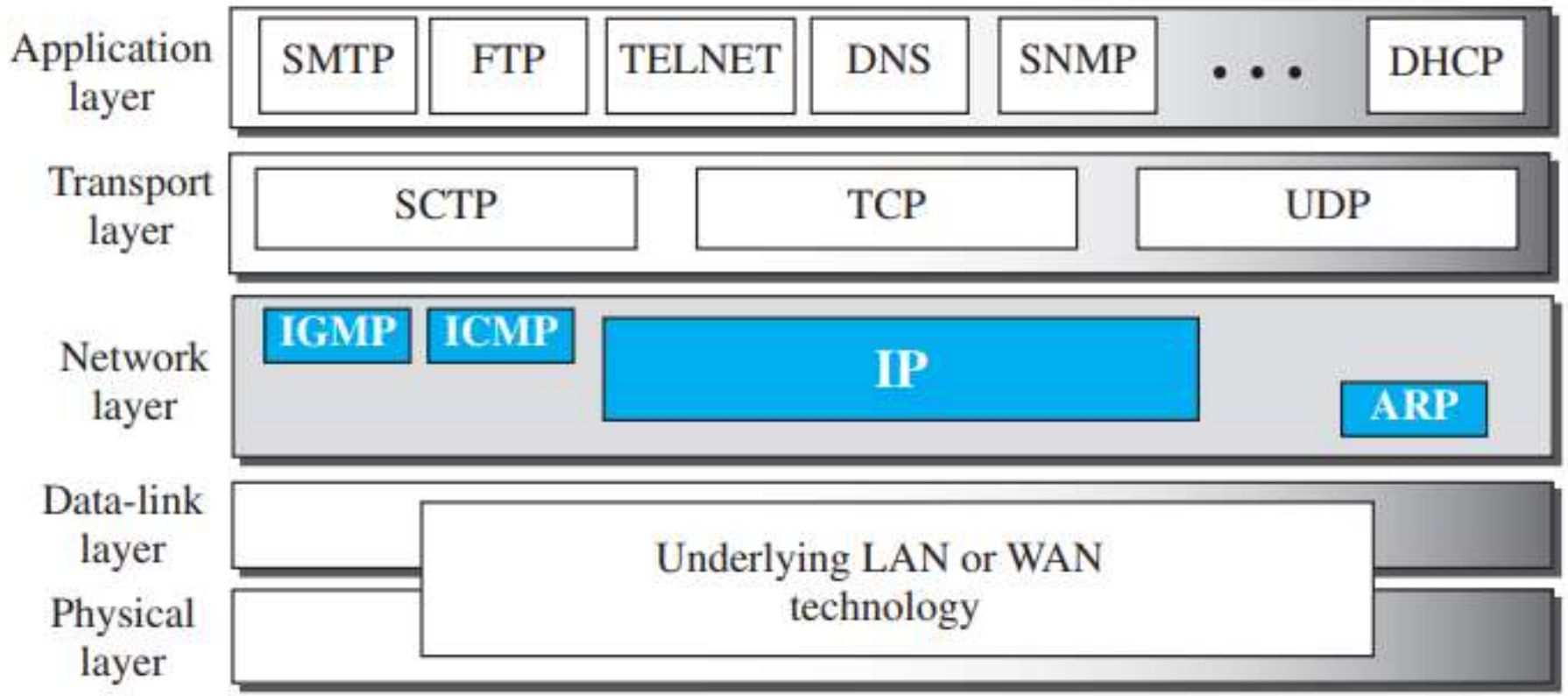
Prof. Kirtankumar Rathod

Dept. Of Computer Science,

ISHLS, Indus University

Internet Protocol:

Figure 19.1 *Position of IP and other network-layer protocols in TCP/IP protocol suite*



Internet Protocol:

- Internet Protocol version 4 (IPv4), is responsible for packetizing, forwarding, and delivery of a packet at the network layer.
- The Internet Control Message Protocol version 4 (ICMPv4) helps IPv4 to handle some errors that may occur in the network-layer delivery.
- The Internet Group Management Protocol (IGMP) is used to help IPv4 in multicasting.
- The Address Resolution Protocol (ARP) is used to glue the network and data-link layers in mapping network-layer addresses to link-layer addresses.

IPv4

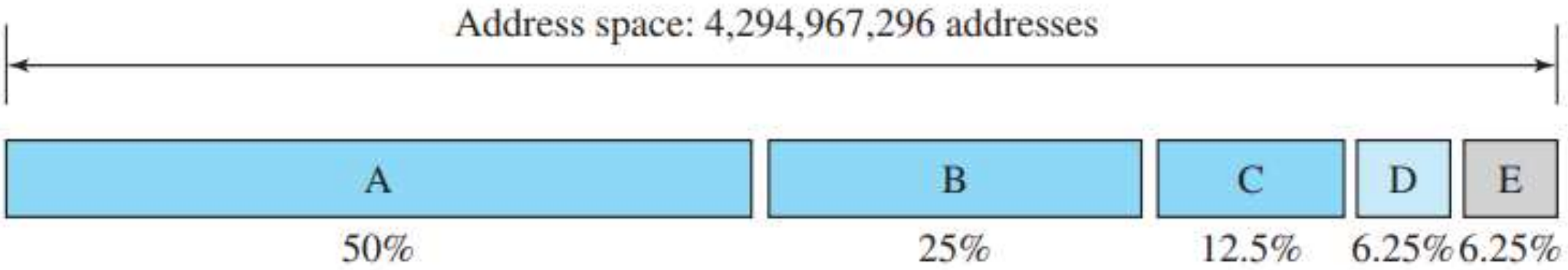
- IPv4 is an **unreliable** datagram protocol—a **best-effort** delivery service.

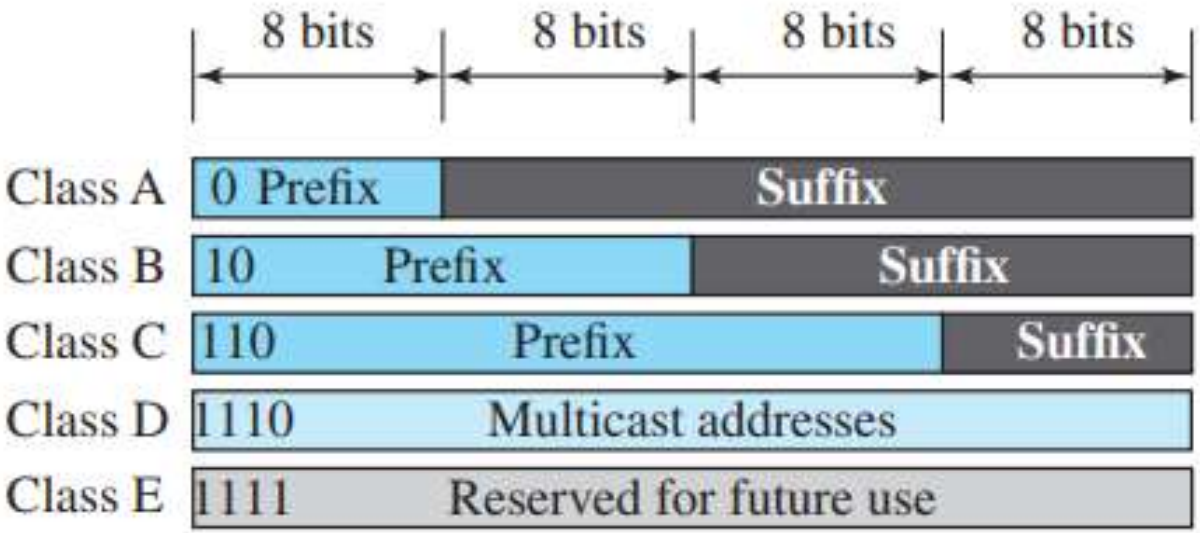
- The term **best-effort** means that IPv4 packets can be corrupted, be lost, arrive out of order, or be delayed, and may create congestion for the network.

- IPv4 is also a **connectionless** protocol that uses the datagram approach.

- This means that each datagram is handled **independently**, and each datagram can follow a different route to the destination.

IPv4 Address Classification:

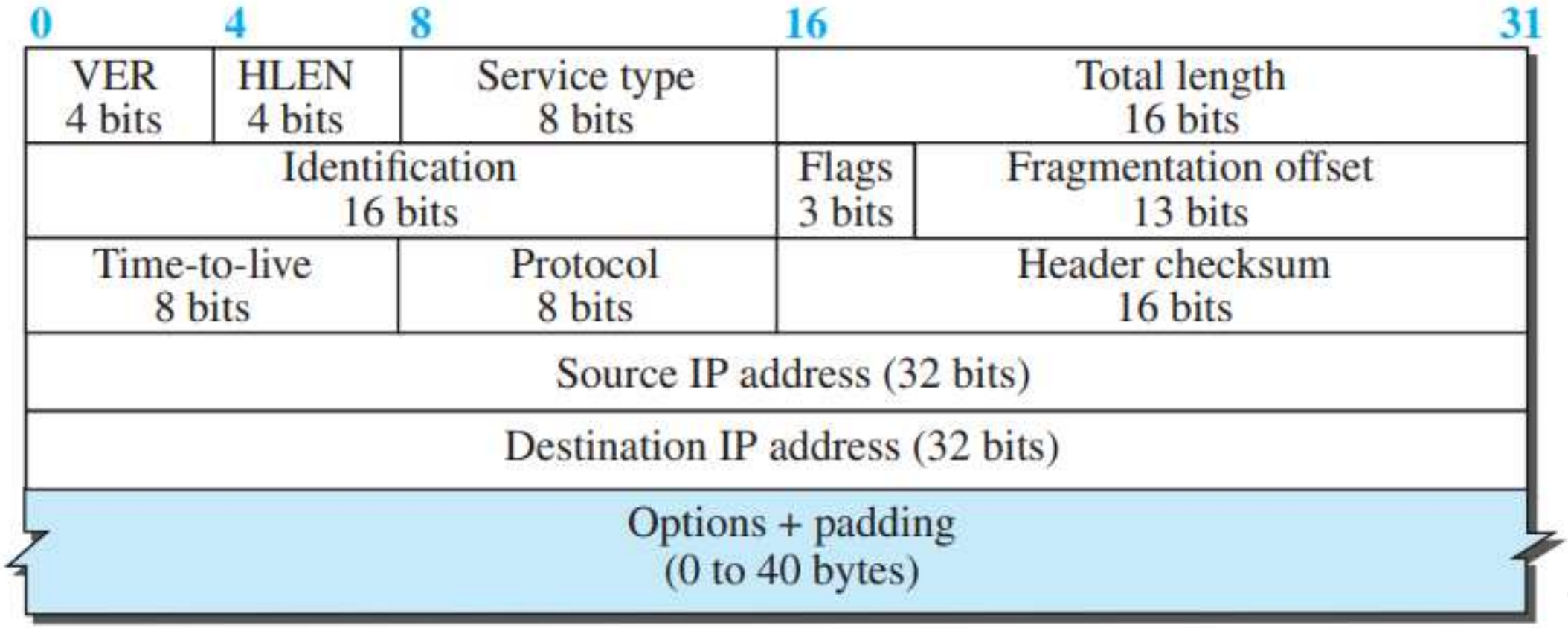




Class	Prefixes	First byte
A	$n = 8$ bits	0 to 127
B	$n = 16$ bits	128 to 191
C	$n = 24$ bits	192 to 223
D	Not applicable	224 to 239
E	Not applicable	240 to 255

IPv4 Datagram Format

A datagram is a variable-length packet consisting of two parts: header and payload (data). The header is 20 to 60 bytes in length and contains information essential to routing and delivery.



IPv4 Datagram :

1. Version Number : The 4-bit version number (VER) field defines the version of the IPv4 protocol, which, obviously, has the value of 4.

2. Header Length : The 4-bit header length (HLEN) field defines the total length of the datagram header in 4-byte words.

3. Total Length : This 16-bit field defines the total length (header plus data) of the IP datagram in bytes. A 16-bit number can define a total length of up to 65,535 (when all bits are 1s).

4. Identification, Flags, and Fragmentation Offset : These three fields are related to the fragmentation of the IP datagram when the size of the datagram is larger than the underlying network can carry.

IPv4 Datagram :

5. Time-to-live : The time-to-live (TTL) field is used to control the maximum number of hops (routers) visited by the datagram. Each router that processes the datagram decrements this number by one. If this value, after being decremented, is zero, the router discards the datagram.

6. Protocol : In TCP/IP, the data section of a packet, called the payload, carries the whole packet from another protocol. A datagram, for example, can carry a packet belonging to any transport-layer protocol such as UDP or TCP.

7. Header checksum : IP is not a reliable protocol; it does not check whether the payload carried by a datagram is corrupted during the transmission. IP puts the burden of error checking of the payload on the protocol that owns the payload, such as UDP or TCP

IPv4 Datagram :

8. Source and Destination Addresses : These 32-bit source and destination address fields define the IP address of the source and destination respectively. The source host should know its IP address. The destination IP address is either known by the protocol that uses the service of IP or is provided by the DNS.

9. Options : A datagram header can have up to 40 bytes of options. Options can be used for network testing and debugging.

10. Payload : Payload, or data, is the main reason for creating a datagram. Payload is the packet coming from other protocols that use the service of IP

Fragmentation :

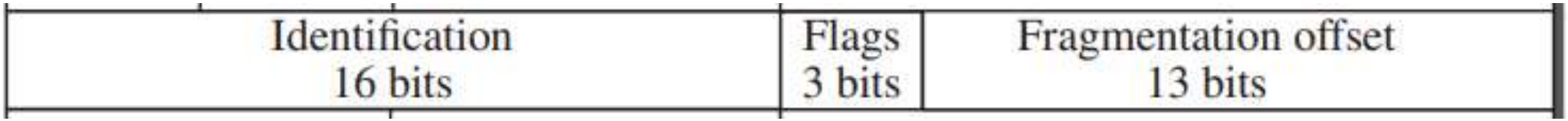
- Each link-layer protocol has its own frame format. Each format has its own MTU (Maximum Transfer Unit) .
- The total size of the datagram must be less than this MTU size.
- The value of the MTU differs from one physical network protocol to another.

- Dividing the datagram for the MTU is known as fragmentation.

- A datagram can be fragmented by the source host or any router in the path.
- The reassembly of the datagram, however, is done only by the destination host, because each fragment becomes an independent datagram.

Fragmentation :

- Three fields in an IP datagram are related to fragmentation: identification, flags, and fragmentation offset.
  1) The 16-bit identification field identifies a datagram originating from the source host.
  2) The 3-bit flags field defines three flags. The leftmost bit is reserved (not used). The second bit (D bit) is called the do not fragment bit. The third bit (M bit) is called the more fragment bit.
  3) The 13-bit fragmentation offset field shows the relative position of this fragment with respect to the whole datagram.



ICMPv4

1. What happens if the final destination host must discard the received fragments of a datagram because it has not received all fragments within a predetermined time limit?
2. What happens if a router must discard a datagram because it cannot find a route to the final destination, or because the time-to-live field has a zero value?

- The Internet Control Message Protocol version 4 (ICMPv4) has been designed to compensate for the above two deficiencies.

ICMPv4:

- ICMP messages are divided into two broad categories: error-reporting messages and query messages.

1. The error-reporting messages report problems that a router or a host (destination) may encounter when it processes an IP packet.

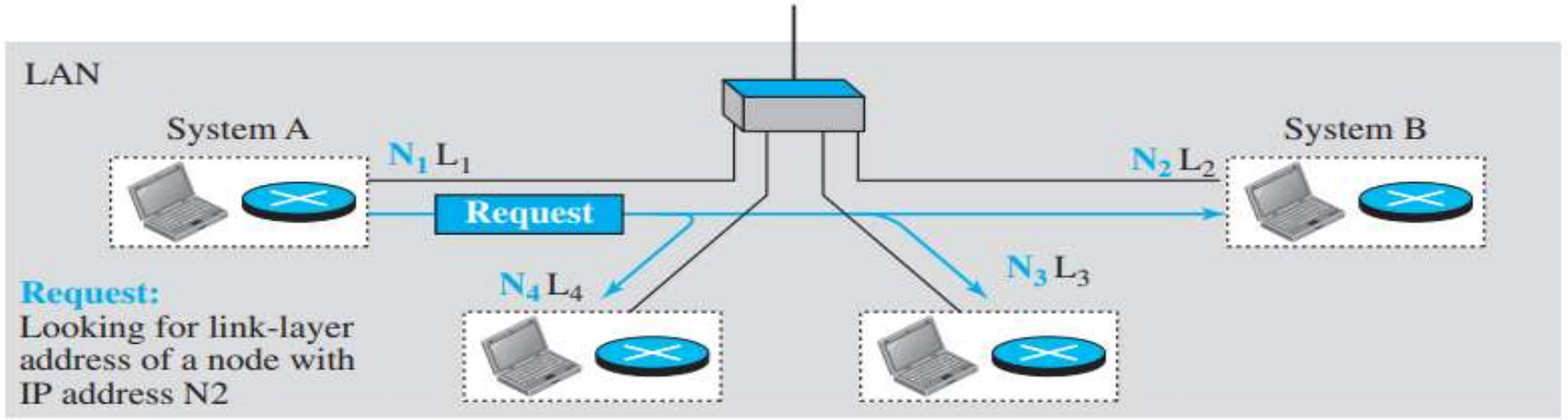
2. The query messages, which occur in pairs, help a host or a network manager get specific information from a router or another host.

IGMP:

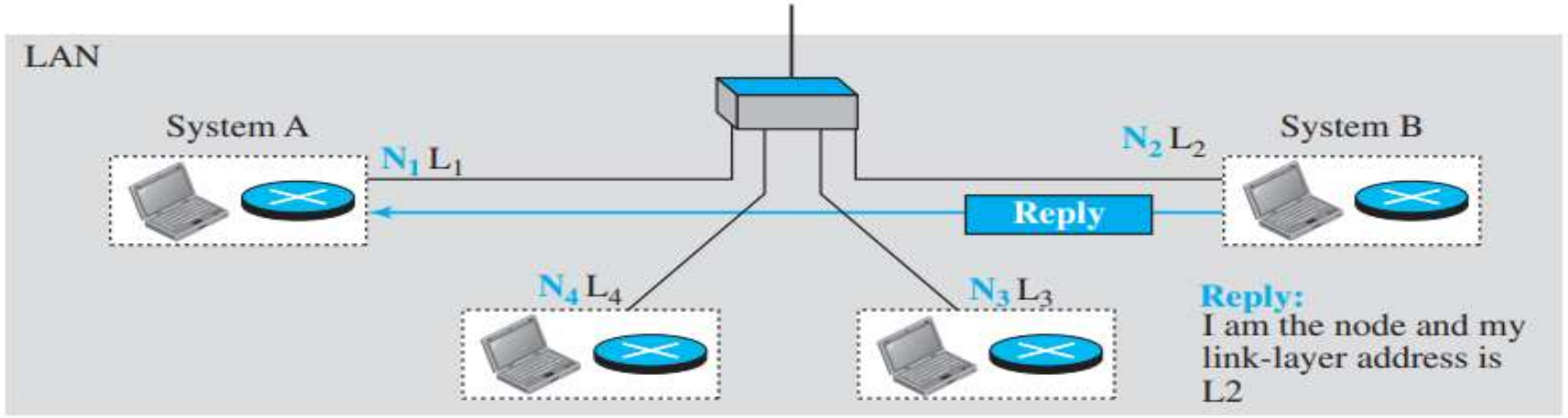
- The protocol that is used today for collecting information about group membership is the Internet Group Management Protocol (IGMP).
- IGMP is a protocol defined at the network layer.
- There are only two types of messages in IGMP version 3, query and report messages.
- A query message is periodically sent by a router to all hosts attached to it to ask them to report their interests about membership in groups.
- A report message is sent by a host as a response to a query message.
- The IGMP message is encapsulated in an IP datagram with the value of the protocol field set to 2 and the TTL field set to 1.

ARP:

- Address Resolution Protocol is defined in the network layer.
- It is used to map an IP address with logical-link address.



a. ARP request is broadcast



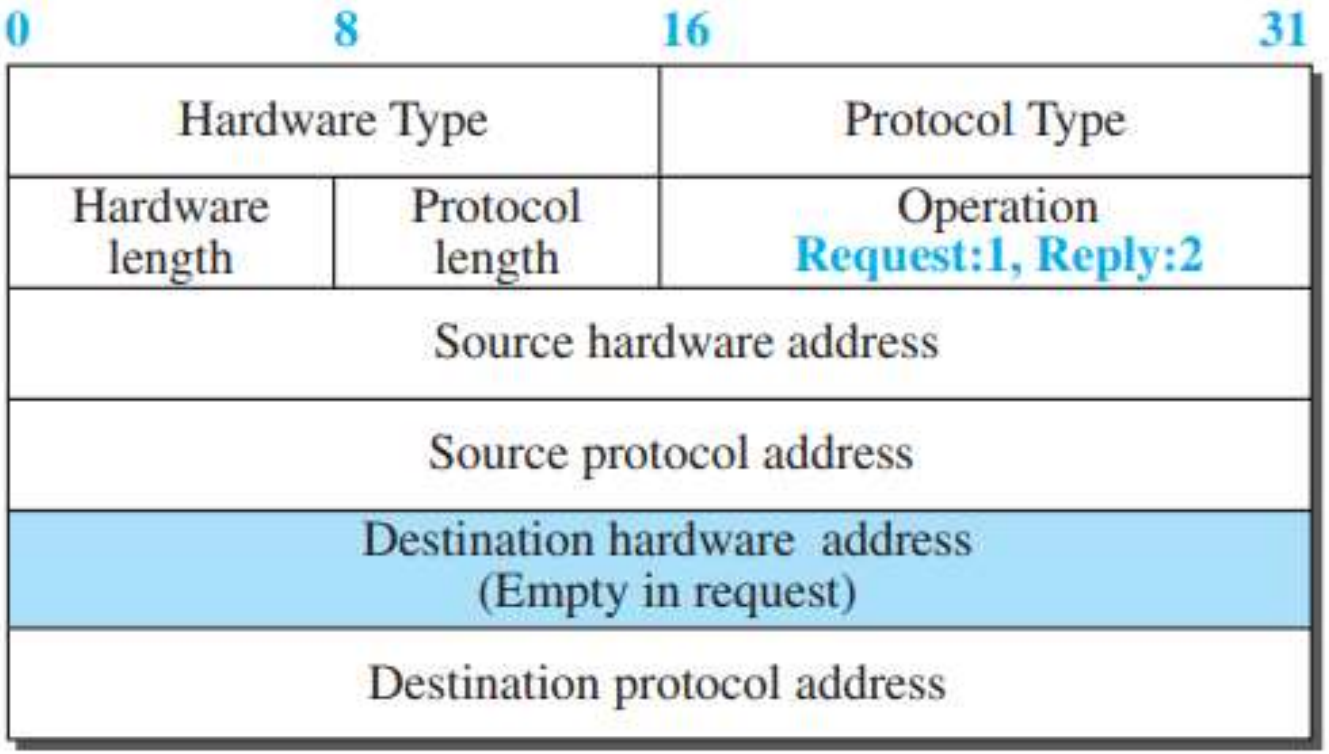
b. ARP reply is unicast

Working of ARP:

- Anytime a host or a router needs to find the link-layer address of another host or router in its network, it sends an **ARP request** packet.
- The packet includes the link-layer and IP addresses of the sender and the IP address of the receiver.
- Because the sender does not know the link-layer address of the receiver, the query is **broadcast** over the link using the link-layer broadcast address.
- Every host or router on the network **receives** and processes the ARP request packet, but only the intended recipient recognizes its IP address and sends back an ARP **response** packet.
- The **response** packet contains the recipient's IP and link-layer addresses.
- The packet is **unicast** directly to the node that sent the request packet.

ARP Packet Format:

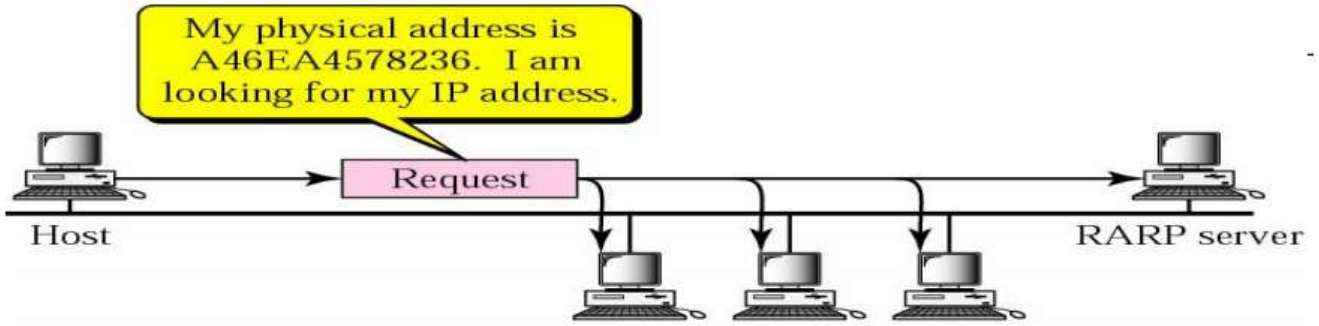
Figure 9.8 *ARP packet*



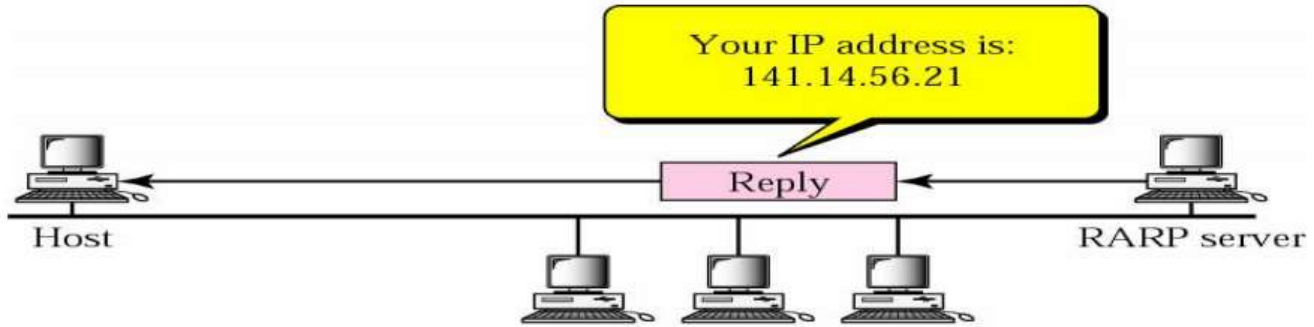
Hardware: LAN or WAN protocol
Protocol: Network-layer protocol

RARP:

- Reverse Address Resolution Protocol (RARP) is used by a client computer to request its Internet Protocol address from a computer network using its MAC address.
- The client broadcasts the request and does not need prior knowledge of the network topology or the identities of servers capable of fulfilling its request.
- RARP requires one or more server hosts to maintain a database of mappings of Link Layer addresses to their respective protocol addresses.



a. RARP request is broadcast



b. RARP reply is unicast

BOOTP:

- The Bootstrap Protocol (BOOTP) is a computer networking protocol used in Internet Protocol networks to automatically assign an IP address to network devices from a configuration server.

- When a computer that is connected to a network is powered up and boots its operating system, the system software broadcasts BOOTP messages onto the network to request an IP address assignment.

- A BOOTP configuration server assigns an IP address based on the request from a pool of addresses configured by an administrator.

- BOOTP has also been used for Unix-like diskless workstations to obtain the network location of their boot image, in addition to the IP address assignment.

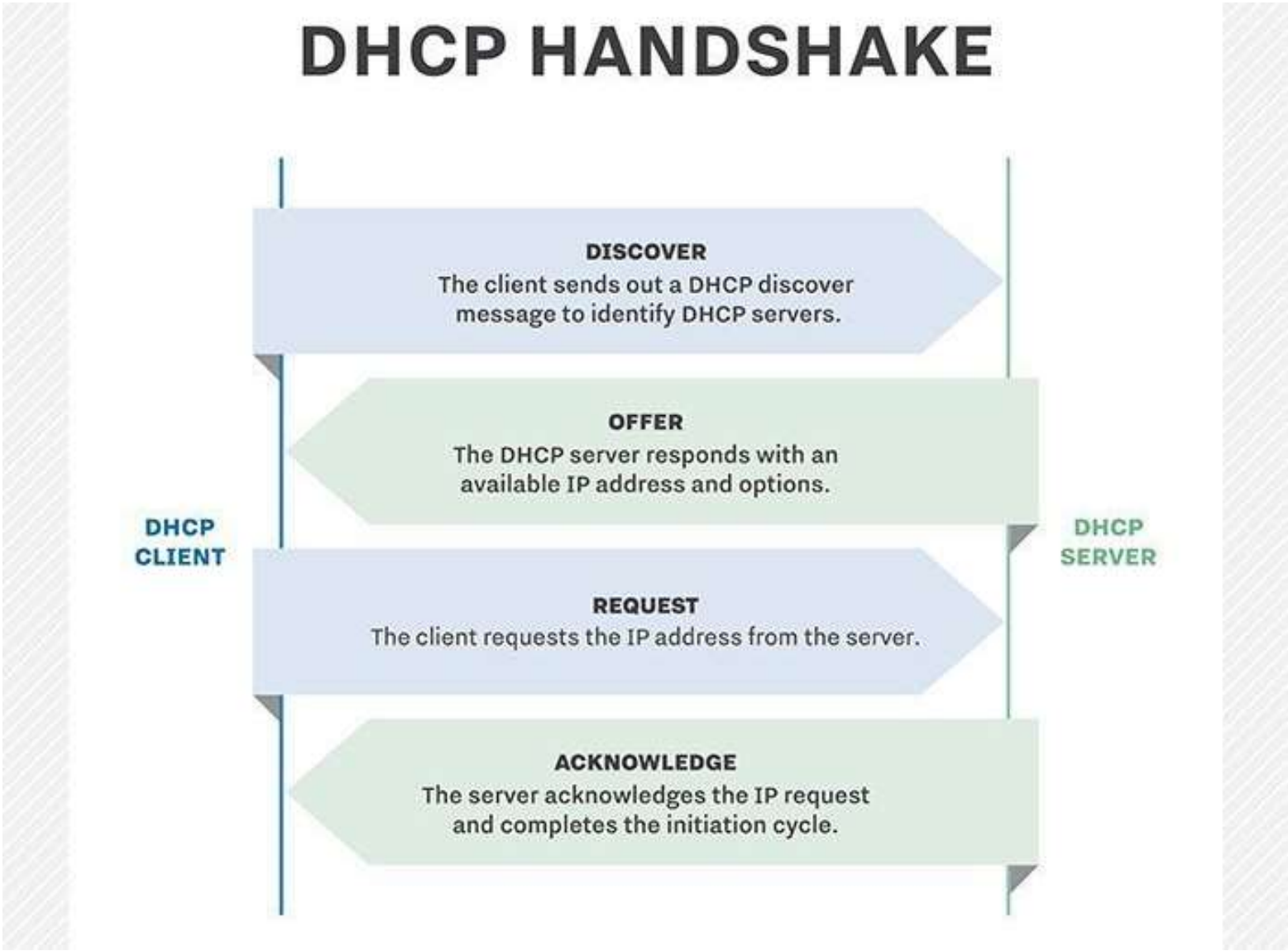
DHCP:

- DHCP stands for dynamic host configuration protocol and is a network protocol used on IP networks where a DHCP server automatically assigns an IP address and other information to each host on the network so they can communicate efficiently with other endpoints.

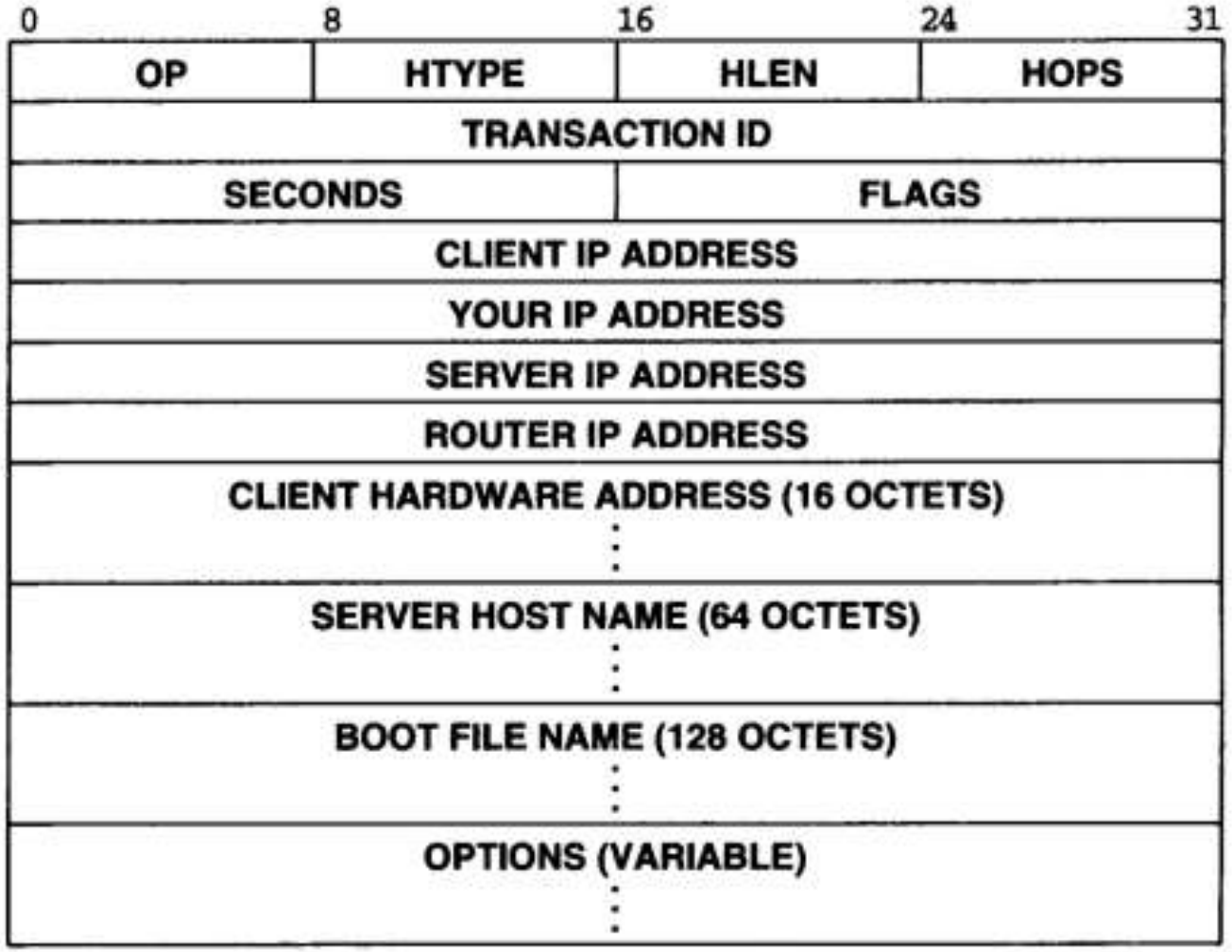
- DHCP server may have three methods of allocating IP-addresses:

1. **Static** allocation: The DHCP server allocates an IP address based on a table with MAC address/IP address pairs, which are manually filled.
2. **Dynamic** allocation: A network administrator assigns a range of IP addresses to DHCP, and each client computer on the LAN is configured to request an IP address from the DHCP server during network initialization.
3. **Automatic** allocation: The DHCP server permanently assigns a free IP address to a requesting client from the range defined by the administrator.

Working of DHCP:



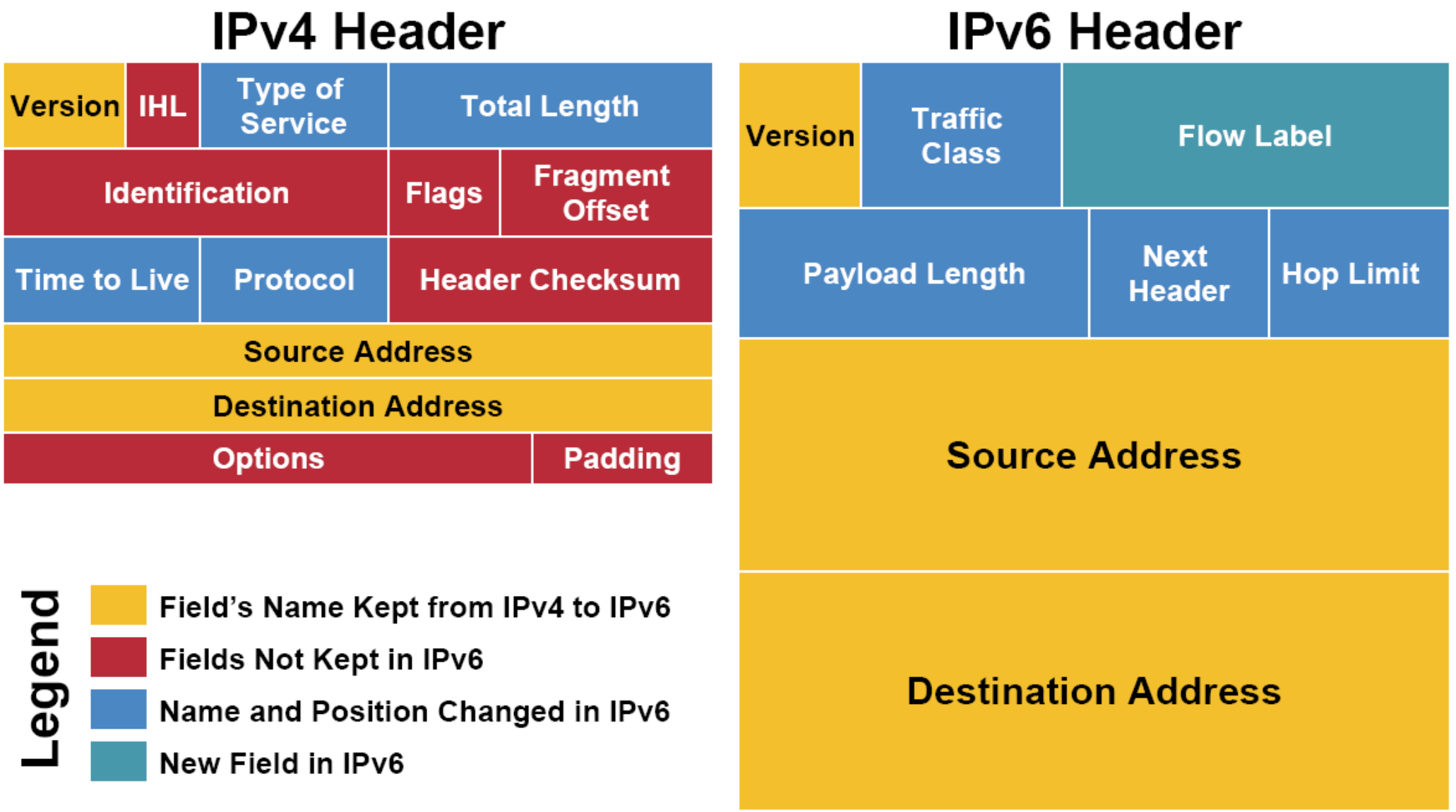
DHCP message format:



IPv6:

- Internet Protocol version 6 is the next generation IP.
- Main reason for migration from IPv4 to IPv6 is the small size of the address space in IPV4.
- IPv6 address is of 128 bits.
  - Example: in hexadecimal (FEF6:BA98:7654:3210:ADEF:2922:FF00)
- It require the change in the protocol format of IPv4.

From IPv4 to IPv6 protocol format:



IPv6 protocol format:

- **Version** field defined the value is 6.
- **Traffic class** is used to distinguish different payloads with different delivery requirements.
- **Flow label** is a 20-bit field used to handle the flow of data.
- **Payload length** contain the length of IP datagram.
- **Next header** define the type of first extension header (if any).
- **Hop limit** field contain number of hops from one router to another router.
- **Source** and **Destination address** contain 128 bit of IP address.

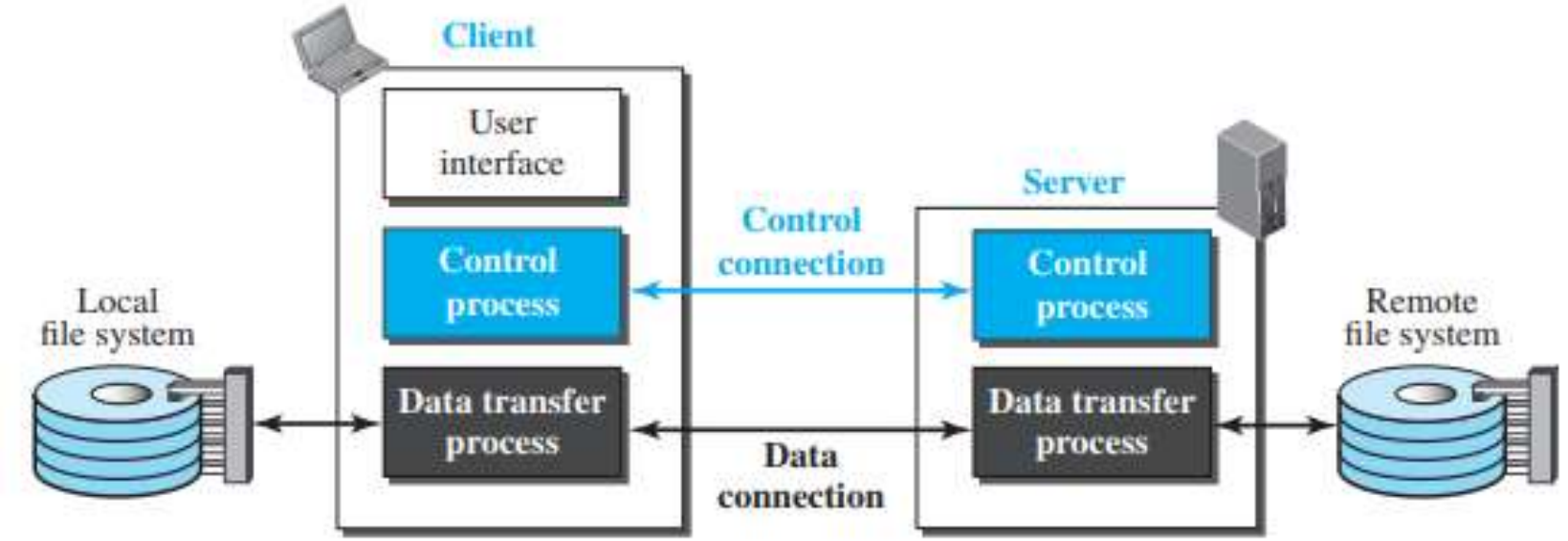
Difference between IPv4 and IPv6

IPv4	IPv6
• IPv4 has 32-bit address length.	• IPv6 has 128-bit address length.
• It Supports Manual and DHCP address configuration.	• It supports Auto and renumbering address configuration.
• Security feature is dependent on application.	• IPSEC is inbuilt security feature in the IPv6 protocol.
• Address representation of IPv4 in decimal.	• Address Representation of IPv6 is in hexadecimal.
• Fragmentation performed by Sender and forwarding routers.	• In IPv6 fragmentation performed only by sender.
• In IPv4 Packet flow identification is not available.	• In IPv6 packet flow identification are available and uses flow label field in the header.
• In IPv4 checksum field is available.	• In IPv6 checksum field is not available.
• IPv4 has header of 20-60 bytes.	• IPv6 has header of 40 bytes fixed.

FTP:

- Transferring files from one system to another seems simple and straightforward, some problems must be dealt with first.
- For example, two systems may use different file name conventions. Two systems may have different ways to represent data. Two systems may have different directory structures.
- All these problems solved by FTP (File Transfer Protocol), which is the standard protocol provided by TCP/IP for copying a file from one host to another.

Figure 26.10 *FTP*

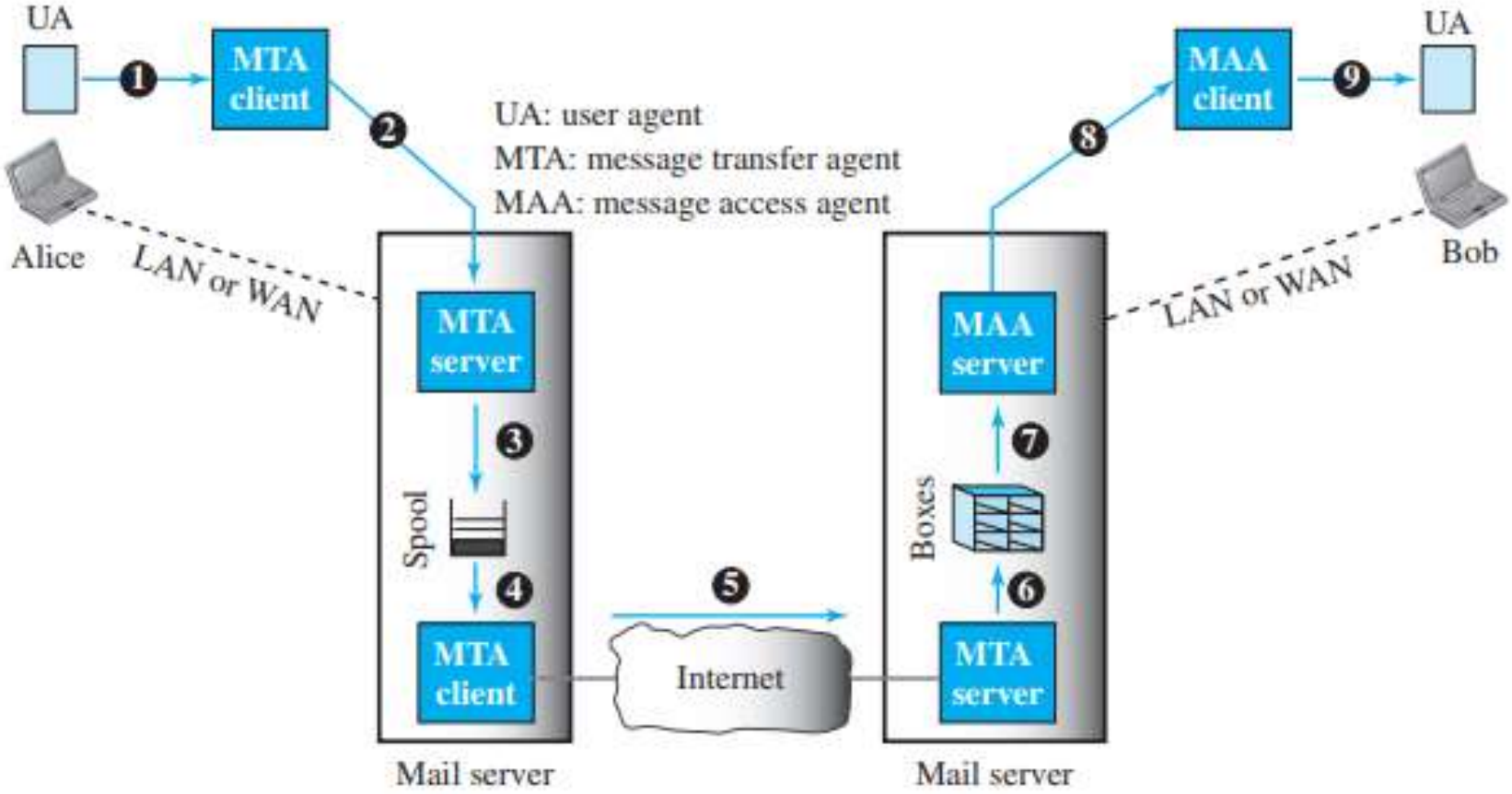


FTP:

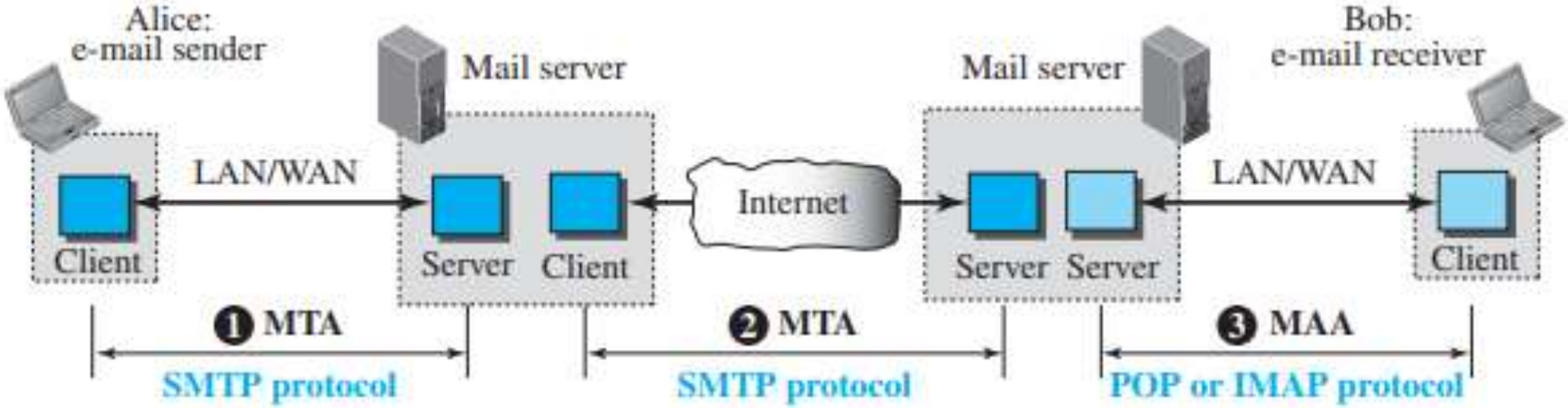
- The client has three components: the user interface, the client control process, and the client data transfer process.
- The server has two components: the server control process and the server data transfer process
- The control connection uses very simple rules of communication.
- We need to transfer only a line of command or a line of response at a time.
- The data connection, on the other hand, needs more complex rules due to the variety of data types transferred.
- The two connections in FTP have different lifetimes.
  - The control connection remains connected during the entire interactive FTP session.
  - The data connection is opened and then closed for each file transfer activity.

E-mail:

- Electronic mail (or e-mail) allows users to exchange messages.
- In FTP server program is running all the time and waiting for client to connect and transfer the file.
- But, in the case of e-mail, it is considered a one-way transaction.



Protocols used in E-mail:



Message Access Agent:

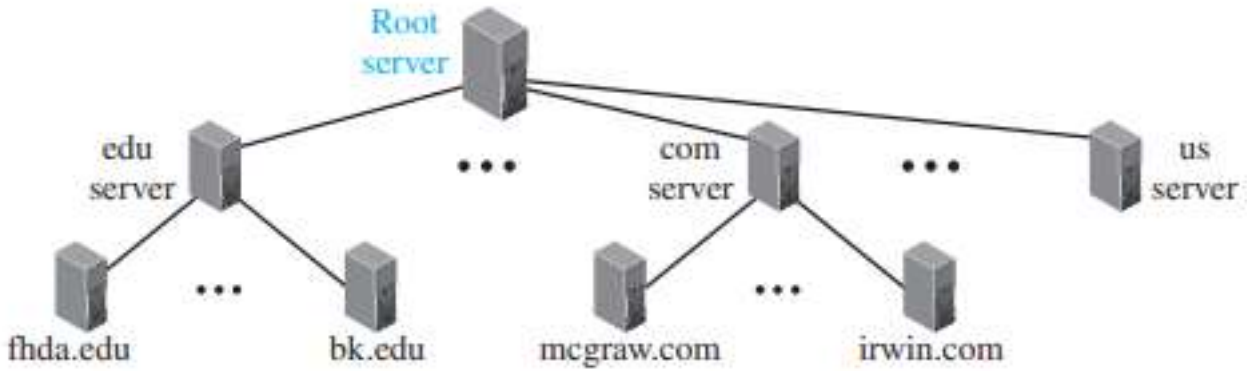
- The first and second stages of mail delivery use SMTP. However, SMTP is not involved in the third stage because SMTP is a push protocol; it pushes the message from the client to the server.
- The direction of the bulk data (messages) is from the client to the server.
- The third stage needs a pull protocol; the client must pull messages from the server.
- The direction of the bulk data is from the server to the client.
- The third stage uses a message access agent.
- Currently two message access protocols are available: Post Office Protocol, version 3 (POP3) and Internet Mail Access Protocol, version 4 (IMAP4).

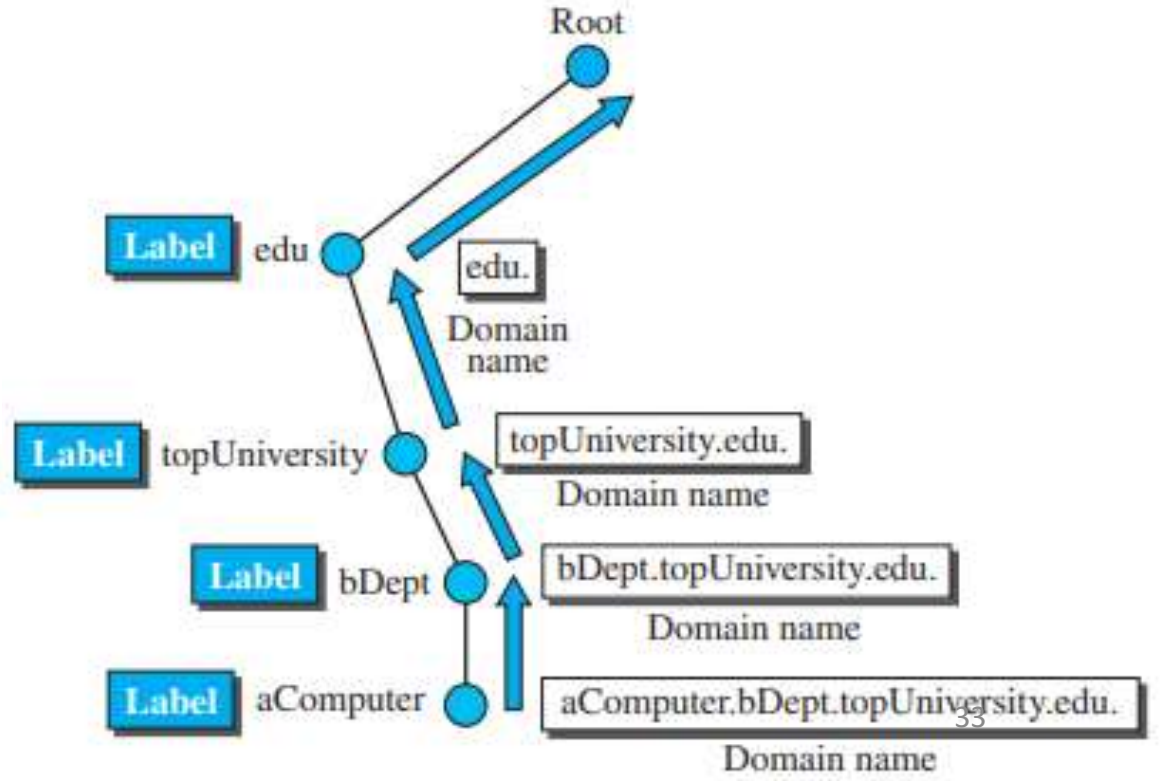
Domain Name System:

- Internet is so huge today, a central directory system cannot hold all the mapping of addresses.
- If the central computer fails, the whole communication network will collapse.
- A better solution is to distribute the information among many computers in the world.
- In this method, the host that needs mapping can contact the closest computer holding the needed information.
- This method is used by the Domain Name System (DNS).
- A name space that maps each address to a unique name can be organized in two ways: flat or hierarchical.

Name Space type:

- In a flat name space, a name is assigned to an address. A name in this space is a sequence of characters without structure.
- In a hierarchical name space, each name is made of several parts. The first part can define the nature of the organization, the second part can define the name of an organization, the third part can define departments in the organization, and so on.





Zone & Root Server:

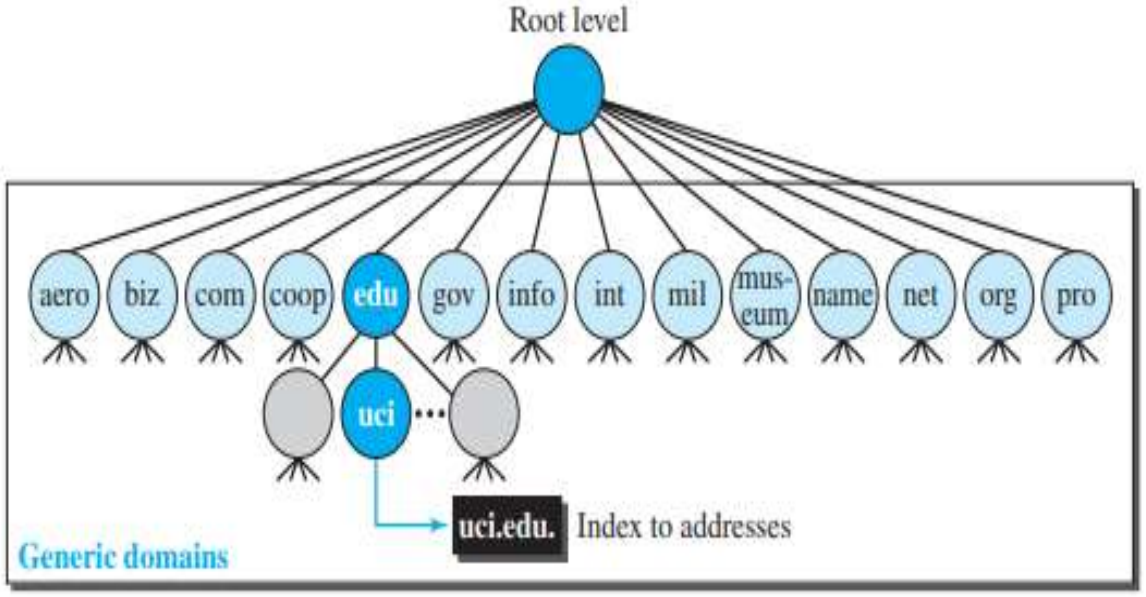
- Since the complete domain name hierarchy cannot be stored on a single server, it is divided among many servers.
- We can define a zone as a contiguous part of the entire tree. If a server accepts responsibility for a domain and does not divide the domain into smaller domains, the “domain” and the “zone” refer to the same thing.
- The server makes a database called a zone file and keeps all the information for every node under that domain.

- A root server is a server whose zone consists of the whole tree.
- A root server usually does not store any information about domains but delegates its authority to other servers, keeping references to those servers.
- There are several root servers, each covering the whole domain name space. The root servers are distributed all around the world.

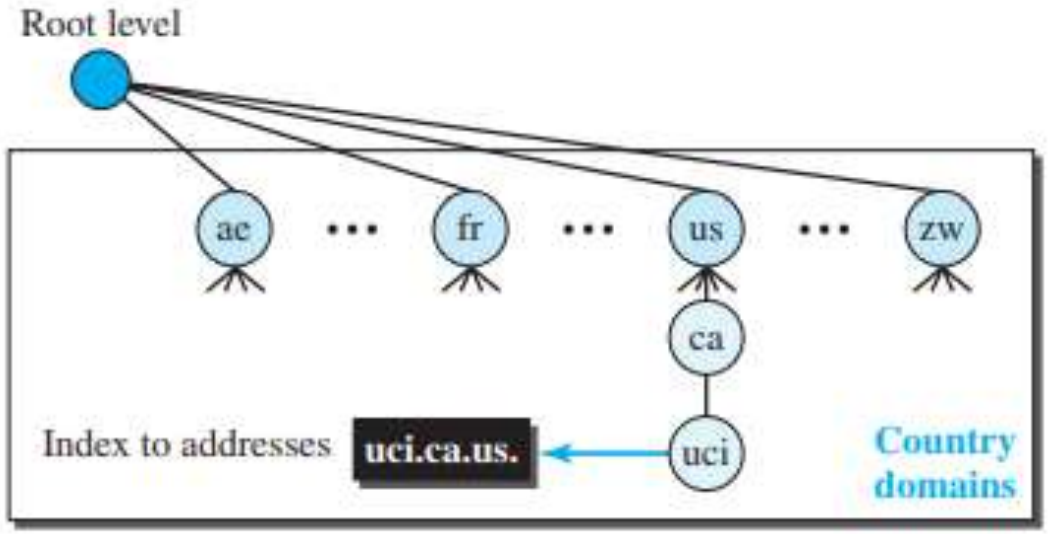
DNS in the Internet:

- DNS is a protocol that can be used in different platforms. In the Internet, the domain name space (tree) was originally divided into three different sections: generic domains, country domains, and the inverse domains (not used now).
- The generic domains define registered hosts according to their generic behavior. Each node in the tree defines a domain, which is an index to the domain name space database.

Label	*Description*	*Label*	*Description*
aero	Airlines and aerospace	**int**	International organizations
biz	Businesses or firms	**mil**	Military groups
com	Commercial organizations	**museum**	Museums
coop	Cooperative organizations	**name**	Personal names (individuals)
edu	Educational institutions	**net**	Network support centers
gov	Government institutions	**org**	Nonprofit organizations
info	Information service providers	**pro**	Professional organizations



- The country domains section uses two-character country abbreviations (e.g., us for United States). Second labels can be organizational, or they can be more specific national designations.



WWW:

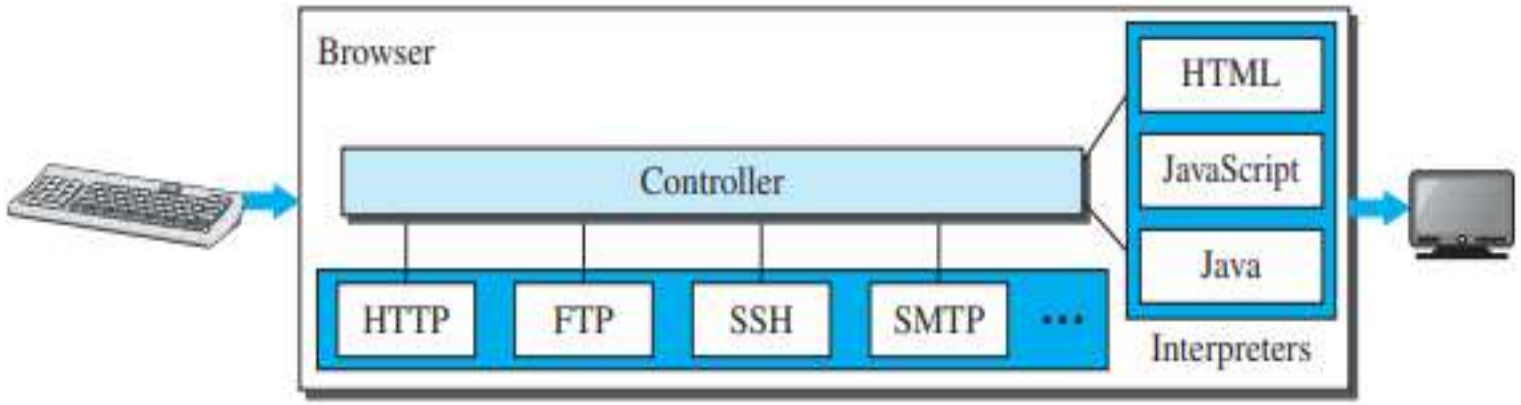
- The idea of Web was first proposed by Tim Berners-Lee in 1989.
- The Web today is a repository of information in which documents, called web pages are distributed all over the world and related documents are linked together.
- The linking of web-pages was achieved using a concept of **hypertext**.
- Today, the web-page contain text document, an image, audio or video files which is consider as a **hypermedia**.
- The **WWW** (World Wide Web) is a client-server service which is distributed over many locations called sites.

Web Client (Browser):

- Each browser consist of **three parts**: a controller, client protocols, and interpreters.

1. The **controller** receives input from the keyboard or mouse.
2. The controller uses one of the **interpreters** (such as HTML, Java or JavaScript) to display the document on the screen.
3. The **client protocol** can be one of the protocol such as HTTP or FTP.

- Some commercial browsers are Internet Explorer, Firefox, Netscape Navigator, etc..



Web Server:

- The web pages are stored at the server.
- Each time the document is sent to the client depending on the request arrive from the client.
- Server stores files in cache memory for the fast access.
- A server can answer more than one request at a time using multiprocessing or multithreading.
- Example of web servers are Microsoft Internet Information Server, Apache Server, etc…

URL: Uniform Resource Locator

- We need four identifiers to define the web page.

1. **Protocol** : It is require to access the web page. Most of the time the protocol is HTTP.
2. **Host** : It can be an IP address of the server or unique name given to it.
3. **Port** : It is a 16-bit integer which is predefined for the client-server application.
4. **Path** : It identifies the location and the name of the file available in OS

Web Documents:

- Documents in the WWW can be static, dynamic or active.

1. **Static documents** are fixed-content documents stored in a server.

- The contents of the documents can be changed but not by the user.

- Whenever any client access the document, a copy of the document is sent.

- This type of documents are prepared using HTML, XML and XHTML.

Web Documents:

2. **Dynamic document** is created by a web server whenever a browser request the document.

- Whenever a request arrives, the web sever runs an application program that creates the dynamic document.

- The CGI (Common Gateway Interface) was used to retrieve a dynamic document in the past, today's option include JSP, ASP, VB language, SQL and many more.

3. For many applications, we need a program or a script to be run at the client side. These are called **active documents**.

HTTP:

- The HTTP (HyperText Transfer Protocol) is used to define how the client-server programs can be written to retrieve web pages from the Web.
- HTTP client send the request and HTTP server returns a response.
- It uses the services of TCP which is connection-oriented and reliable protocol.
- There are two types of connections established in HTTP. (Non-persistent and Persistent)

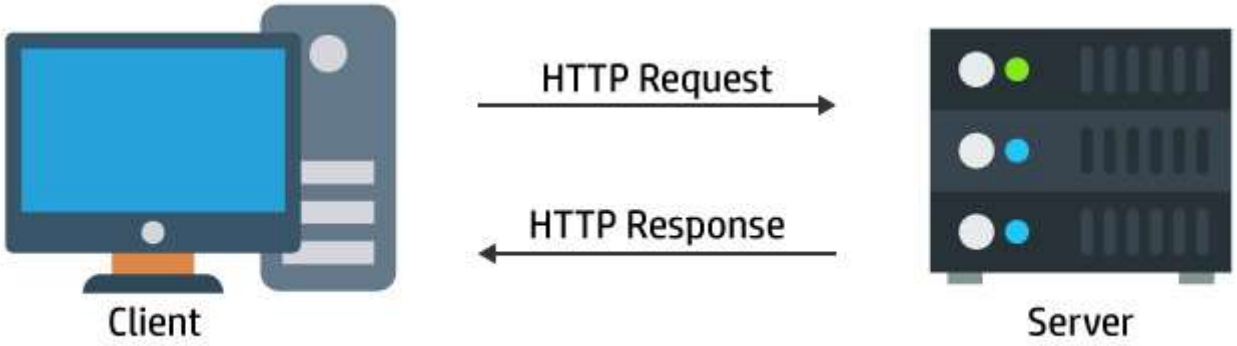


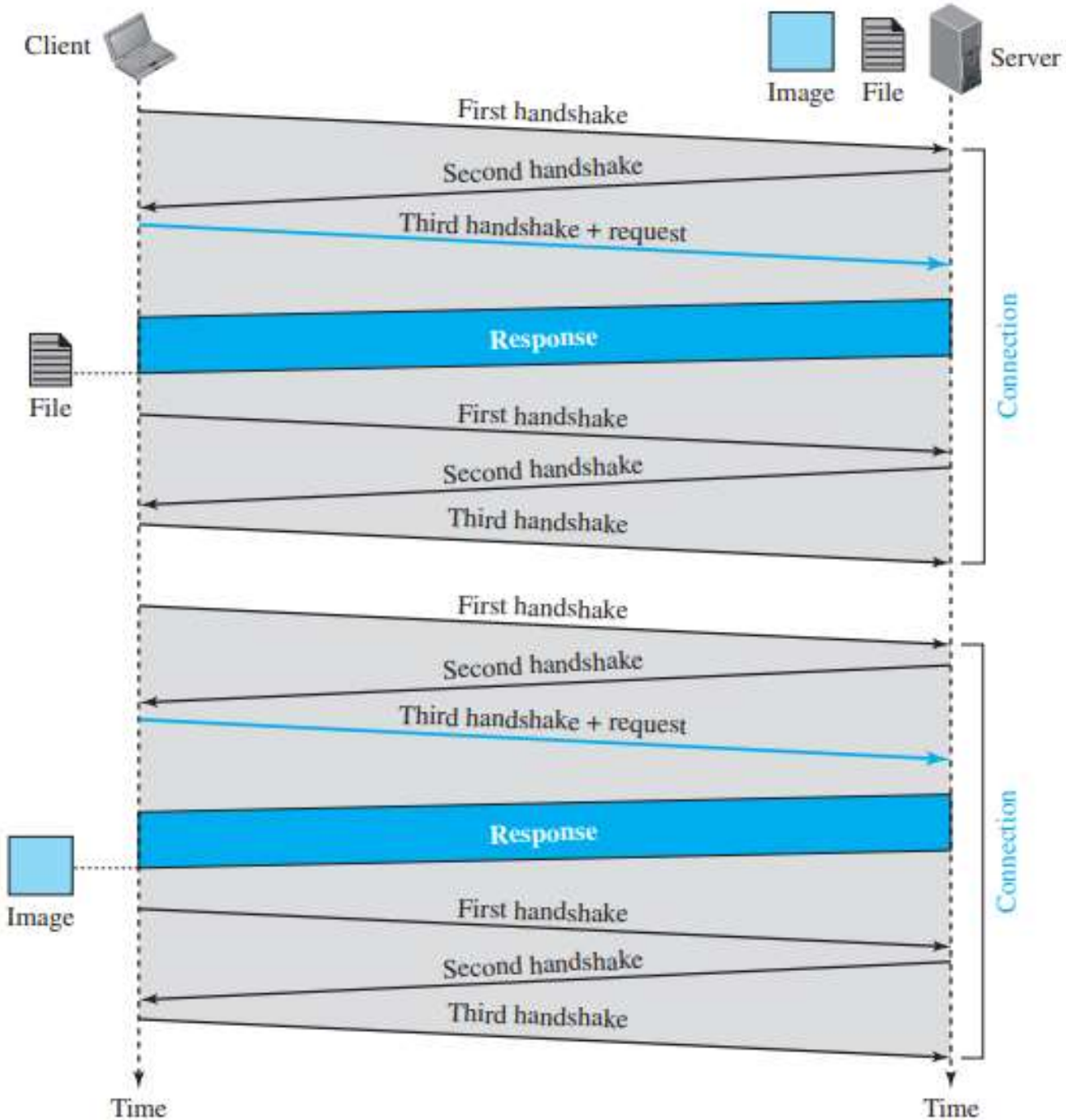
Fig: HTTP Protocol

HTTP:

- In a **non-persistent connection**, one TCP connection is made for each request/response.

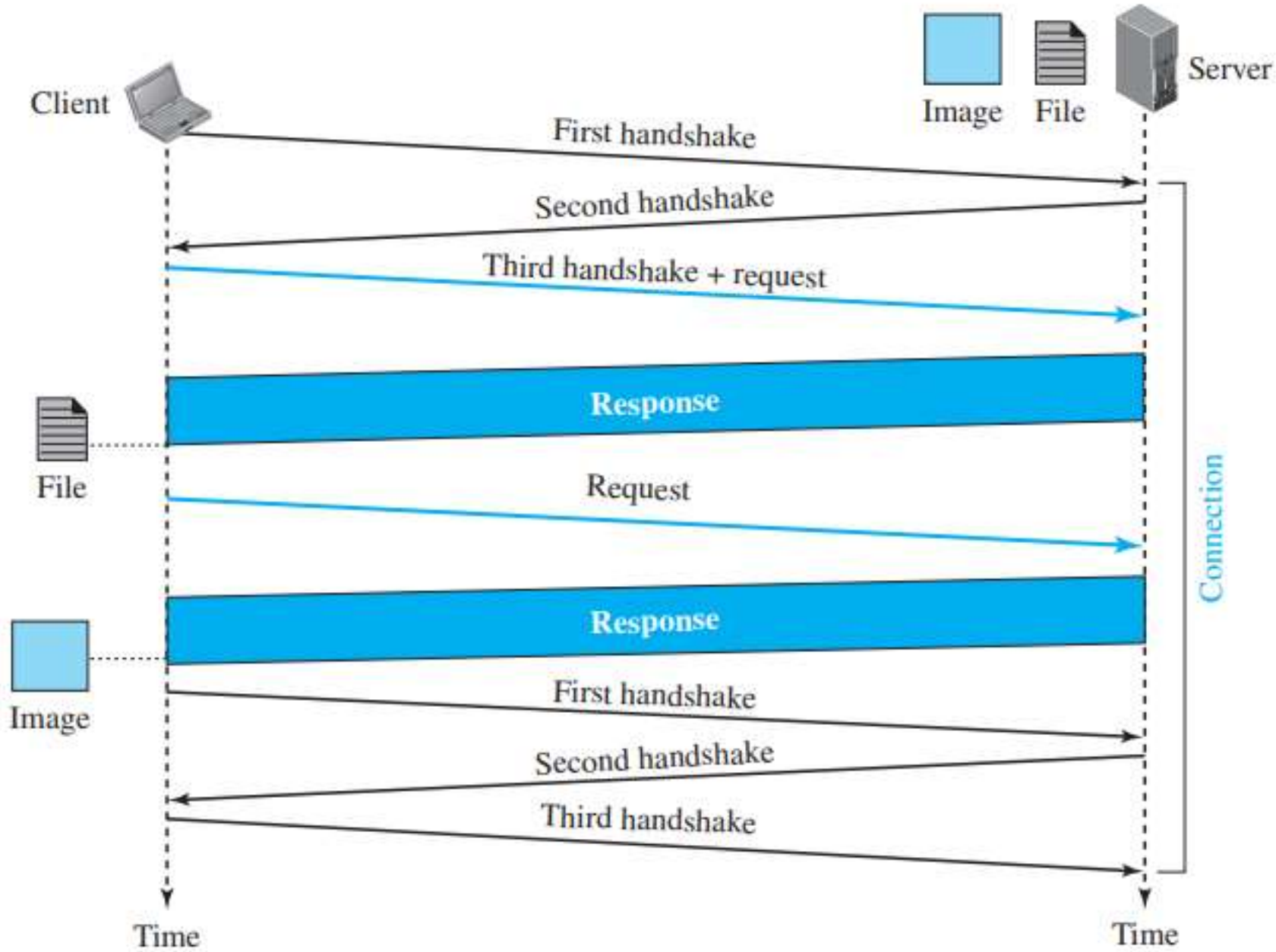
- Step 1: The client opens a TCP connection and sends a request.
- Step 2: The server send the response and close the connections.
- Step 3: The client reads the data until it encounters an end-of-file marker; it then closes the connection.

- If a file contains links to N different pictures in different files, the connection must be opened and closed N+1 times.

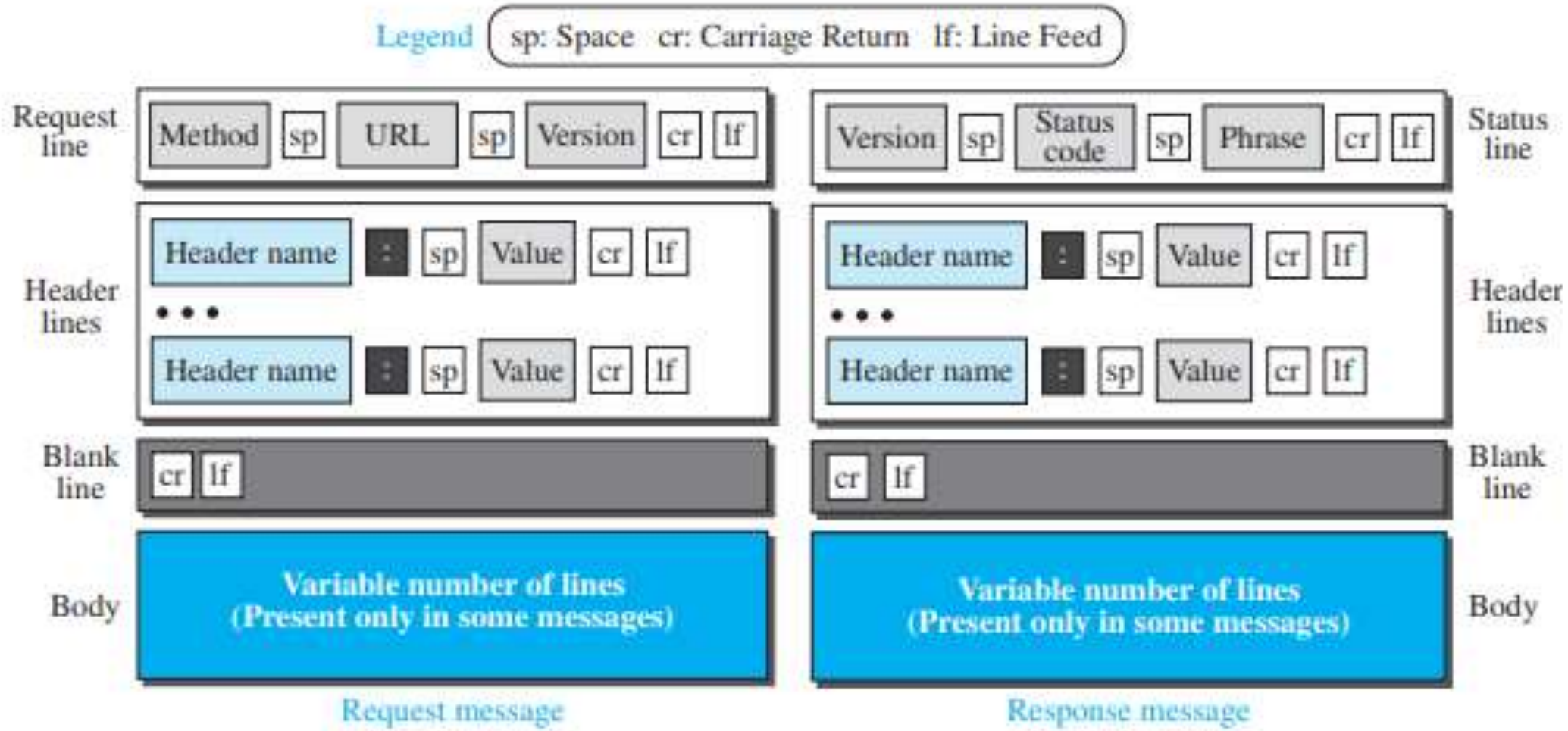

Client
Image
File
Server
First handshake
Second handshake
Third handshake + request
Response
File
First handshake
Second handshake
Third handshake
Connection
First handshake
Second handshake
Third handshake + request
Response
Image
First handshake
Second handshake
Third handshake
Connection
Time
Time

HTTP:

- In a **persistent connection**, the server leaves the connection open for more requests after sending a response.
- The server can close the connection at the request of a client or if a time-out has been reached.
- Only one set of buffers and variables need to be set for the connection at each site.
- The round trip time for connection establishment and connection termination is saved.


Client
Image
File
Server
First handshake
Second handshake
Third handshake + request
Response
File
Request
Response
Image
First handshake
Second handshake
Third handshake
Connection
Time
Time

HTTP message format:



HTTP message type:

1. Request Message:

- The first line in this message is request line which contain three fields method, URL and version.
  - **Method** field define the request type. (like, GET, POST, HEAD, DELETE, etc…)
  - **URL** defines the address and name of the corresponding web page.
  - **Version** gives the version of protocol i.e. 1.1 version.
- After this request line next line contain header line for additional information from client to server.
- Header names can be User-agent, Host, Cookie, Accept, Authorization, etc…

HTTP message type:

2. Response Message:

- The first line in this message is status line which contain three fields version, status code and phrase.
  - **Version** field defines the HTTP version 1.1
  - **Status code** field define the status of the request depending on the range like 100 range only informational, 200 range successful request, 300 range redirect the client, 400 range indicate an error at client and 500 range indicate an error at server.
  - The **phrase** explain the status code in text format.
- After the status line, next line is header line which contain additional information such as date, server, content-encoding, content-type, location, etc…

Web Caching : Proxy Servers

- HTTP supports proxy servers. It is a computer that keeps copies of responses to recent requests.
- The proxy server reduce the load on the original server, decreases traffic and improve latency.