Institute of Electrical and Electronic Engineering, University M'Hamed BOUGARA of Boumerdes

Chapter 2
Network Protocols and Communications

By: Hadjira BELAIDI

Objectives

After completing this chapter, you will be able to:

- ✓ Explain how rules are used to facilitate communication.
- ✓ Explain the role of protocols and standards organizations in facilitating interoperability in network communications.
- ✓ Explain how devices on a LAN access resources in a small to medium-sized business network.

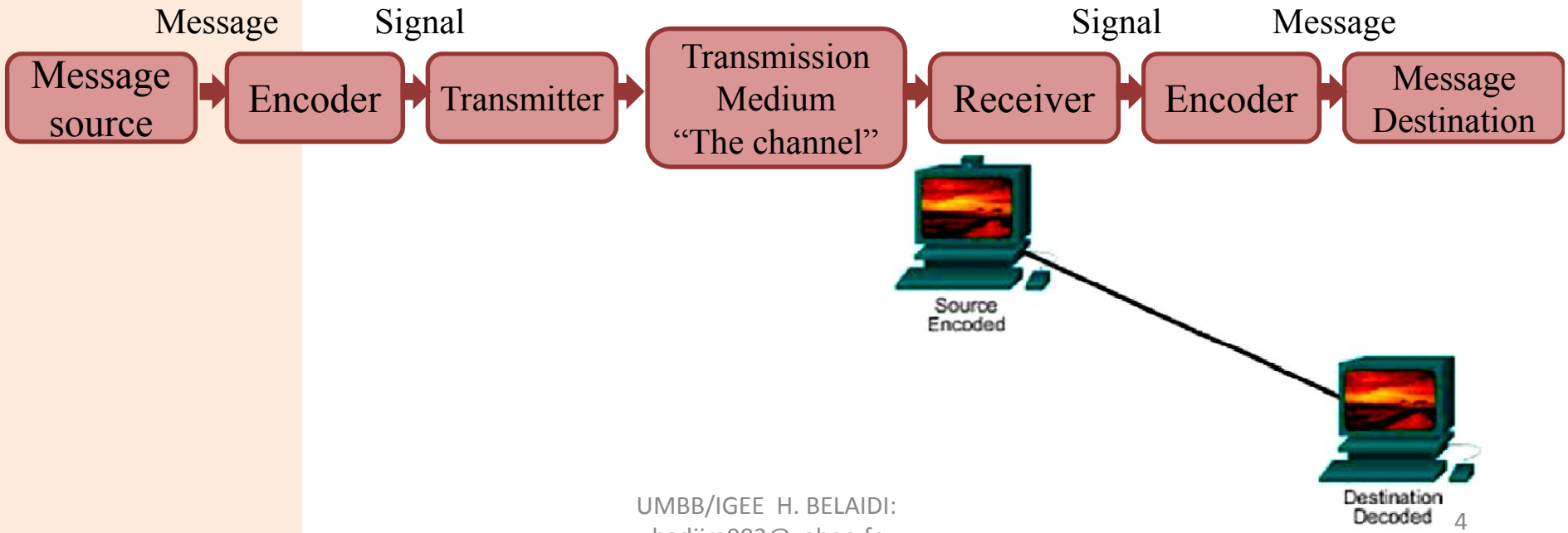
Chap2 Outlines

- Introduction
- Rules of Communication
- Network Protocols and Standards
- Moving Data in the Network

What is Communication?

Human communication

Computer communication



Example: Personal letter contains the following elements:

✓ Identifier of the recipient's location
✓ Identifier of the sender's location
✓ Salutation or greeting
✓ Recipient identifier
✓ The message content
✓ Source identifier
✓ End of message indicator

What is a protocol?

- In diplomatic circles, a protocol is the set of rules governing a conversation between people
- We have seen that the client and server carry on a machine-to-machine conversation
- A network protocol is the set of rules governing a conversation between a client and a server
- There are many protocols, HTTP is just one

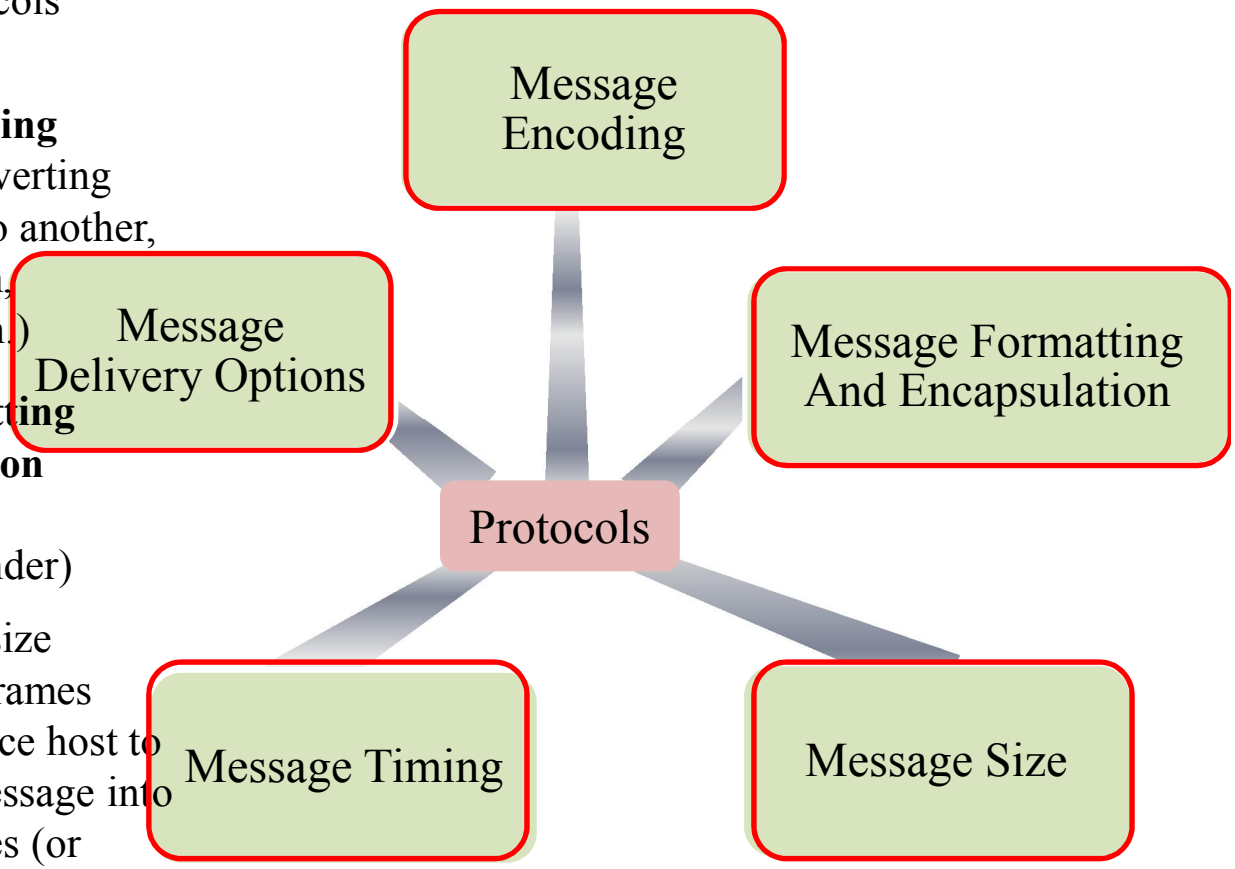
1. Rule Establishment

While there are many protocols, common computer protocols include:

Message encoding (process of converting information into another, acceptable form, for transmission.)

Message formatting and encapsulation (identifier of the recipient and sender)

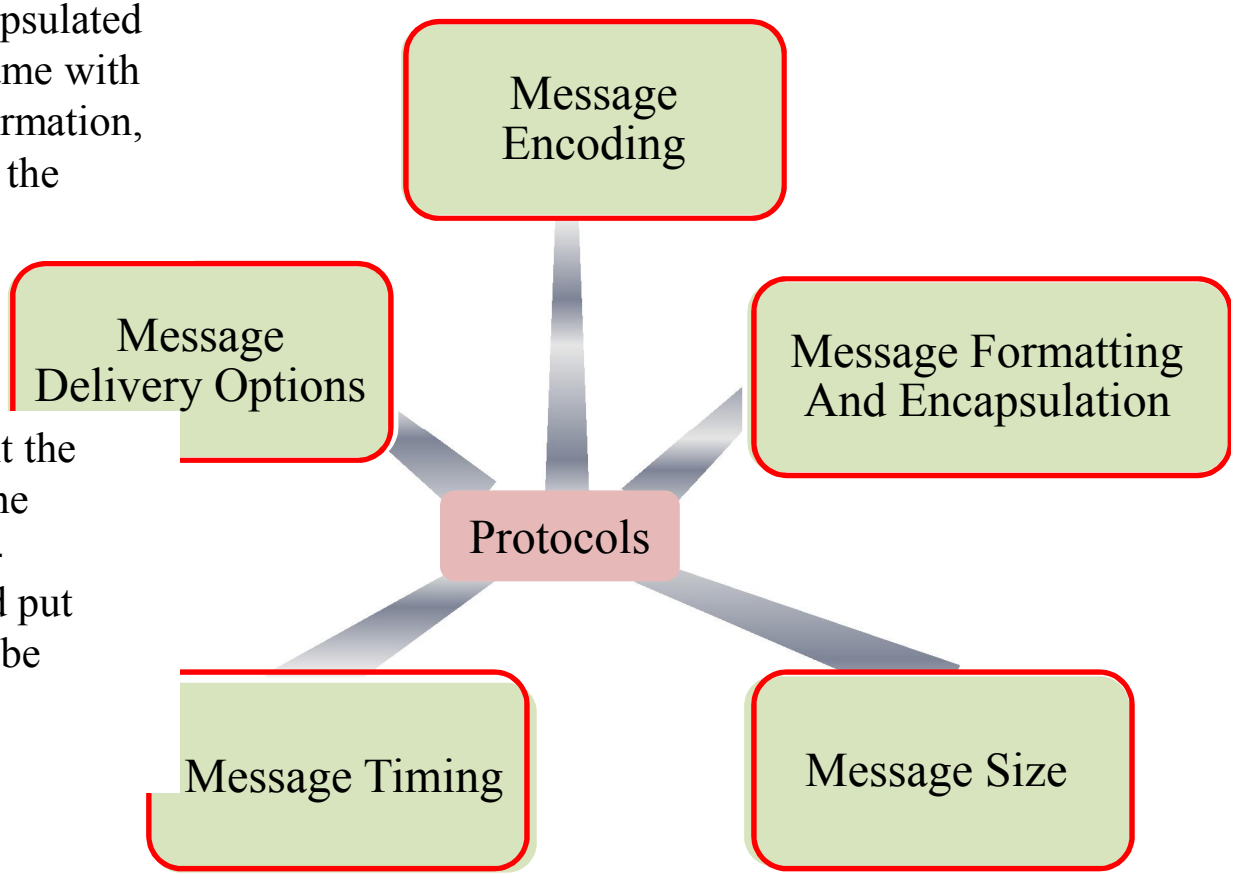
Message size (size restrictions of frames require the source host to break a long message into individual pieces (or segments) that meet both the minimum and maximum size requirements.).



1. Rule Establishment

Message size (Each segment is encapsulated in a separate frame with the address information, and is sent over the network).

Message size (At the receiving host, the messages are de-encapsulated and put back together to be processed and interpreted).

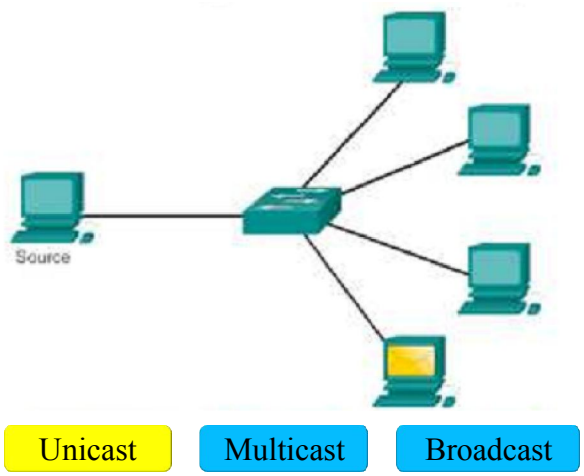


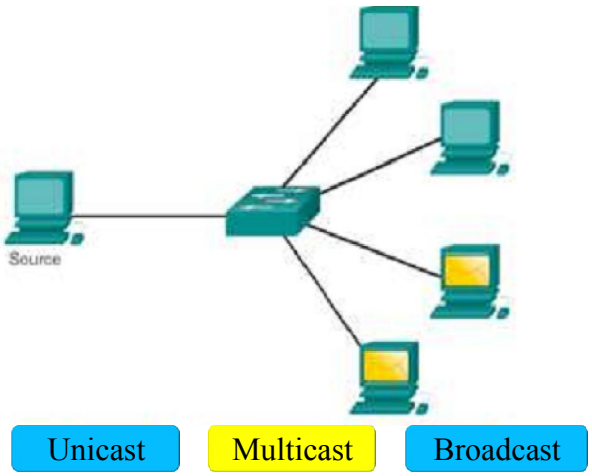
Message timing (Access Method, **Flow Control**, Response Timeout)

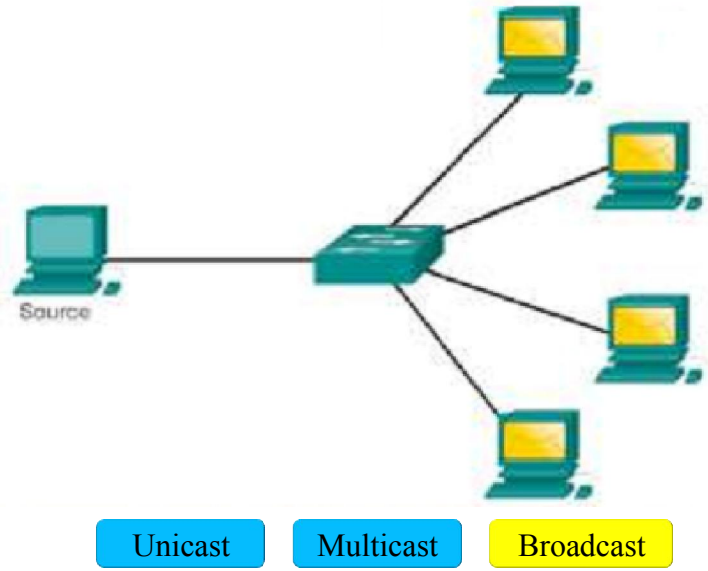
Message delivery options (Unicast, Multicast, Broadcast)

- Introduction
- Rules of Communication
- Network Protocols and Standards
- Moving Data in the Network

Message Delivery Options







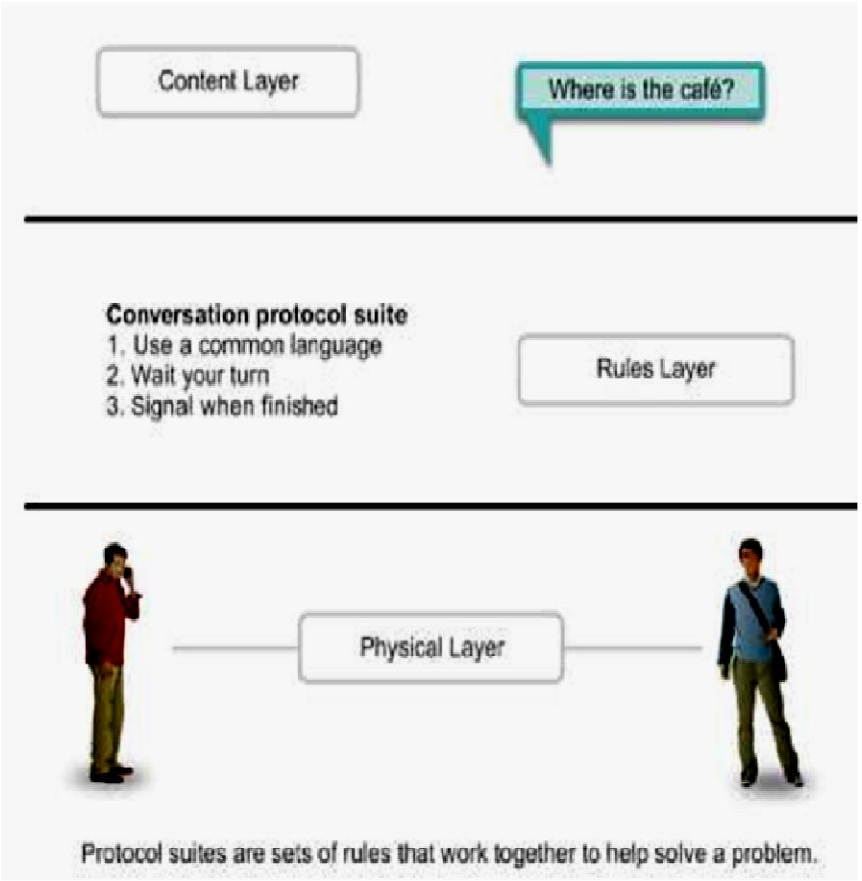
- Introduction
- Rules of Communication
- Network Protocols and Standards
- Moving Data in the Network

2. Network Protocols and Standards

Networking protocols define a common format and set of rules for exchanging messages between devices.

Some common networking protocols are IP, HTTP, and DHCP

Networking protocols define a common format and set of rules for exchanging messages between devices.

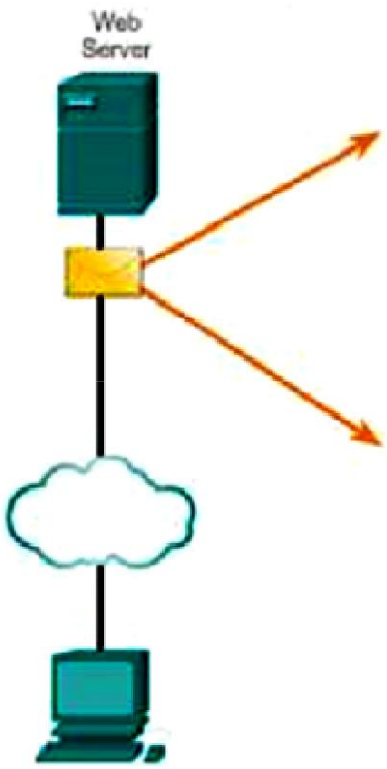


2.1. Network Protocols

- How the message is formatted or structured
- The process by which networking devices share information about pathways with other networks
- How and when error and system messages are passed between devices
- The setup and termination of data transfer sessions
- Proprietary protocols have their definition and operation controlled by one company or vendor.
- The TCP/IP protocol suite is an open standard, not a proprietary protocol.

- Introduction
- Rules of Communication
- Network Protocols and Standards
- Moving Data in the Network

2.2. Interaction of Protocols



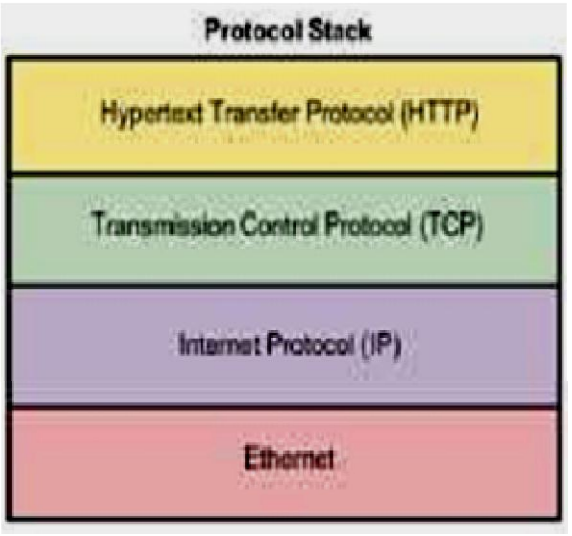
Layer Name

Application

Transport

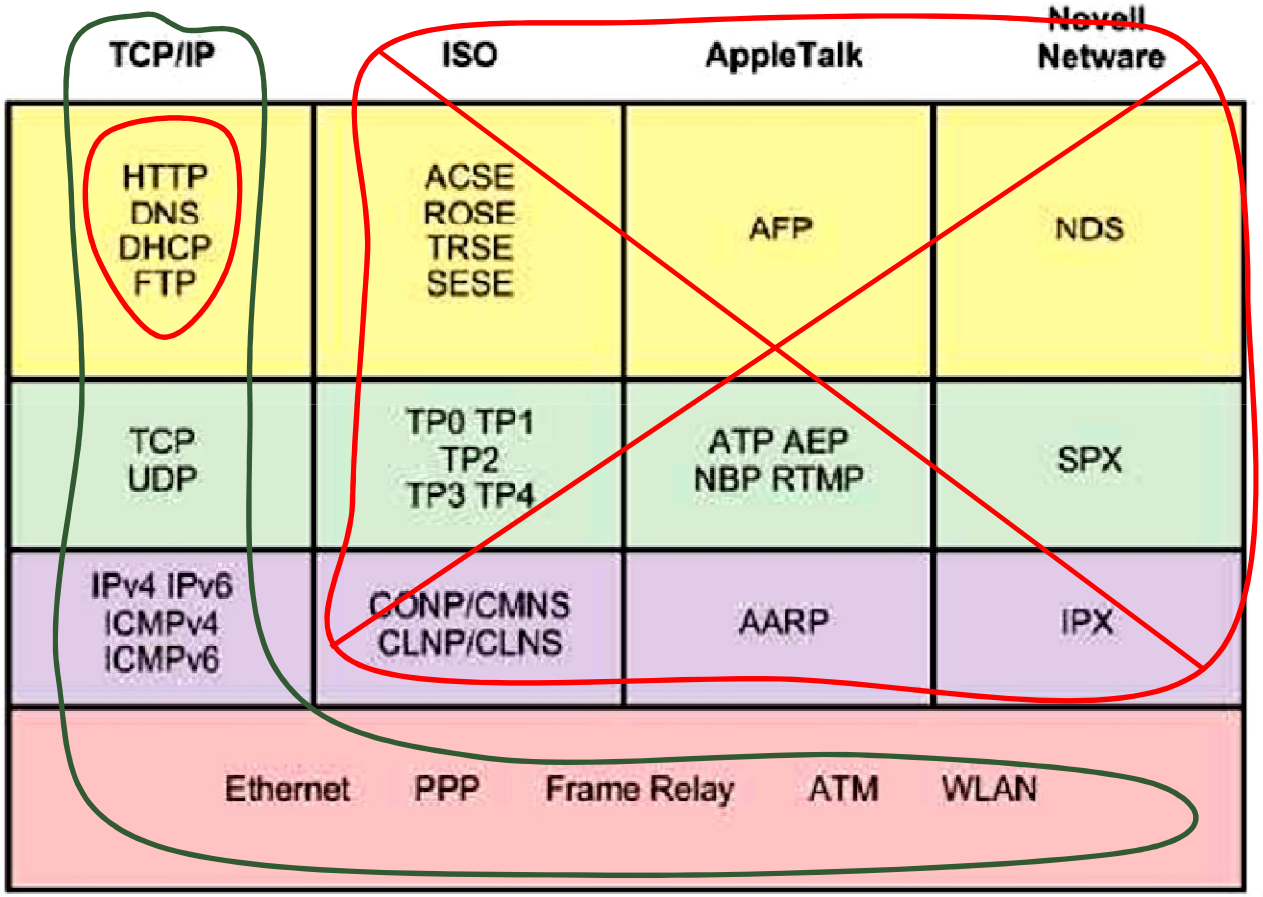
Internet

Network Access



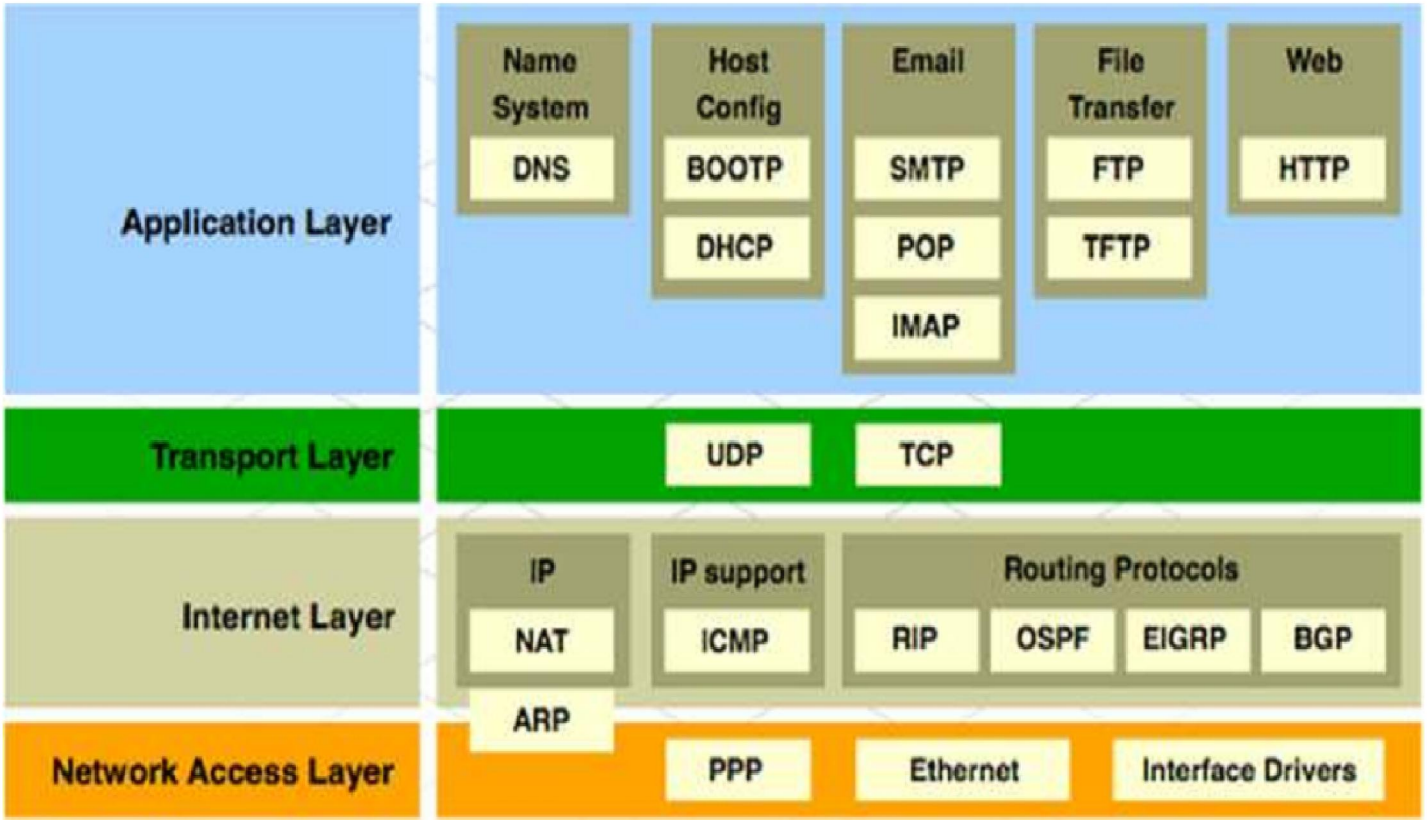
- Introduction
- Rules of Communication
- Network Protocols and Standards
- Moving Data in the Network

2.3. Protocol suits and Industry Standards



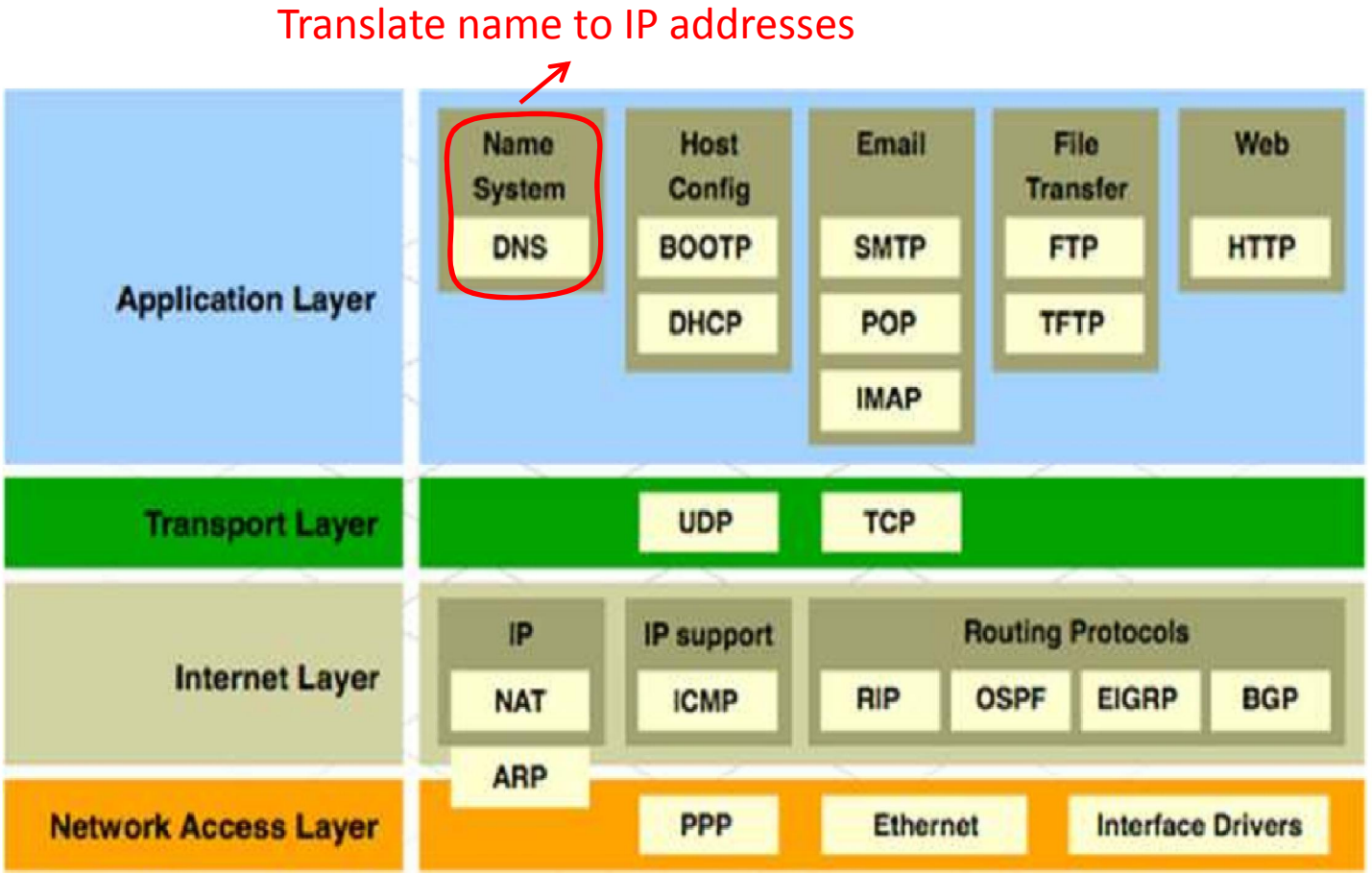
- Introduction
- Rules of Communication
- Network Protocols and Standards
- Moving Data in the Network

2.4. TCP/IP Protocol Suite and Communication



- Introduction
- Rules of Communication
- Network Protocols and Standards
- Moving Data in the Network

2.4. TCP/IP Protocol Suite and Communication



2.4. TCP/IP Protocol Suite and Communication

We refer to computers on the Internet (Internet hosts), by names like:

bpastudio.csudh.edu

These are called domain names or, if you want to be really geeky, “fully qualified domain names.”

The key point is that the name identifies a particular computer – no two hosts have the same domain name.

There are a limited number of top-level domains (TLDs), including:

- ✓ .edu, educational
- ✓ .com, commercial
- ✓ .gov, government
- ✓ .org, non profit
- ✓ .net, networking organizations

These are called "generic" TLDs.

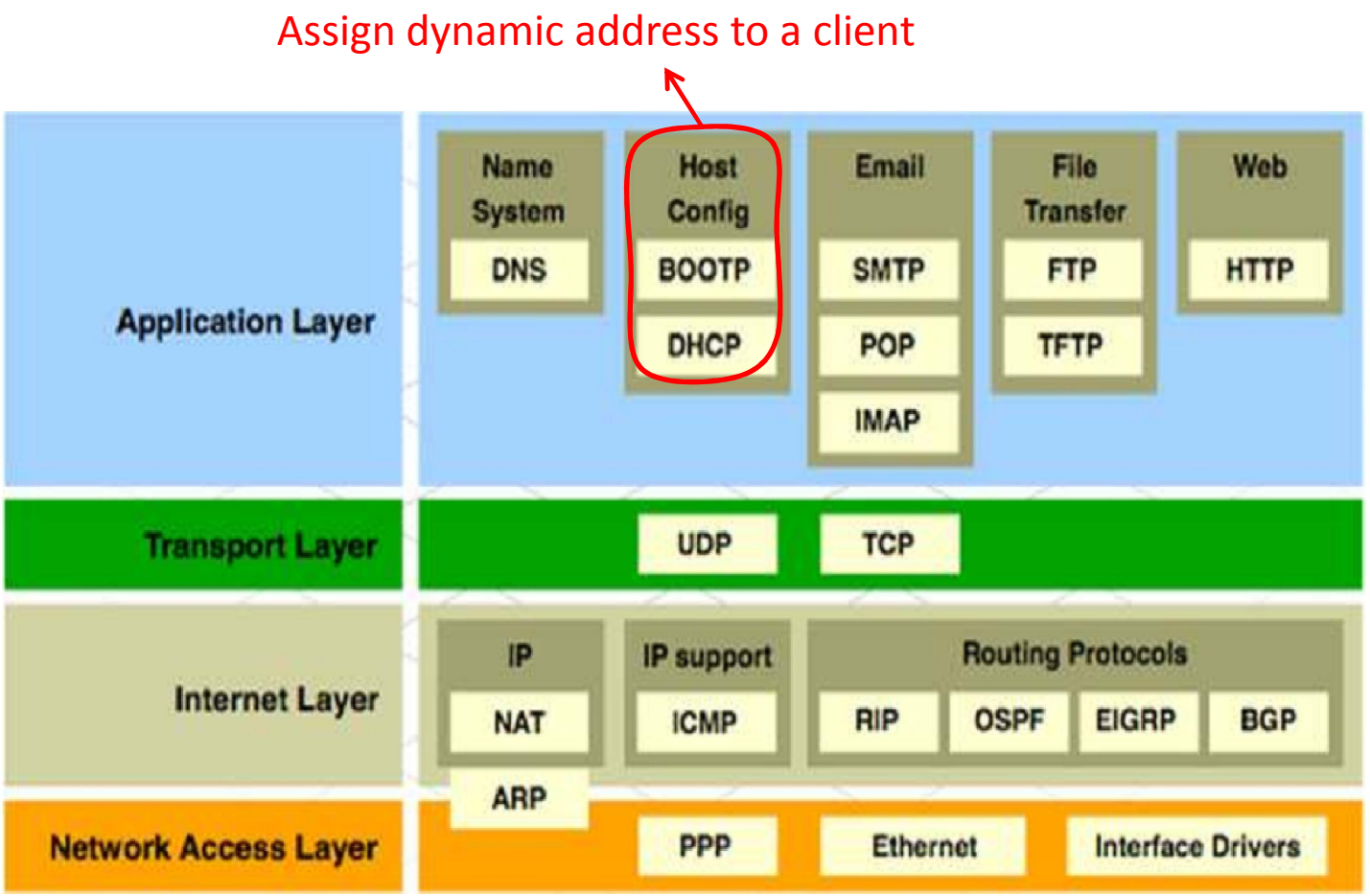
Some TLDs use a four-level hierarchy:

- http://www.google.co.uk/
- http://www.unam.edu.mx/
- http://www.ox.ac.uk/
- http://www.google.com.mx/

…..

- Introduction
- Rules of Communication
- Network Protocols and Standards
- Moving Data in the Network

2.4. TCP/IP Protocol Suite and Communication



2.4. TCP/IP Protocol Suite and Communication

The Bootstrap Protocol (BOOTP) is a client/server protocol that configures a diskless computer or a computer that is booted for the first time. BOOTP provides the

•IP address
•net mask
•the address of a default router
•the address of a name server.

BOOTP is static. When a client workstation asks for the above info, it is retrieved from a fixed table. Every time the client asks for the info, it gets the same results.

A diskless workstation or PC on a *local-area network (LAN)* is a computer system that does not have its own disk. Instead, it stores files on a network file server.

2.4. TCP/IP Protocol Suite and Communication

The Dynamic Host Configuration Protocol (DHCP) provides static and dynamic address allocation that can be manual or automatic.

Bootp is static, but DHCP is dynamic (but it can also be static).

DHCP has a pool of available addresses. When a request arrives, DHCP pulls out the next available address and assigns it to the client for a negotiable time period.

When a request comes in from a client, the DHCP server first consults the static table.

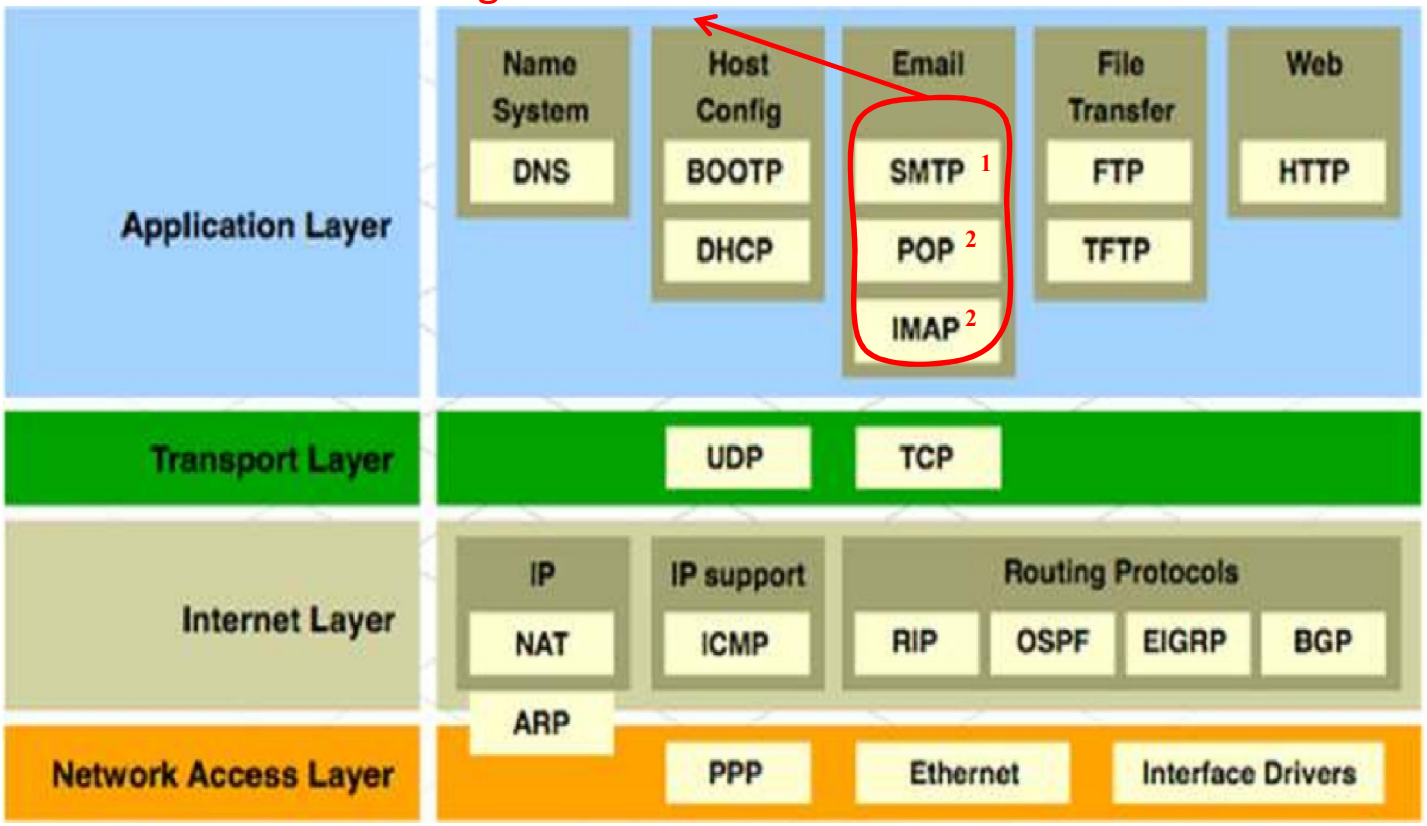
DHCP is great when devices and IP addresses change.

The DHCP packet format is almost identical to the BOOTP packet format (in order to be compatible with BOOTP). Only difference is 1-bit flag.

- Introduction
- Rules of Communication
- Network Protocols and Standards
- Moving Data in the Network

2.4. TCP/IP Protocol Suite and Communication

Protocols used for (1)sending and
(2)receiving e-mails

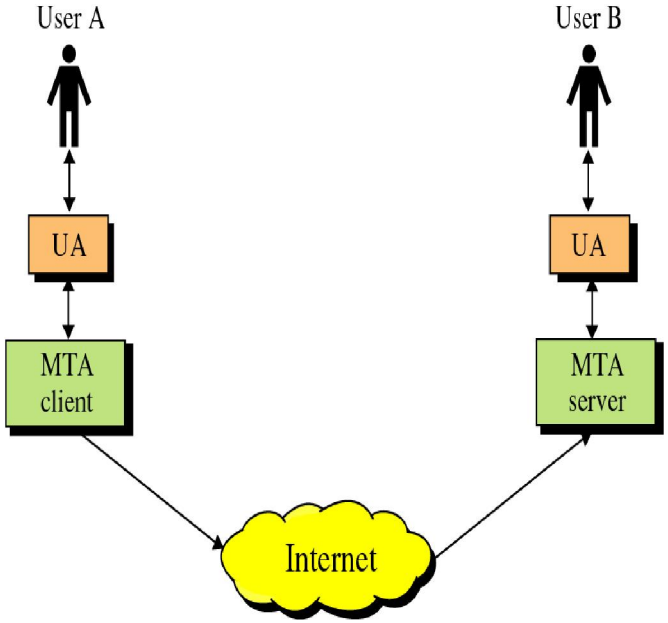


2.4. TCP/IP Protocol Suite and Communication

Basic SMTP Architecture

SMTP clients and servers have two main components:

- User Agents (UA): It prepares a message and encloses in an envelope.
- Mail Transfer Agents (MTA): It transfers the mail across the internet.



2.4. TCP/IP Protocol Suite and Communication

- Introduction
- Rules of Communication
- Network Protocols and Standards
- Moving Data in the Network

POP vs IMAP

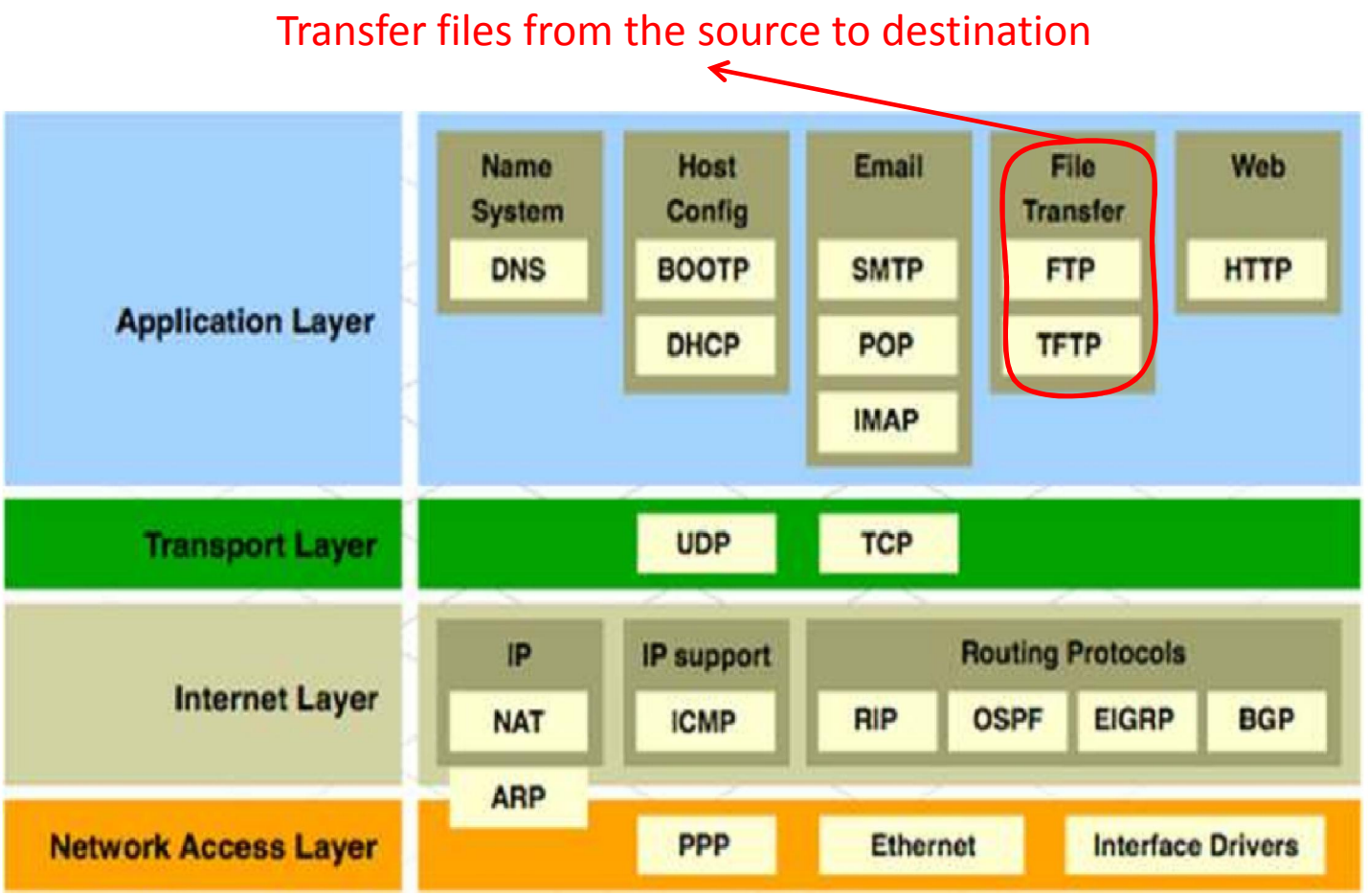
- With IMAP, all your mail stays on the server in multiple folders, some of which you have created. This enables you to connect to any computer and see all your mail and mail folders. In general, IMAP is great if you have a dedicated connection to the Internet or you like to check your mail from various locations.

- With POP3 you only have one folder, the Inbox folder. When you open your mailbox, new mail is moved from the host server and saved on your computer. If you want to be able to see your old mail messages, you have to go back to the computer where you last opened your mail.

- With POP3 "leave mail on server" only your email messages are on the server, but with IMAP your email folders are also on the server.

- Introduction
- Rules of Communication
- Network Protocols and Standards
- Moving Data in the Network

2.4. TCP/IP Protocol Suite and Communication



2.4. TCP/IP Protocol Suite and Communication

- Introduction
- Rules of Communication
- Network Protocols and Standards
- Moving Data in the Network

FTP

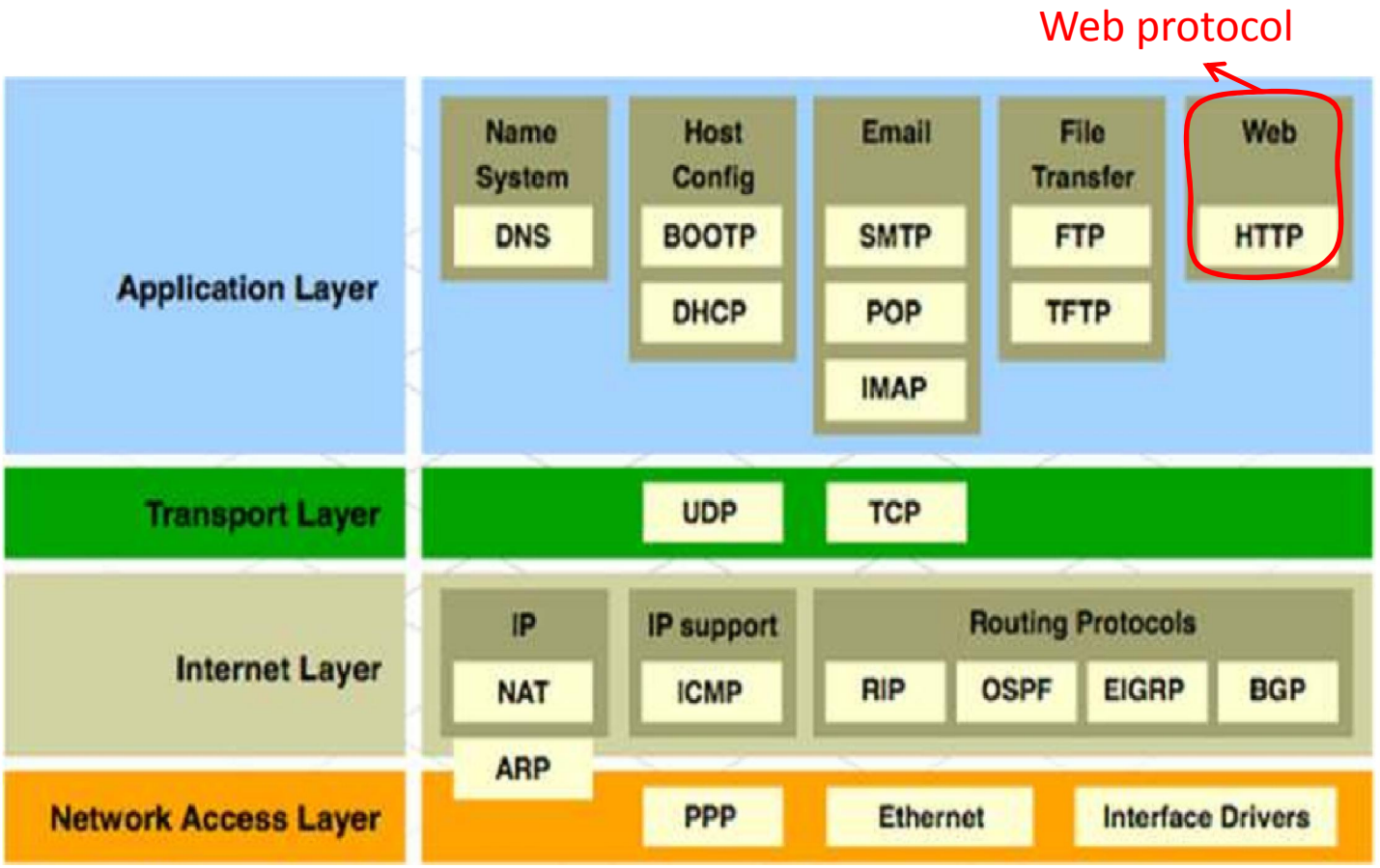
- FTP (File Transfer Protocol) is a network protocol used to transfer files from one computer to another over a TCP network.
- FTP uses two TCP ports: port 20 for sending data and port 21 for sending control commands.
- FTP can use authentication, but all data is sent in clear text, including usernames and passwords.

TFTP

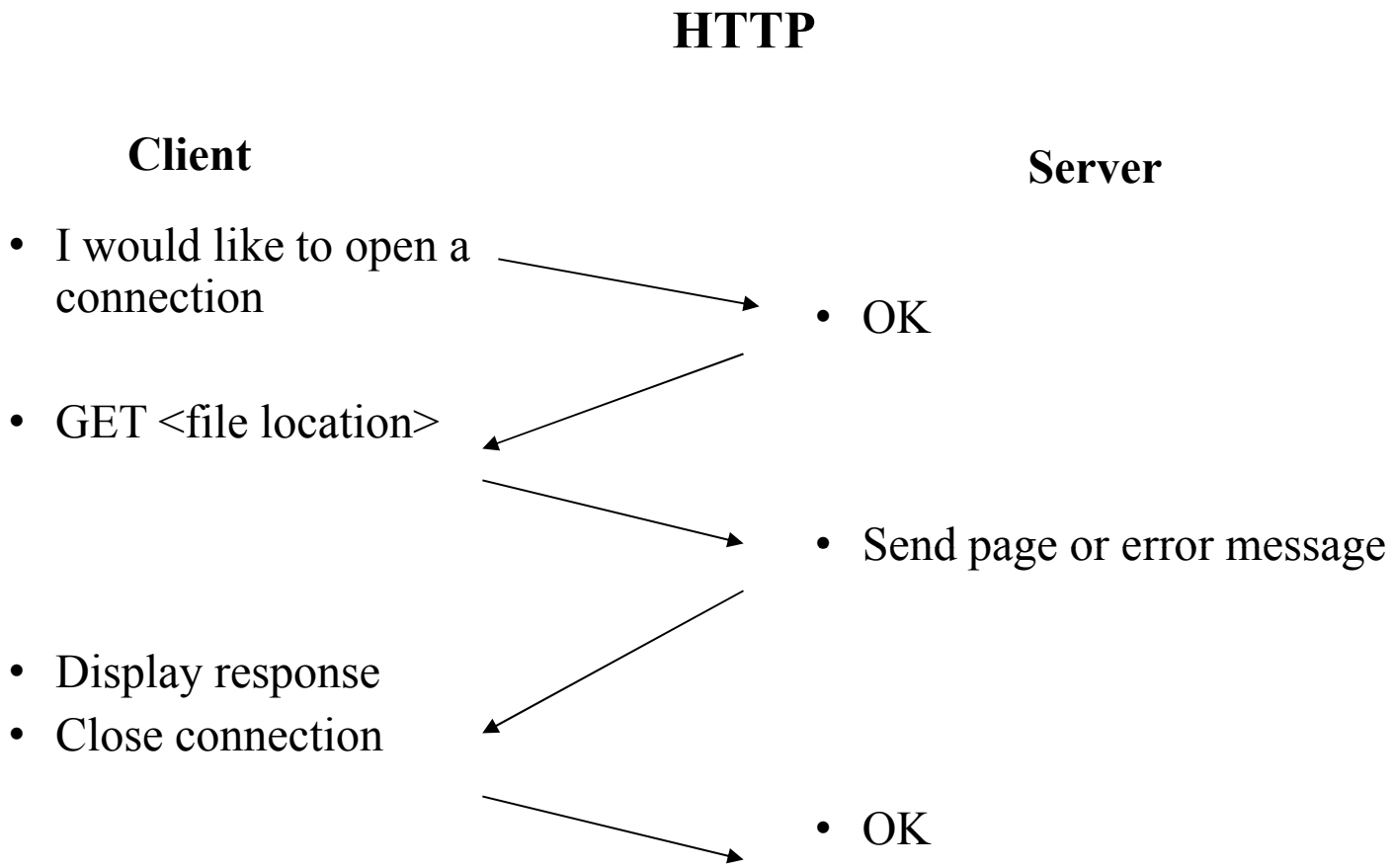
- TFTP (Trivial File Protocol) is a network protocol used to transfer files between remote machines.
- It is a simple version of FTP, lacking some of the more advanced features FTP offers, but requiring less resources than FTP.
- It uses UDP port 69 for communication.
- TFTP doesn't support user authentication and sends all data in clear text.

- Introduction
- Rules of Communication
- Network Protocols and Standards
- Moving Data in the Network

2.4. TCP/IP Protocol Suite and Communication



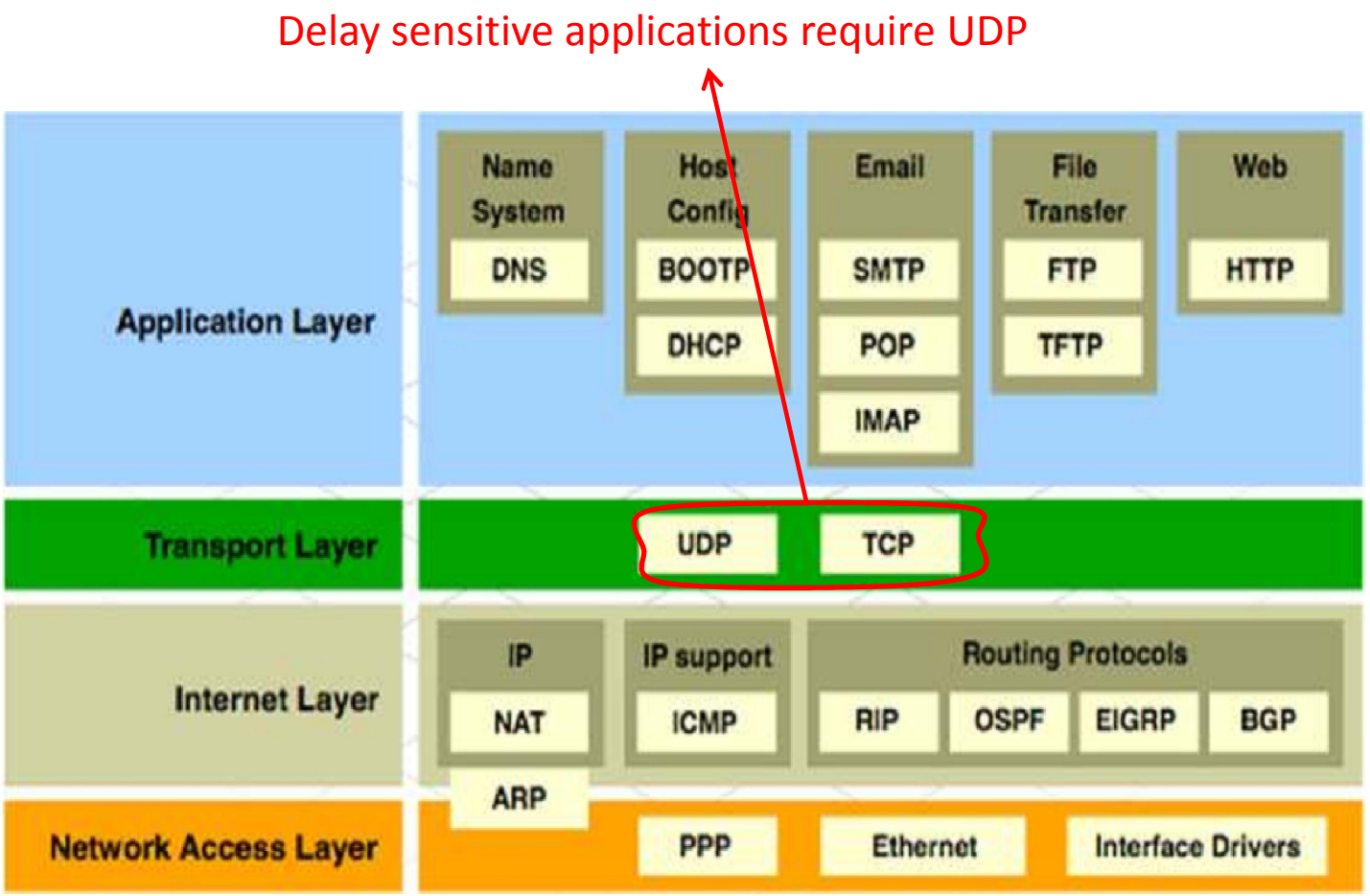
2.4. TCP/IP Protocol Suite and Communication



HTTP is the set of rules governing the format and content of the conversation between a Web client and server

- Introduction
- Rules of Communication
- Network Protocols and Standards
- Moving Data in the Network

2.4. TCP/IP Protocol Suite and Communication



2.4. TCP/IP Protocol Suite and Communication

UDP—User Datagram Protocol

- An unreliable, connectionless transport layer protocol
- Two additional functions beyond IP:
  - Demultiplexing: deliver to different upper layer entities such as DNS, RTP, SNMP based on the destination port # in the header. i.e., UDP can support multiple applications in the same end systems.
  - (Optionally) check the integrity of entire UDP. (recall IP only checks the integrity of IP header.)

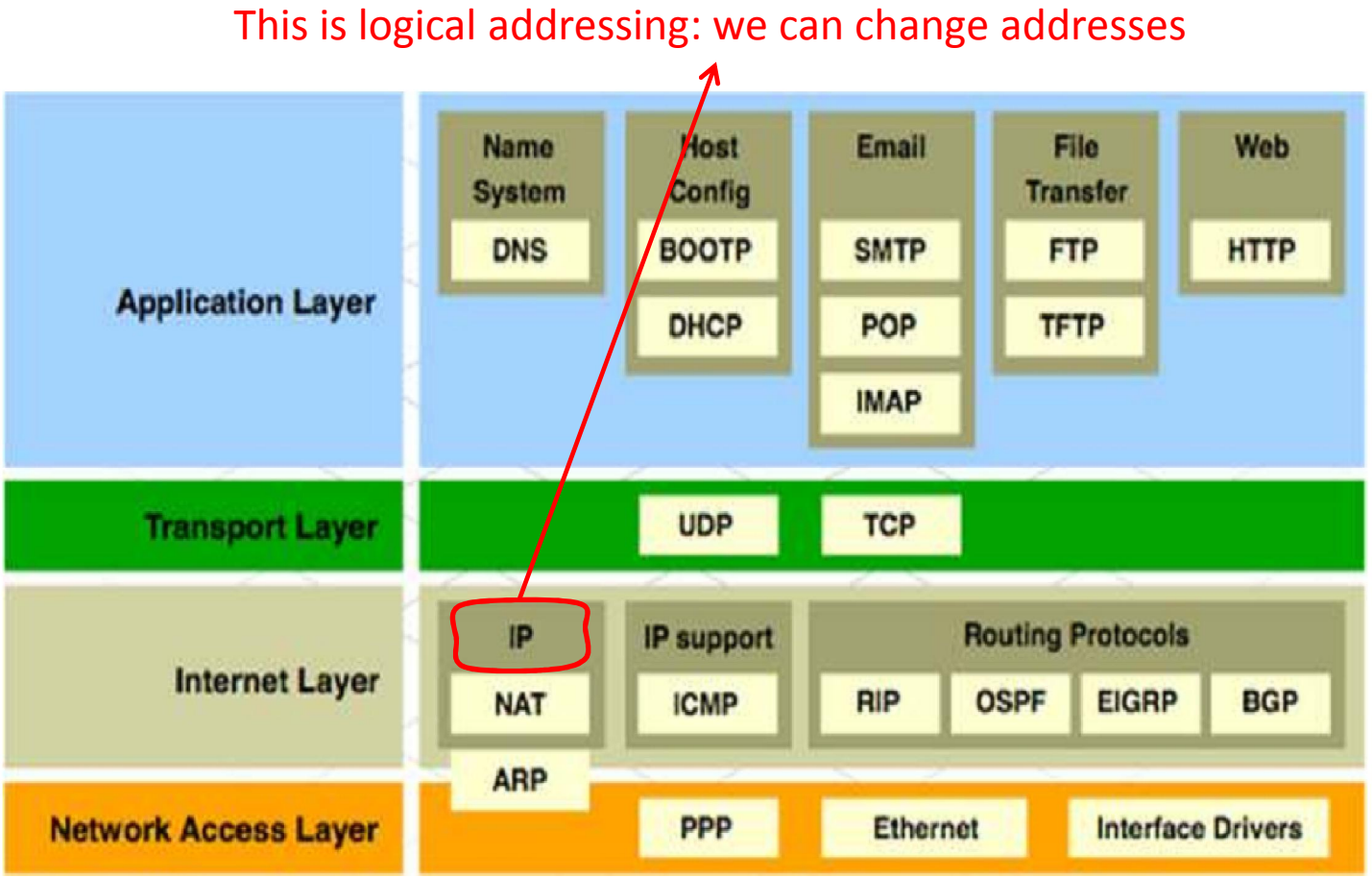
2.4. TCP/IP Protocol Suite and Communication

TCP—transmission control protocol

- TCP functionality
  - Provides connection-oriented, reliable, in-sequence, byte-stream service
  - Provides a logical full-duplex (two way) connection
  - Provides flow-control by *advertised window*.
  - Provides congestion control by *congestion window.*
  - Support multiple applications in the same end systems.
- TCP establishes connection by *setting up variables* that are used in two peer TCP entities. Most important variables are *initial sequence numbers*.
- TCP terminates each direction of connection independently, allowing data to continue flowing in one direction after closing the other direction.
- TCP does not keep messages boundaries and treats data as byte stream. e.g, when source sends out two chunks of data with length 400 and 600 bytes, the receiver may receive data in chunks of 300, 400, and 300 bytes, or 100 and 900 bytes.

- Introduction
- Rules of Communication
- Network Protocols and Standards
- Moving Data in the Network

2.4. TCP/IP Protocol Suite and Communication



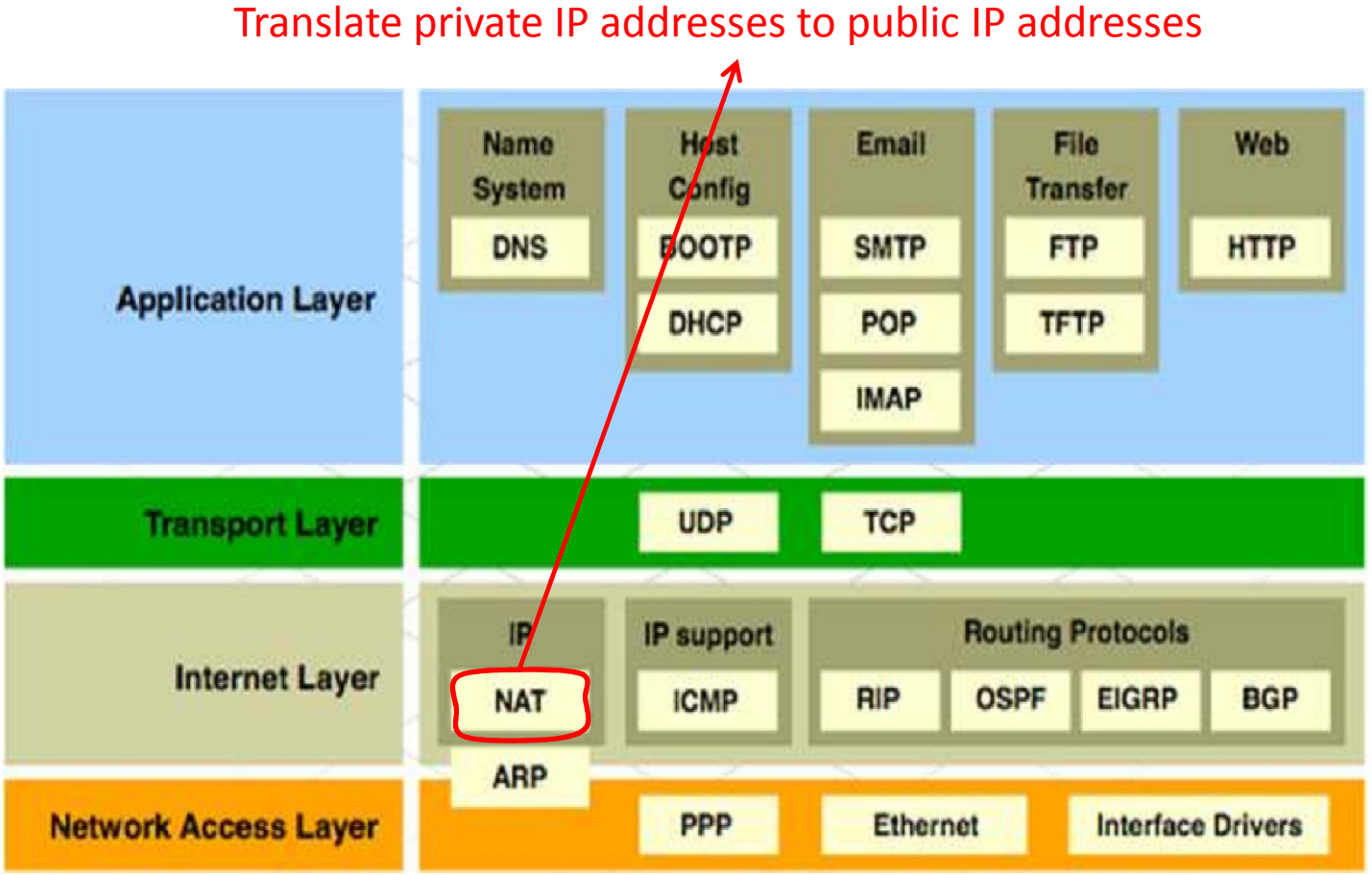
2.4. TCP/IP Protocol Suite and Communication

IP— Internet Protocol

- A way to identify machines on a network
- A unique identifier
- Used to connect to another computer
- Allows transfers of files and e-mail
- IP addresses consist of four sections
- Each section is 8 bits long
- Each section can range from 0 to 255
- Written, for example, 128.35.0.72

- Introduction
- Rules of Communication
- Network Protocols and Standards
- Moving Data in the Network

2.4. TCP/IP Protocol Suite and Communication



- Introduction
- Rules of Communication
- Network Protocols and Standards
- Moving Data in the Network

2.4. TCP/IP Protocol Suite and Communication

NAT - Network Address Translation

Private IP network is an IP network that is not directly connected to the Internet

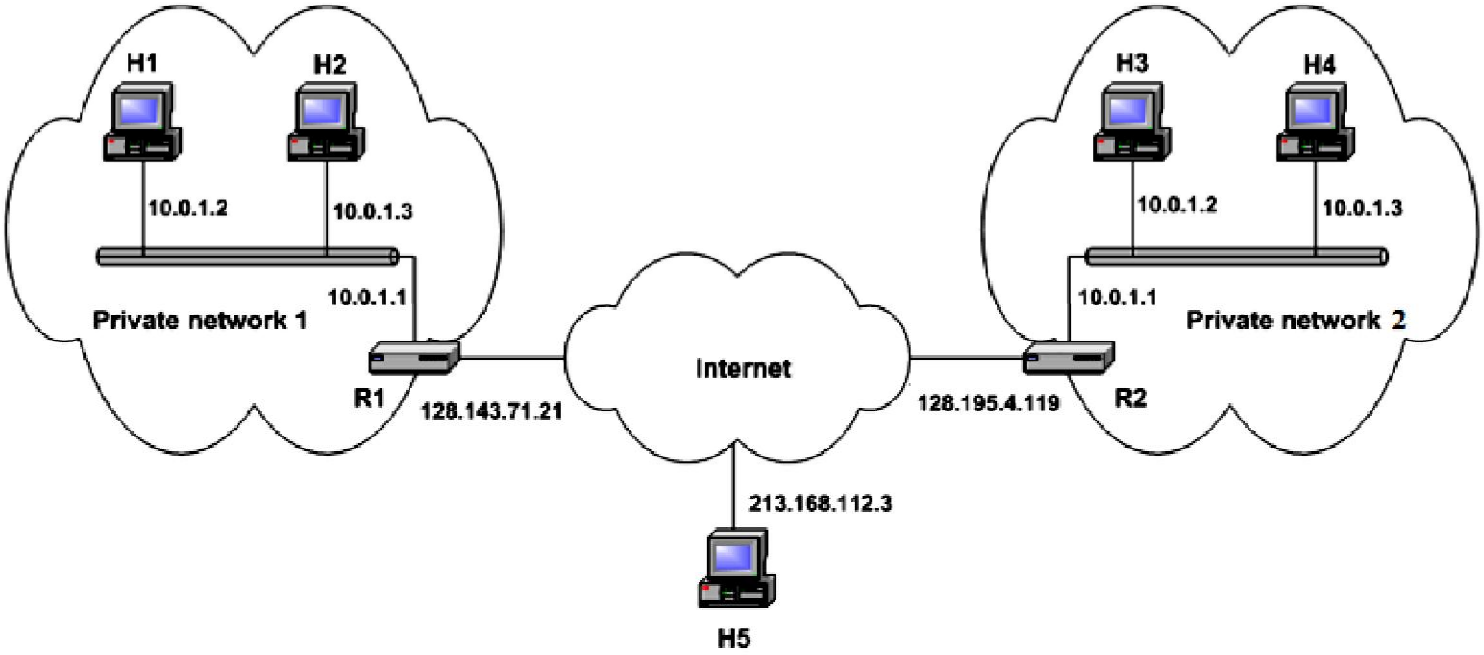
IP addresses in a private network can be assigned arbitrarily.

Not registered and not guaranteed to be globally unique

2.4. TCP/IP Protocol Suite and Communication

- Introduction
- Rules of Communication
- Network Protocols and Standards
- Moving Data in the Network

NAT - Network Address Translation



2.4. TCP/IP Protocol Suite and Communication

NAT - Network Address Translation

A short term solution to the problem of the depletion of IP addresses

Long term solution is IP v6

CIDR (Classless InterDomain Routing) is a possible short term solution

NAT is another

NAT is a way to conserve IP addresses

Can be used to hide a number of hosts behind a single IP address

Uses private addresses:

10.0.0.0-10.255.255.255,
172.16.0.0-172.32.255.255 or
192.168.0.0-192.168.255.255

2.4. TCP/IP Protocol Suite and Communication

NAT - Network Address Translation

NAT is a router function where IP addresses (and possibly port numbers) of IP datagrams are replaced at the boundary of a private network.

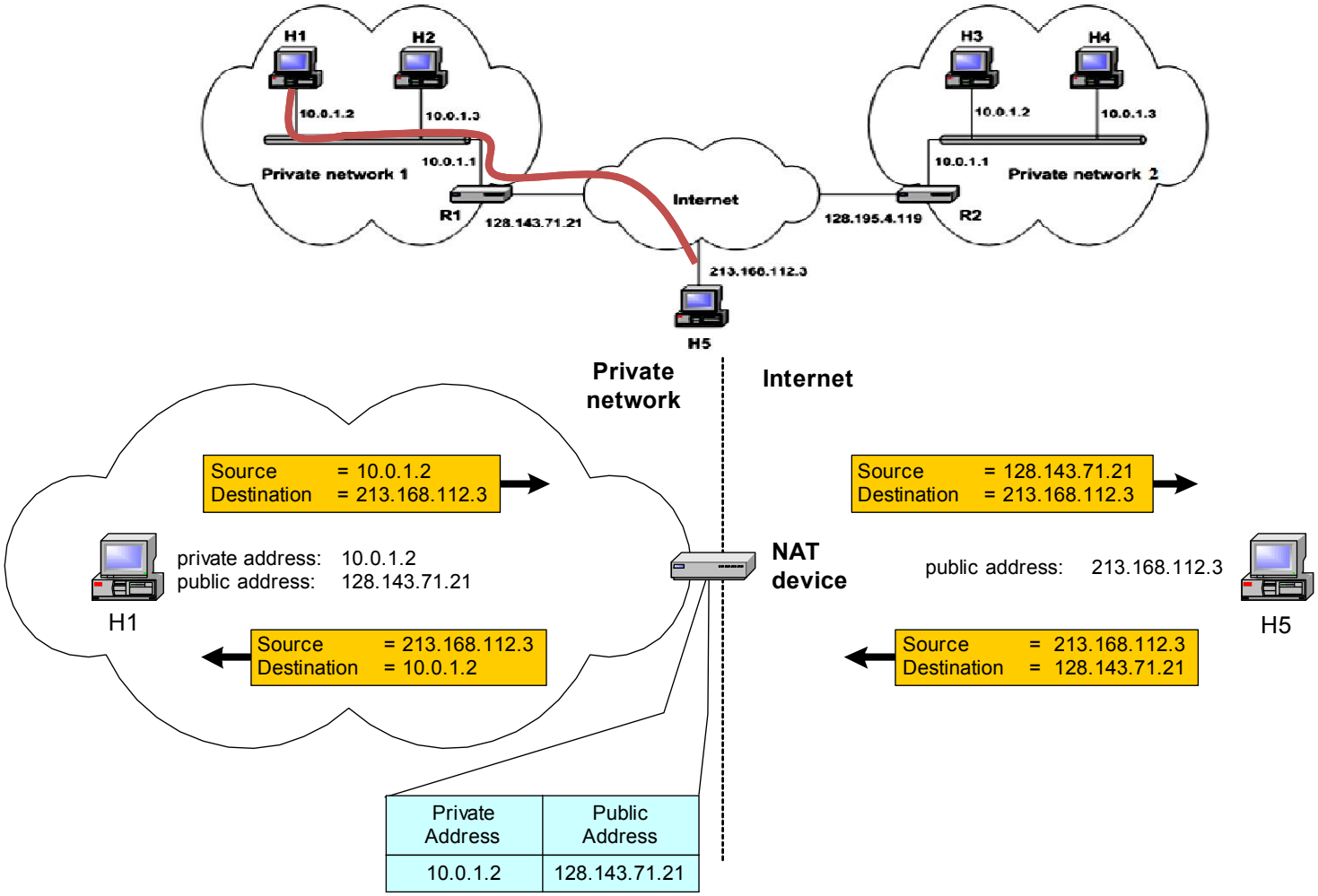
NAT is a method that enables hosts on private networks to communicate with hosts on the Internet.

NAT is run on routers that connect private networks to the public Internet, to replace the IP address-port pair of an IP packet with another IP address-port pair.

2.4. TCP/IP Protocol Suite and Communication

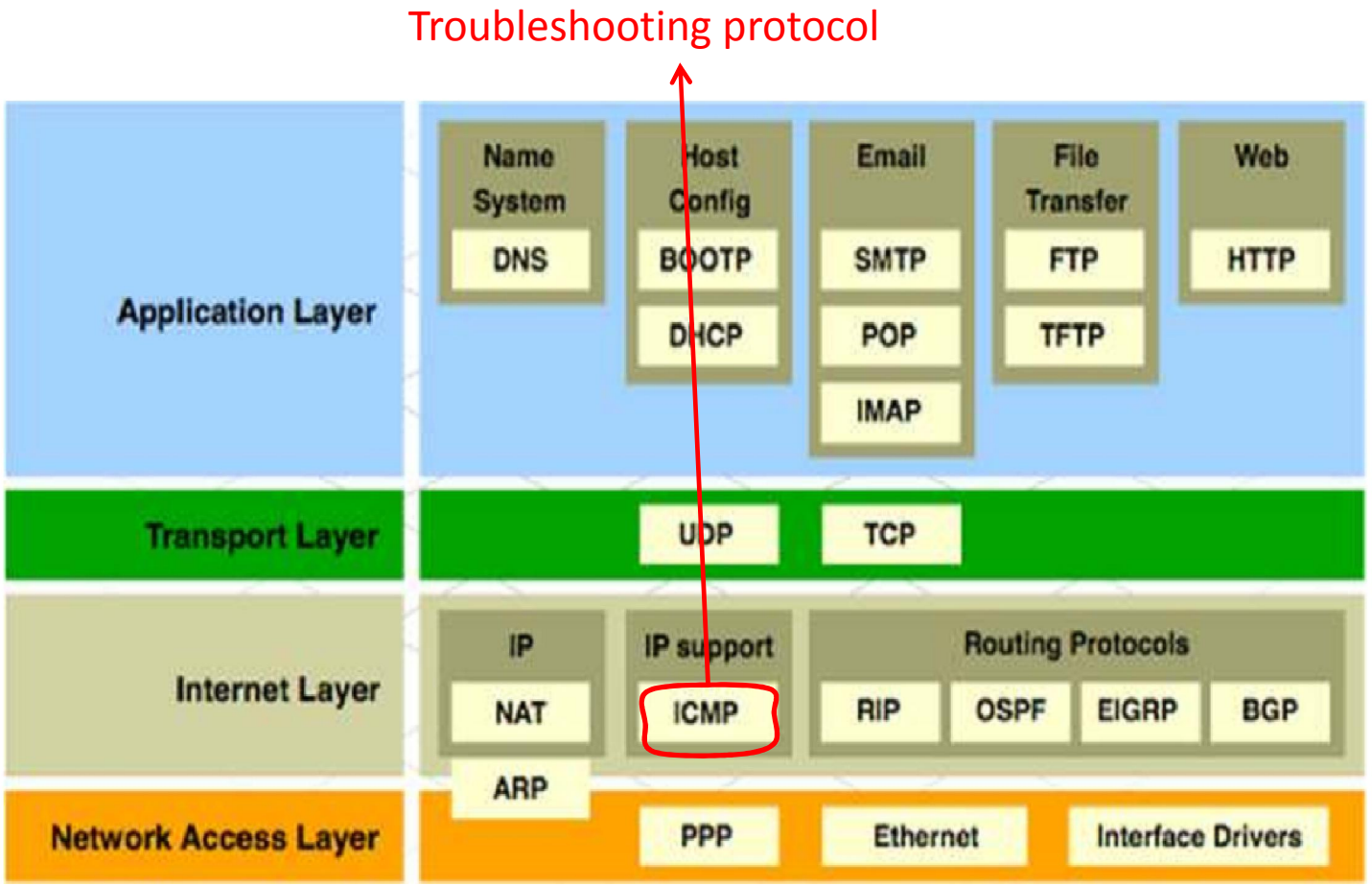
- Introduction
- Rules of Communication
- Network Protocols and Standards
- Moving Data in the Network

NAT - Network Address Translation



- Introduction
- Rules of Communication
- Network Protocols and Standards
- Moving Data in the Network

2.4. TCP/IP Protocol Suite and Communication



2.4. TCP/IP Protocol Suite and Communication

ICMP - Internet Control Message Protocol

The Internet Control Message Protocol is a protocol for the exchange of error messages and other vital information between (Physical) Internet entities such as hosts and routers.

Often, it is placed next to the IP protocol.

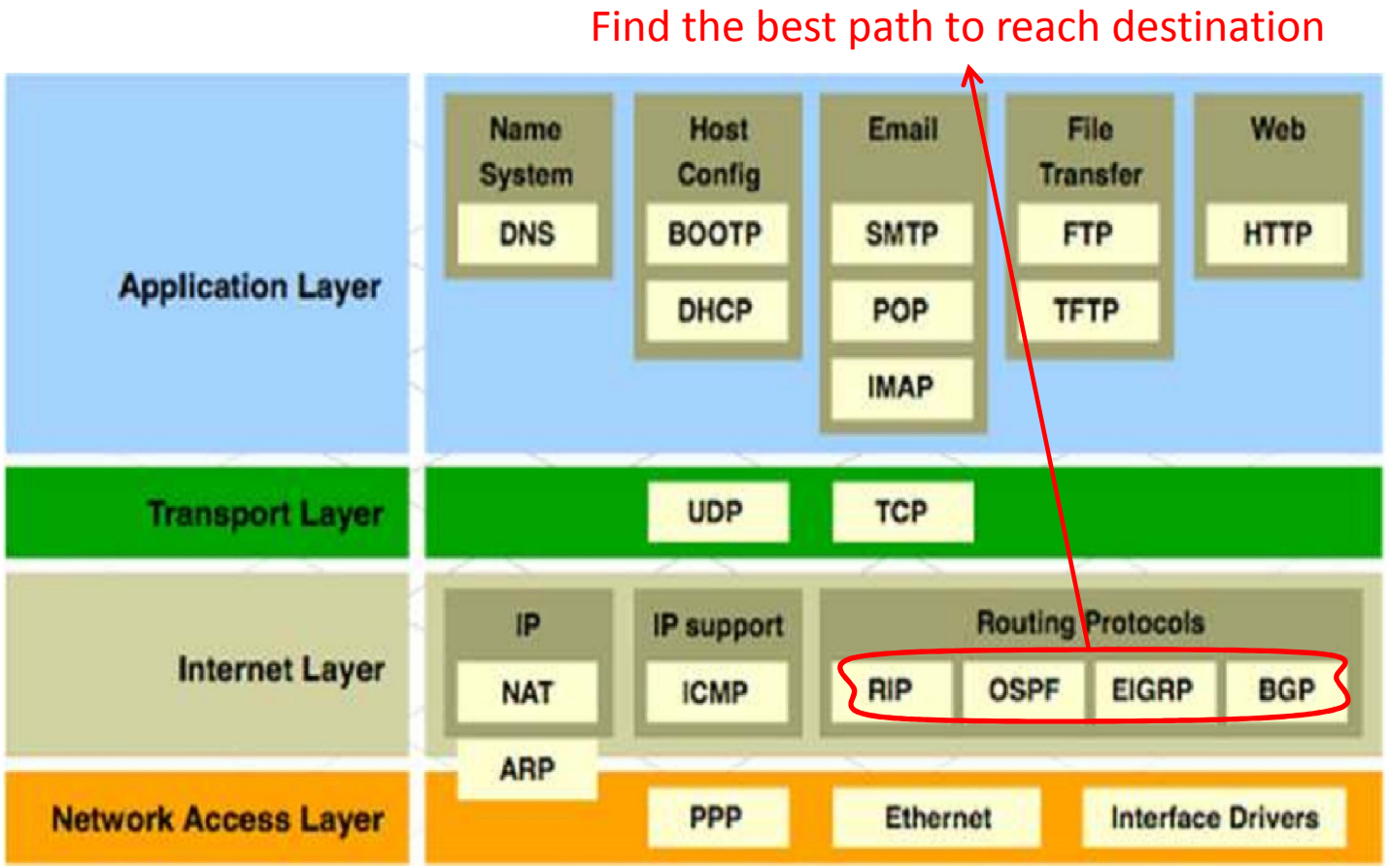
2.4. TCP/IP Protocol Suite and Communication

ICMP functions

- **Announce network errors**: such as a host or entire portion of the network being unreachable, due to some type of failure. A TCP or UDP packet directed at a port number with no receiver attached is also reported via ICMP.
- **Announce network congestion**: When a router begins buffering too many packets, due to an inability to transmit them as fast as they are being received, it will generate ICMP *Source Quench* messages. Directed at the sender, these messages should cause the rate of packet transmission to be slowed.
- **Assist Troubleshooting**: ICMP supports an *Echo* function, which just sends a packet on a round--trip between two hosts. Ping, a common network management tool, is based on this feature. Ping will transmit a series of packets, measuring average round--trip times and computing loss percentages.
- **Announce Timeouts**: If an IP packet's TTL field drops to zero, the router discarding the packet will often generate an ICMP packet announcing this fact. TraceRoute is a tool which maps network routes by sending packets with small TTL values and watching the ICMP timeout announcements.

- Introduction
- Rules of Communication
- Network Protocols and Standards
- Moving Data in the Network

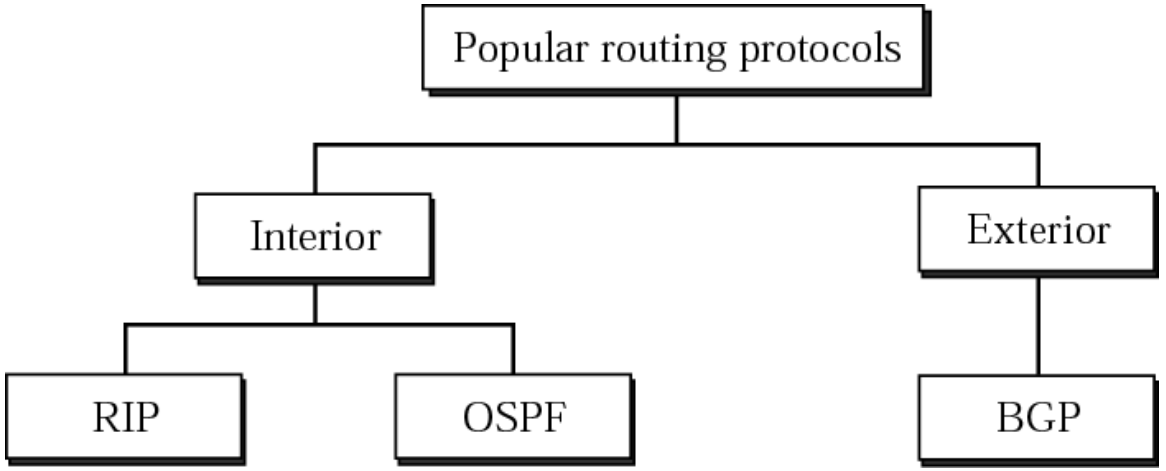
2.4. TCP/IP Protocol Suite and Communication



2.4. TCP/IP Protocol Suite and Communication

Routing protocols

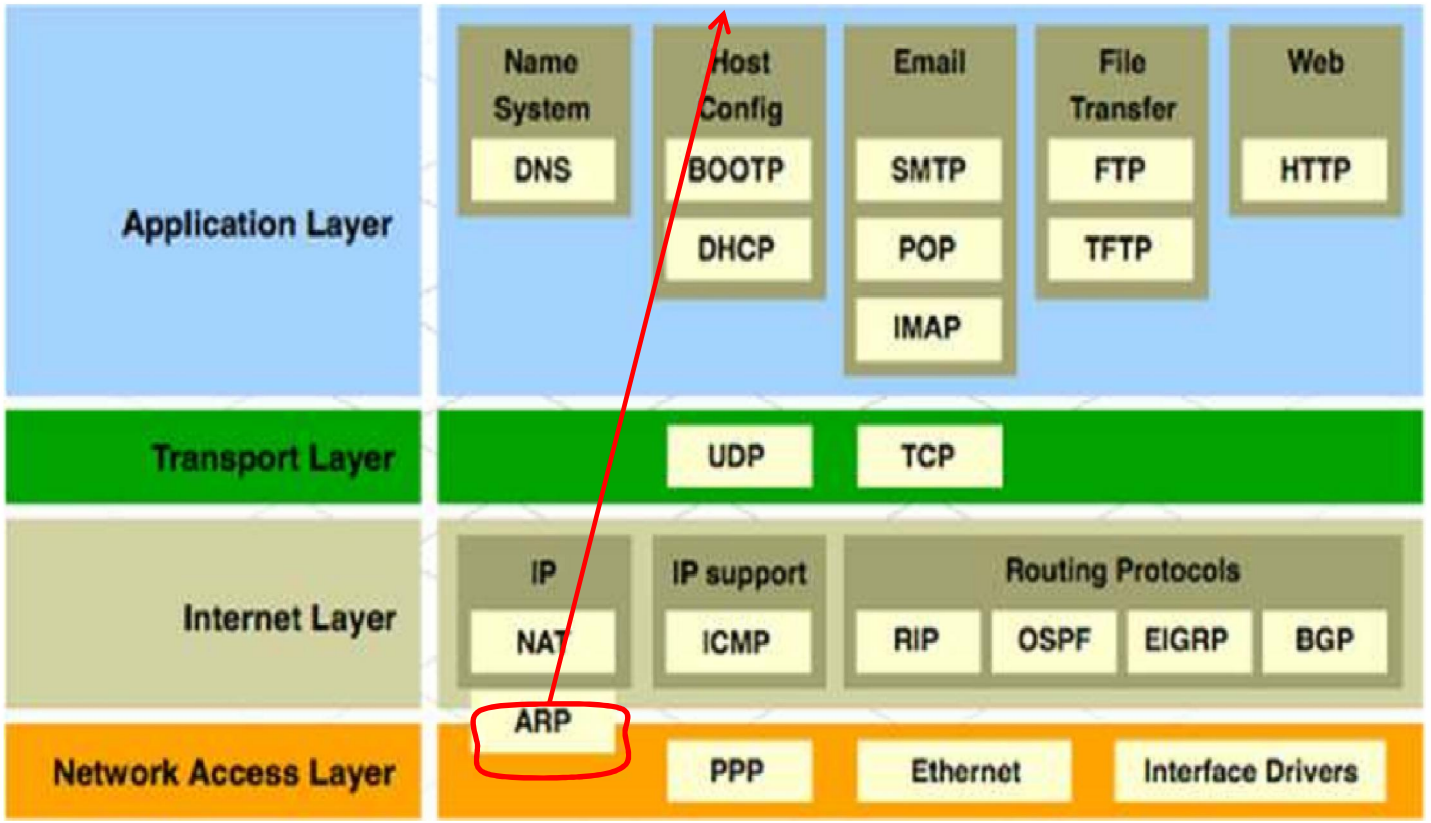
- Dynamic protocols
  - Sharing neighborhood information
- Use different metrics.
- RIP (one hop count, how many networks a packet crosses), Networks are treated equally
- BGP (depend on the policy, set by administrator)
- OSPF (TOS, minimize delay, maximize throughput)



- Introduction
- Rules of Communication
- Network Protocols and Standards
- Moving Data in the Network

2.4. TCP/IP Protocol Suite and Communication

To see what MAC address correspond to a given IP address

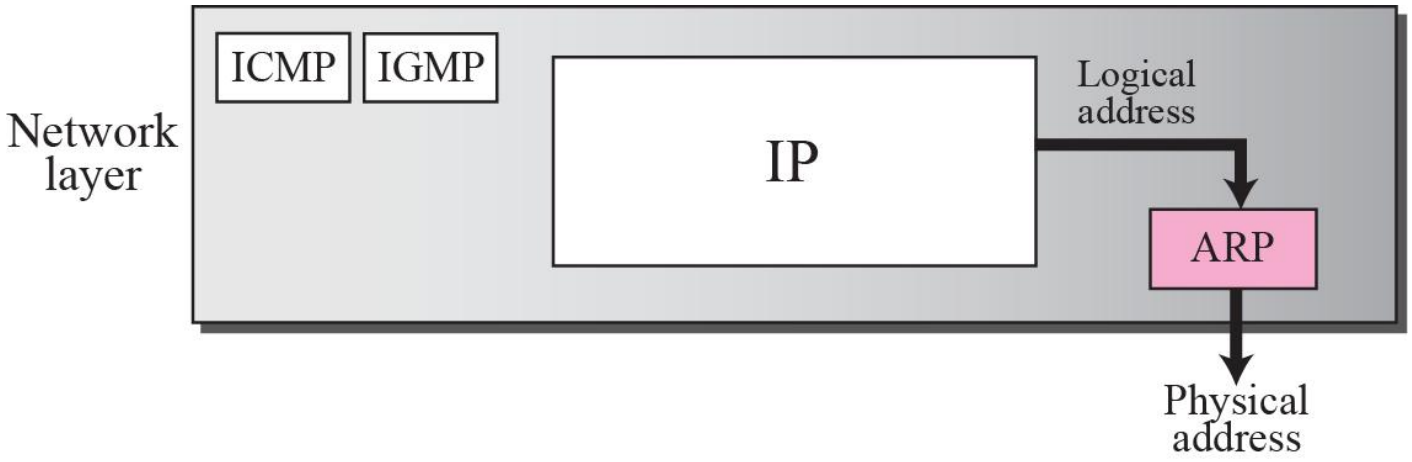


2.4. TCP/IP Protocol Suite and Communication

ARP - Address Resolution Protocol

•Stations need to know MAC address to communicate
•How does IP address get mapped to MAC address?
  •Manual configuration by hand is tedious
  •Automatic process by ARP

✓ARP map any network level address (such as IP) to its corresponding data link address (such as Ethernet)
✓support protocol in data link layers, not data link layer protocol.

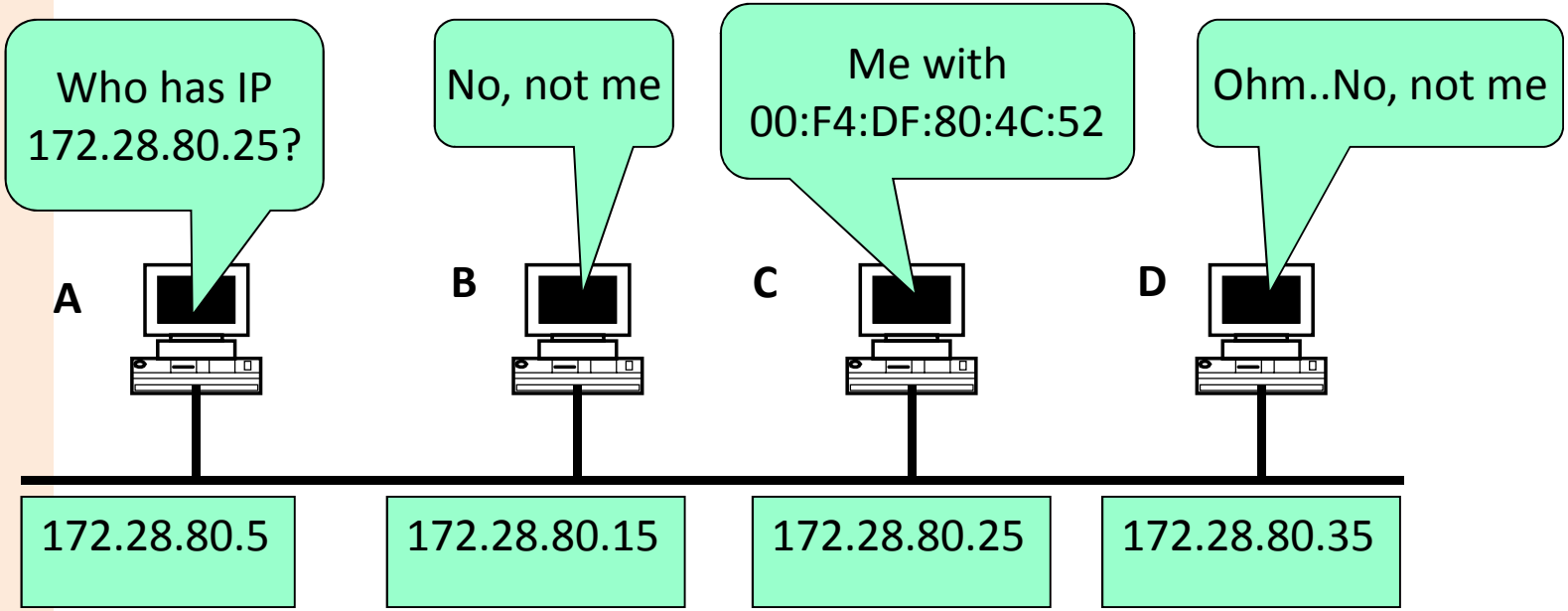


2.4. TCP/IP Protocol Suite and Communication

- Introduction
- Rules of Communication
- Network Protocols and Standards
- Moving Data in the Network

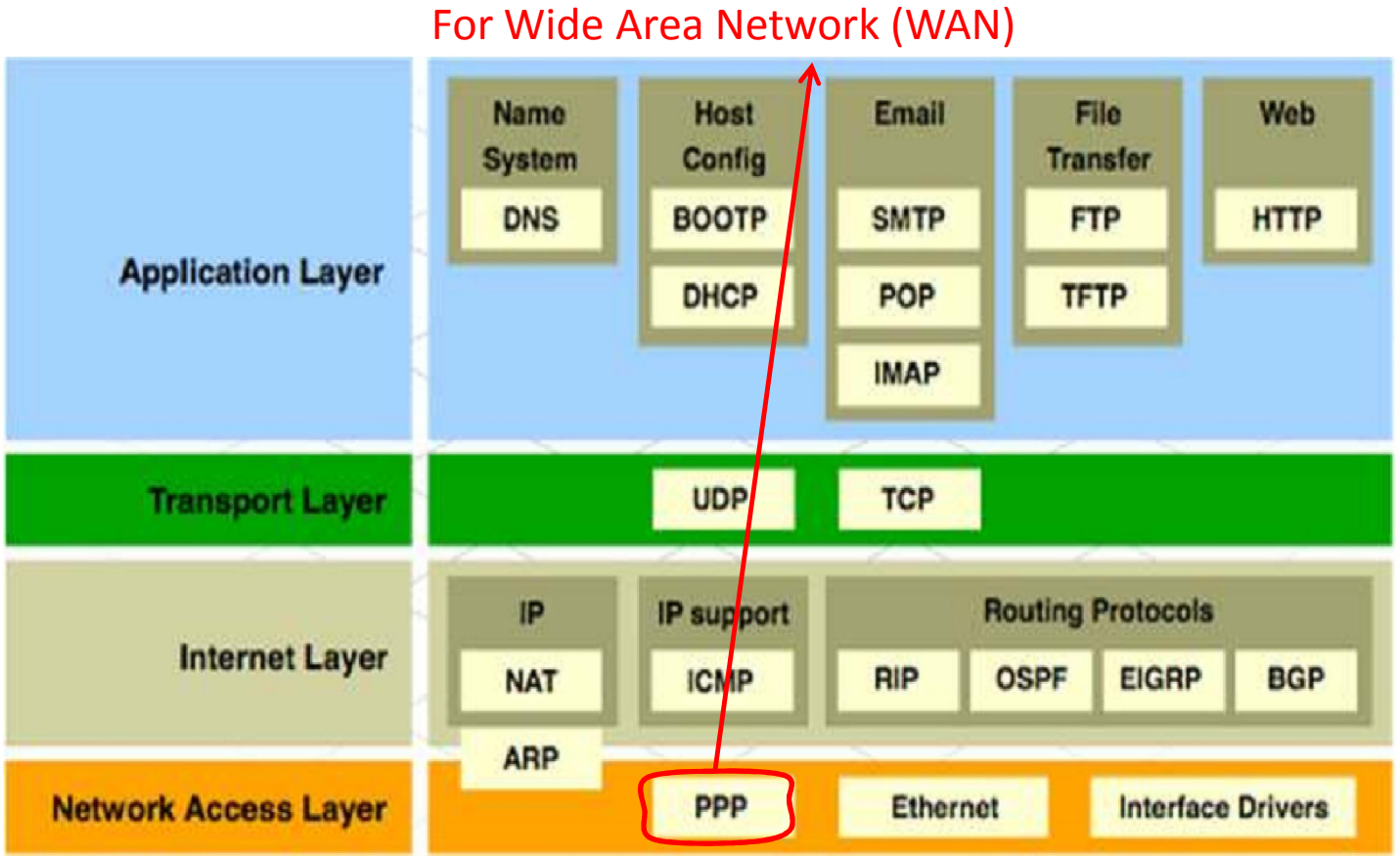
ARP - Address Resolution Protocol

- Host A want to resolve MAC address of C
  - A sends broadcast ARP request
  - A gets unicast ARP reply from C



- Introduction
- Rules of Communication
- Network Protocols and Standards
- Moving Data in the Network

2.4. TCP/IP Protocol Suite and Communication

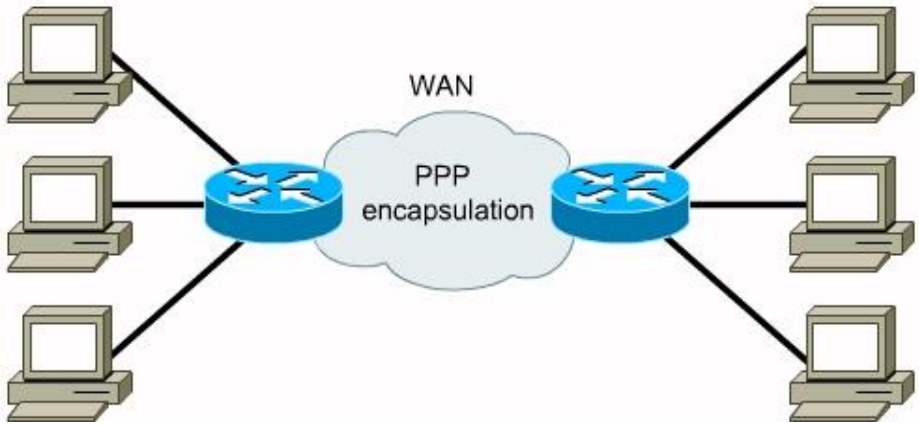


2.4. TCP/IP Protocol Suite and Communication

PPP - Point-to-Point Protocol

➢In order to move data between any two nodes or routers, a data path must be established, and flow control procedures must be in place to ensure delivery of data. This is also true in the WAN environment and is accomplished by using WAN protocols such as Point-to-Point Protocol.

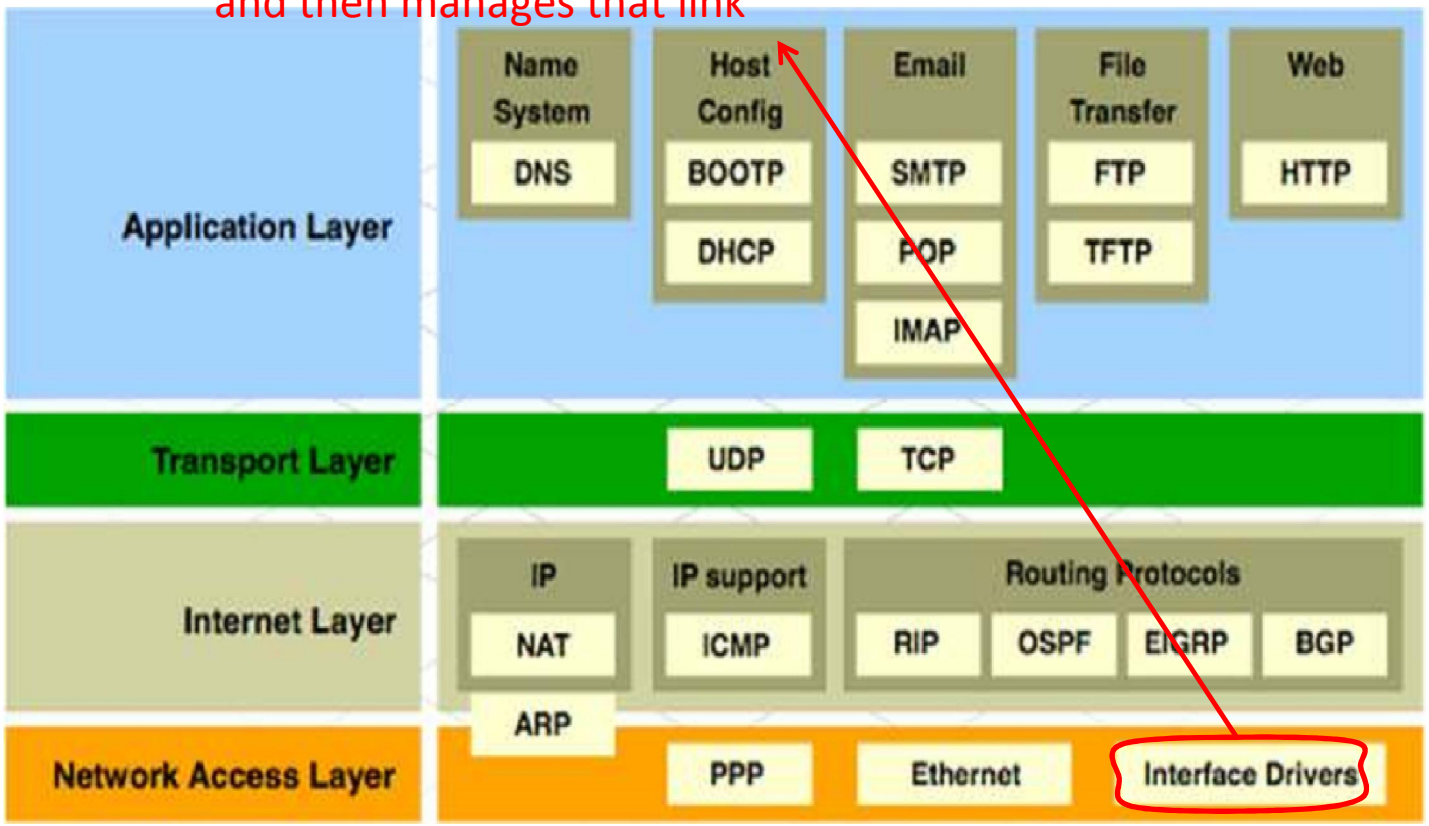
➢PPP provides router-to-router and host-to-network connections over both synchronous and asynchronous circuits.



- Introduction
- Rules of Communication
- Network Protocols and Standards
- Moving Data in the Network

2.4. TCP/IP Protocol Suite and Communication

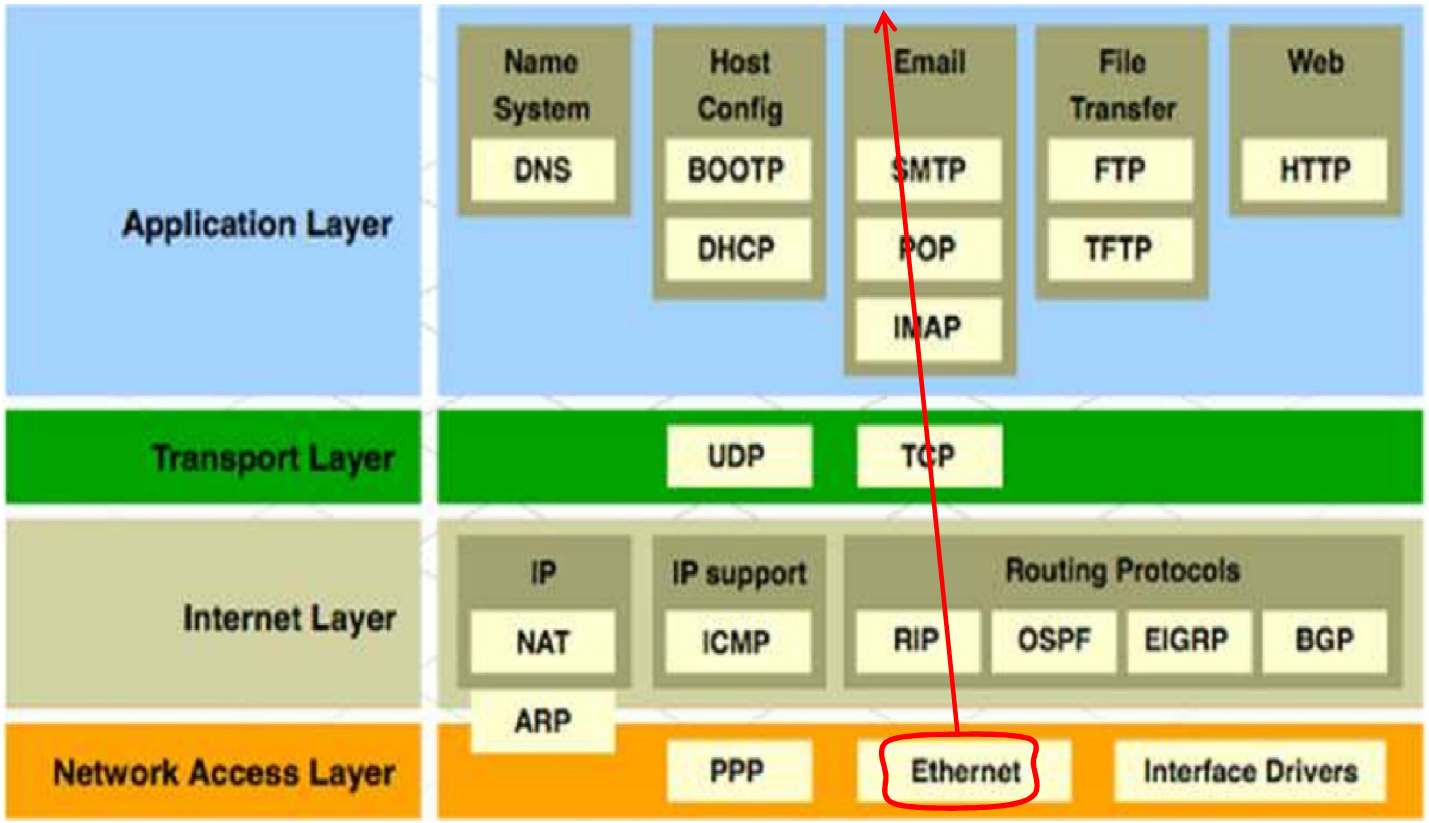
establishes a link between a computer and a network, and then manages that link



- Introduction
- Rules of Communication
- Network Protocols and Standards
- Moving Data in the Network

2.4. TCP/IP Protocol Suite and Communication

Tells you what kind of cabling you are using



2.5. Open Standards

• Open standards encourage competition and innovation.

• An advantage of network devices implementing open standards protocols, such as from the TCP/IP suite, is that clients and servers running different operating systems can communicate with each other.

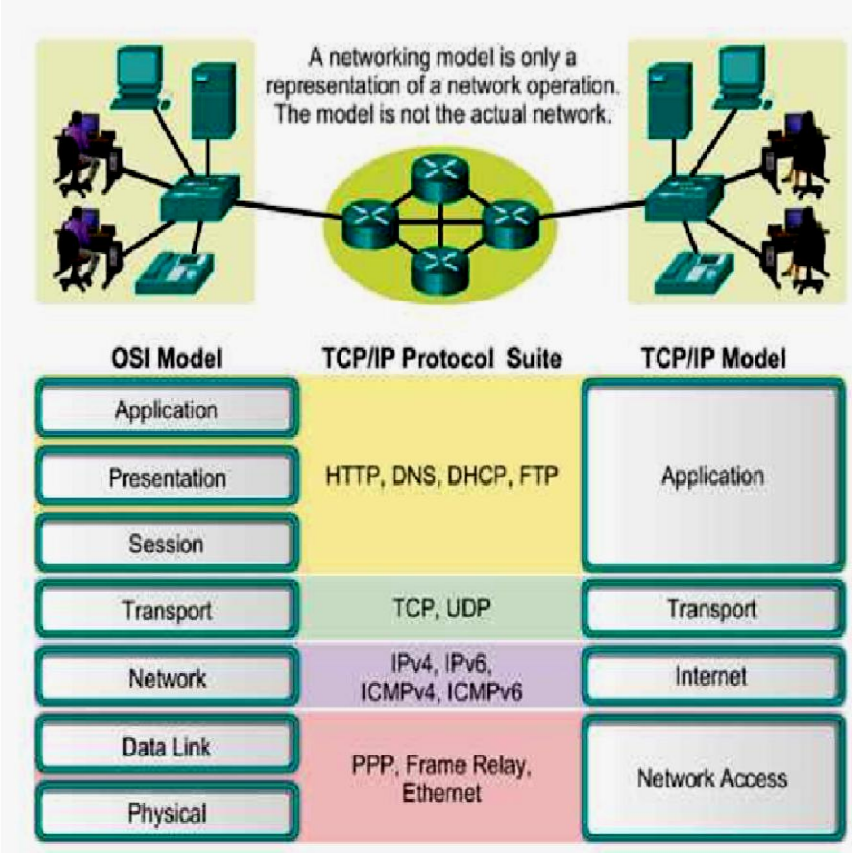
Some open standards are:

- The Internet Society (ISOC)
- The Internet Architecture Board (IAB)
- The Internet Engineering Task Force (IETF)
- Institute of Electrical and Electronics Engineers (IEEE)
- The International Organization for Standards (ISO)

2.6. Benefits of Using a Layered Model

• Assists in protocol design.
• Fosters competition
• Prevents technology or capability changes in one layer from affecting other layers above and below.

• Provides a common language to describe networking functions and capabilities.



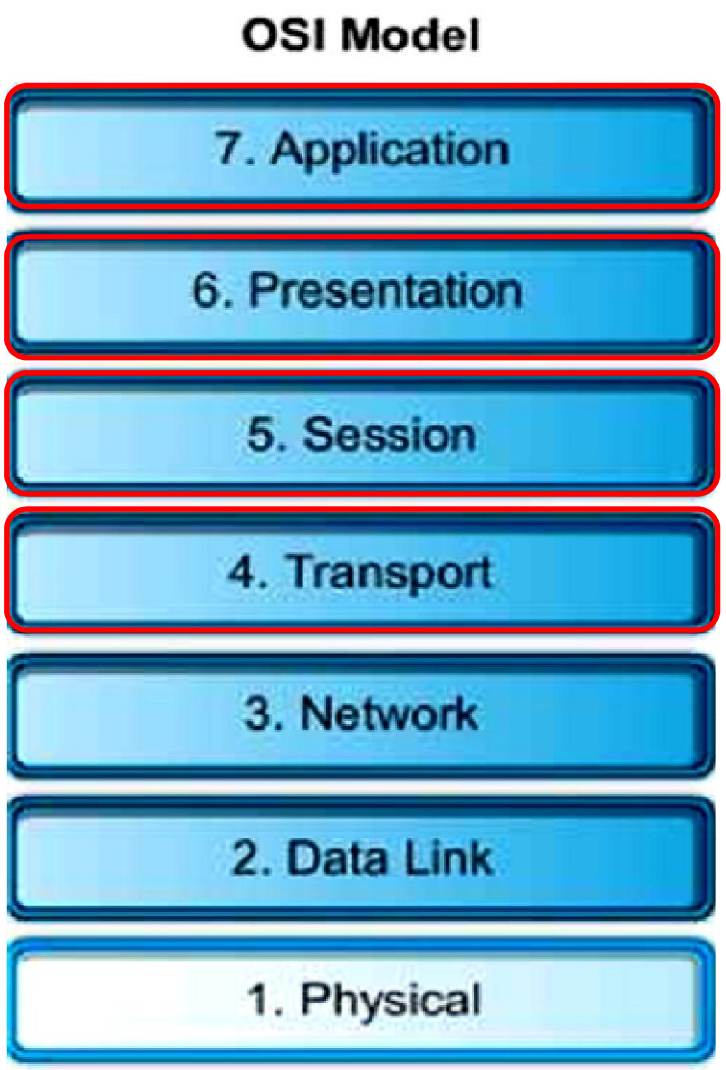
2.7. The OSI Reference Model

• **Application layer**: It provides the means for end-to-end connectivity between individuals in the human network using data networks.

• **Presentation layer**: It provides the means for common representation of the data transferred between application layer services.

• **Session layer**: It provides services to the presentation layer to organize its dialogue and to manage data exchange.

• **Transport layer**: It defines services to segment, transfer, and reassemble the data for individual communications between the end devices.

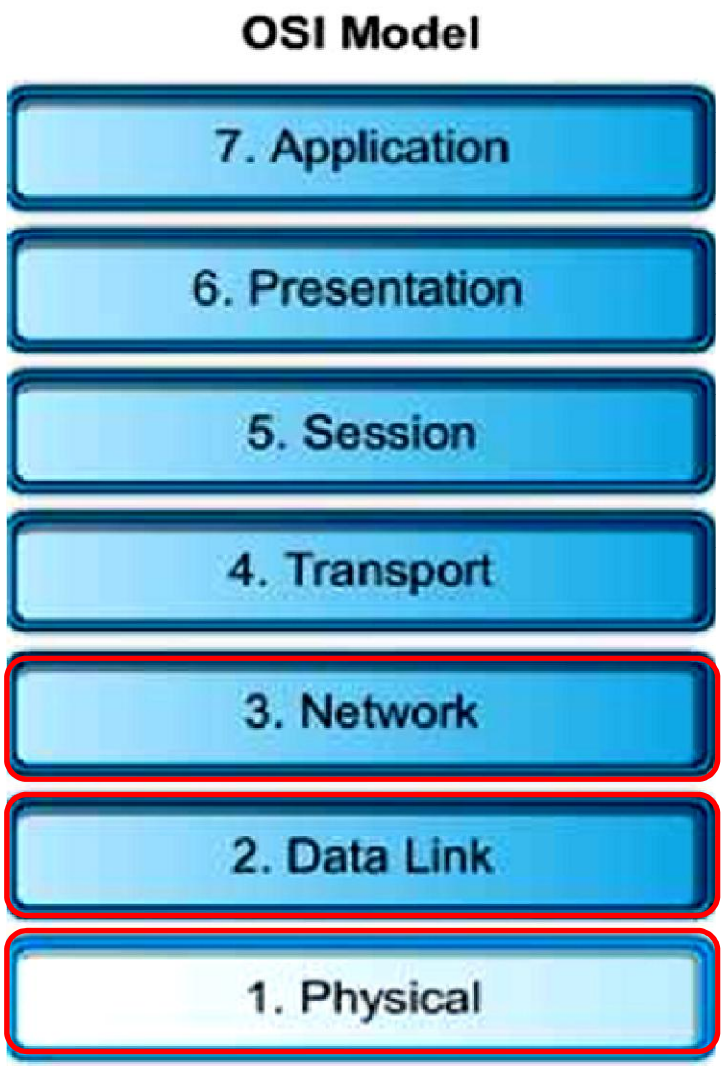


2.7. The OSI Reference Model

• **Network layer**: It provides services to exchange the individual pieces of data over the network between identified end devices.

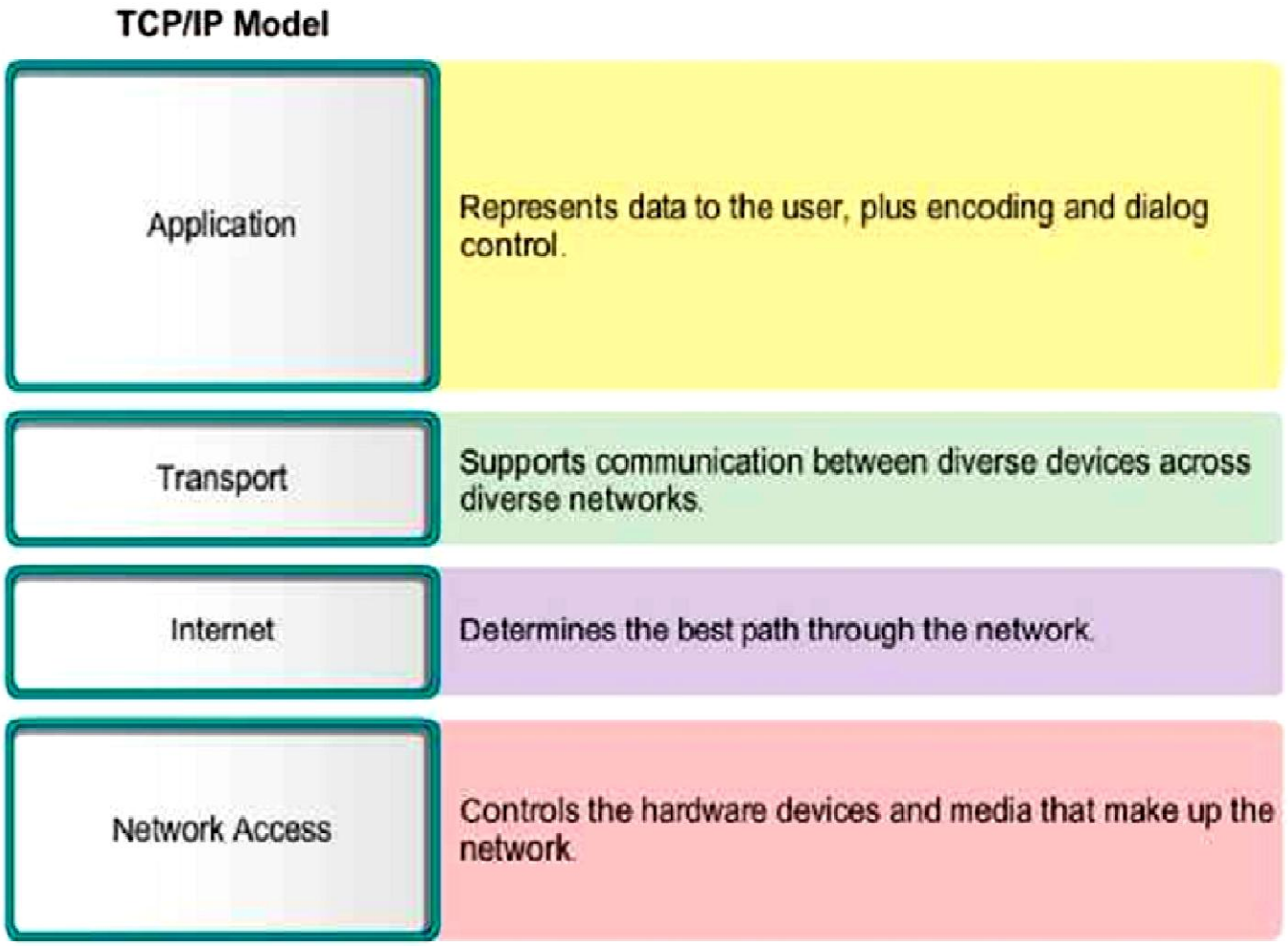
• **Data link layer**: The data link layer protocols describe methods for exchanging data frames between devices over a common media.

• **Physical layer**: The physical layer protocols describe the mechanical, electrical, functional, and procedural means to activate, maintain, and de-activate physical-connections for bit transmission (1s and 0s) to and from a network device.



- Introduction
- Rules of Communication
- Network Protocols and Standards
- Moving Data in the Network

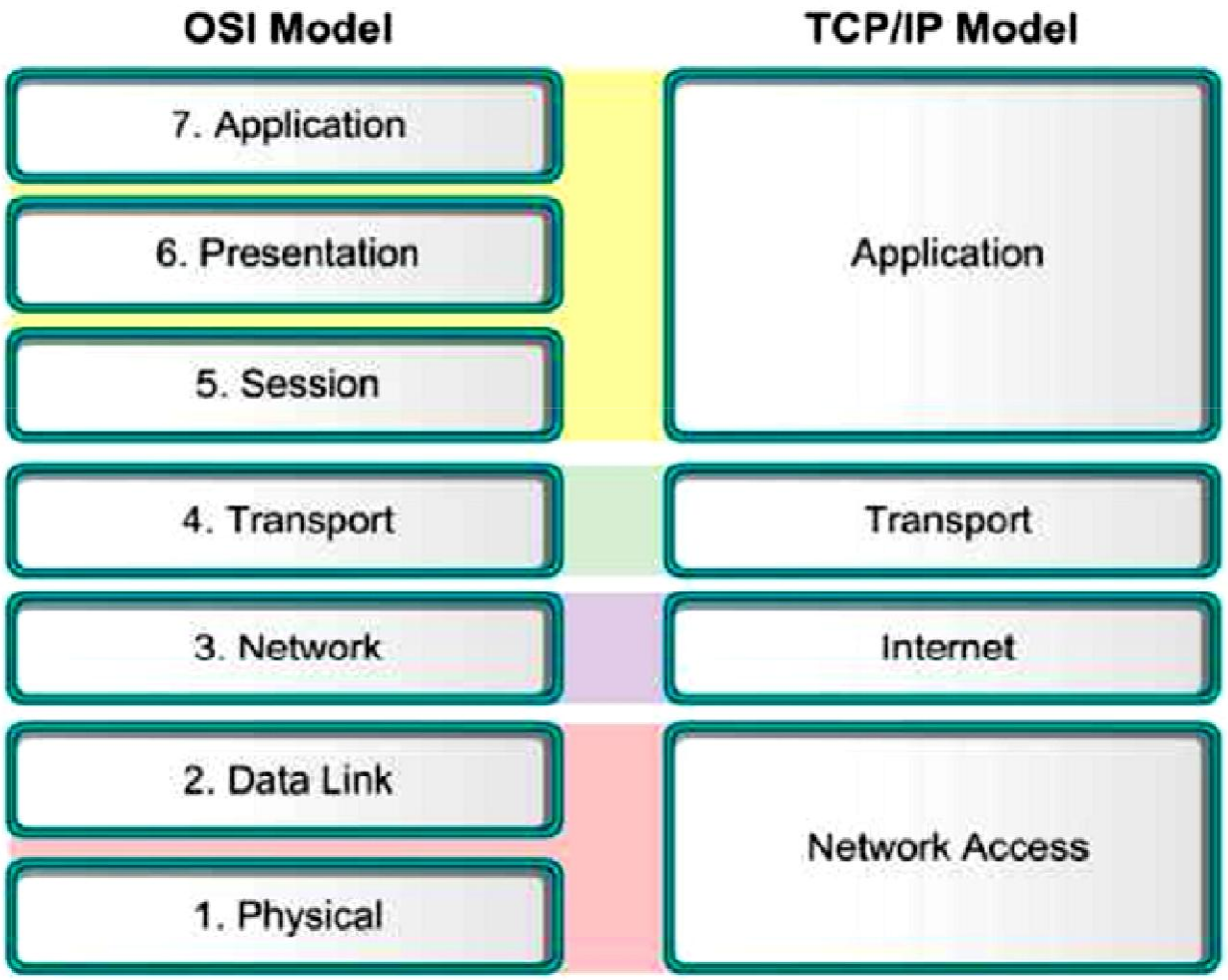
2.8. The TCP/IP Reference Model



- Introduction
- Rules of Communication
- Network Protocols and Standards
- Moving Data in the Network

2.8. The TCP/IP Reference Model

Comparing the ISO and TCP/IP models



3. Moving Data in the Network

3.1. Message Segmentation

•In a packet-switched telecommunication network, segmentation and reassembly (SAR, sometimes just referred to as *segmentation*) is the process of breaking a packet into smaller units before transmission and reassembling them into the proper order at the receiving end of the communication.

•Packets are made smaller to speed them through the network and specifically because of specified packet size restrictions in a given path. In the Open Systems Interconnection (OSI) model, SAR is performed in the Transport layer at both ends.

•A transport protocol determines the size of the smallest maximum protocol data unit (PDU) supported by any of the involved networks, and segments the packets accordingly.

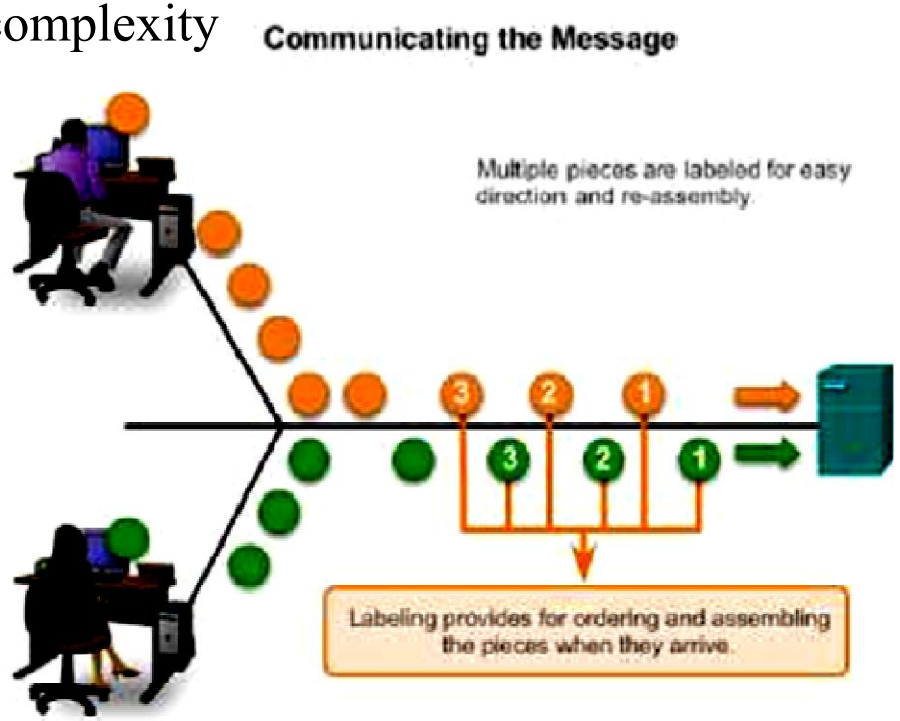
❑Segmenting message benefits

Different conversations can be interleaved

Increased reliability of network communications

❑ Segmenting message disadvantage

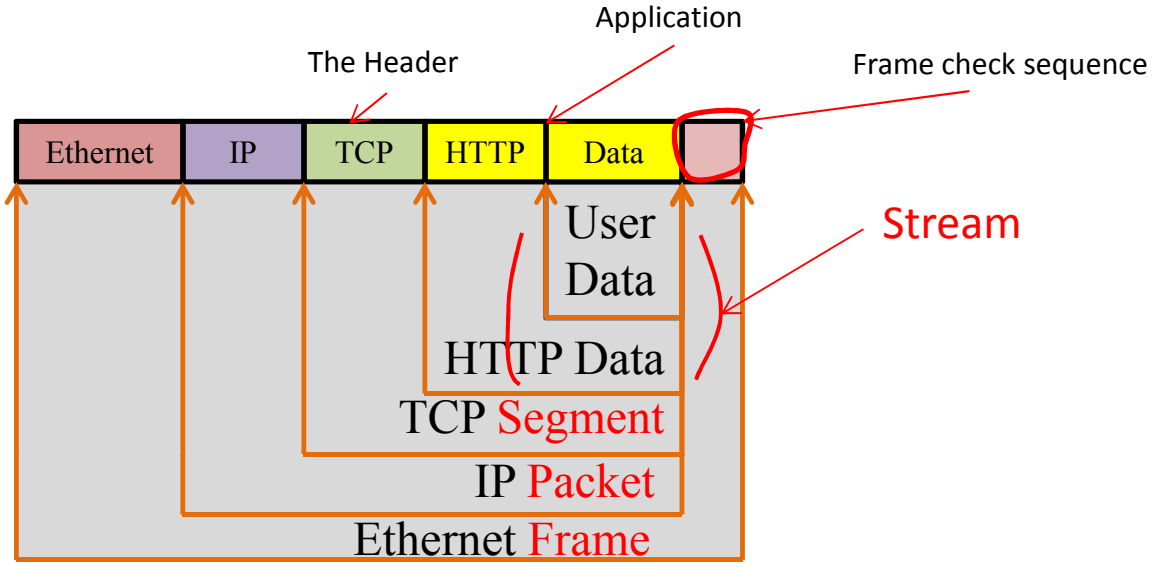
Increased level of complexity

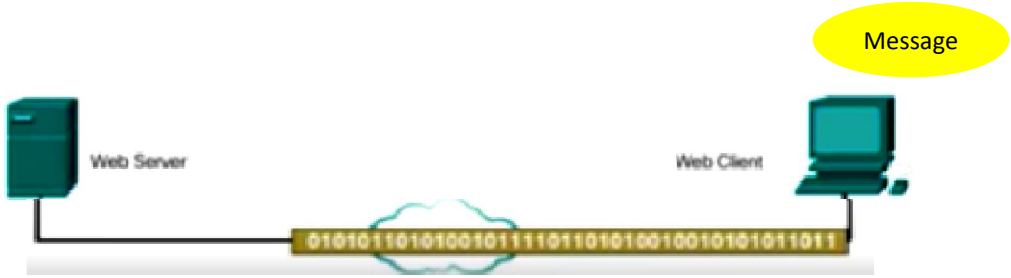


- Introduction
- Rules of Communication
- Network Protocols and Standards
- Moving Data in the Network

3.2. Data Encapsulation

Protocol operation – Message sending





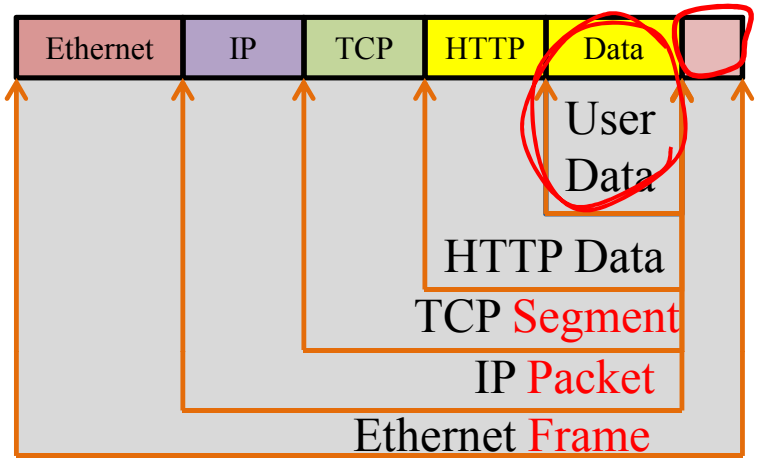
3.3. De-Encapsulation

Protocol operation – Message receiving

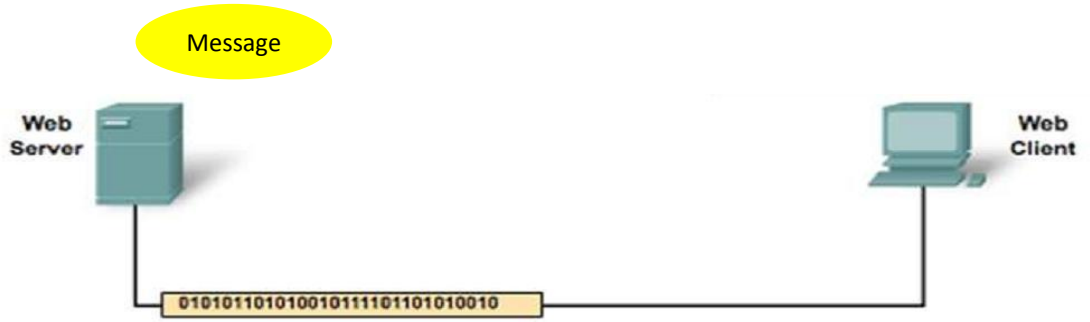
2. Check the address MAC (it can be unicast, multicast or broadcast)

3. Look for the port numbers, source, destination …

1. Check if the data has not been uncorrupted



4. That's we got the data we want to send up.



3.4. Protocol Data Units (PDUs)

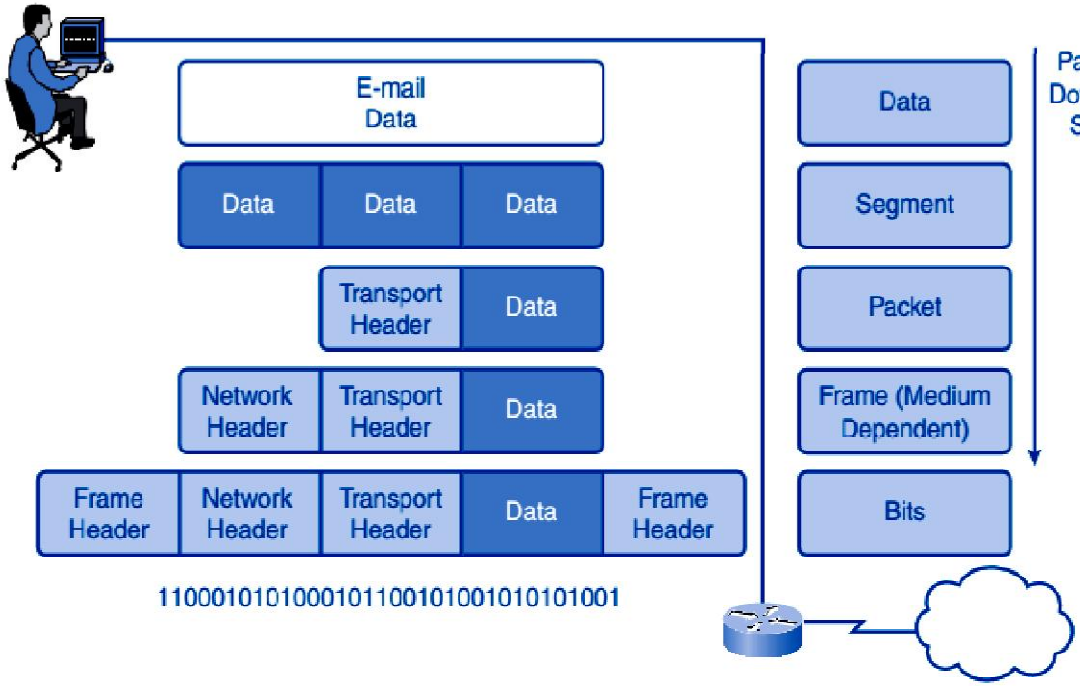
❑ For application data to travel uncorrupted from one host to another, header (or control data), which contains control and addressing information, is added to the data as it moves down the layers. The process of adding control information as it passes through the layered model is called encapsulation.

❑ Decapsulation is the process of removing the extra information and sending only the original application data up to the destination application layer. Each layer adds control information at each step. The generic term for data at each level is protocol data unit (PDU), but a PDU is different at each layer. The different names for PDUs at each layer are listed in Table below.

- Introduction
- Rules of Communication
- Network Protocols and Standards
- Moving Data in the Network

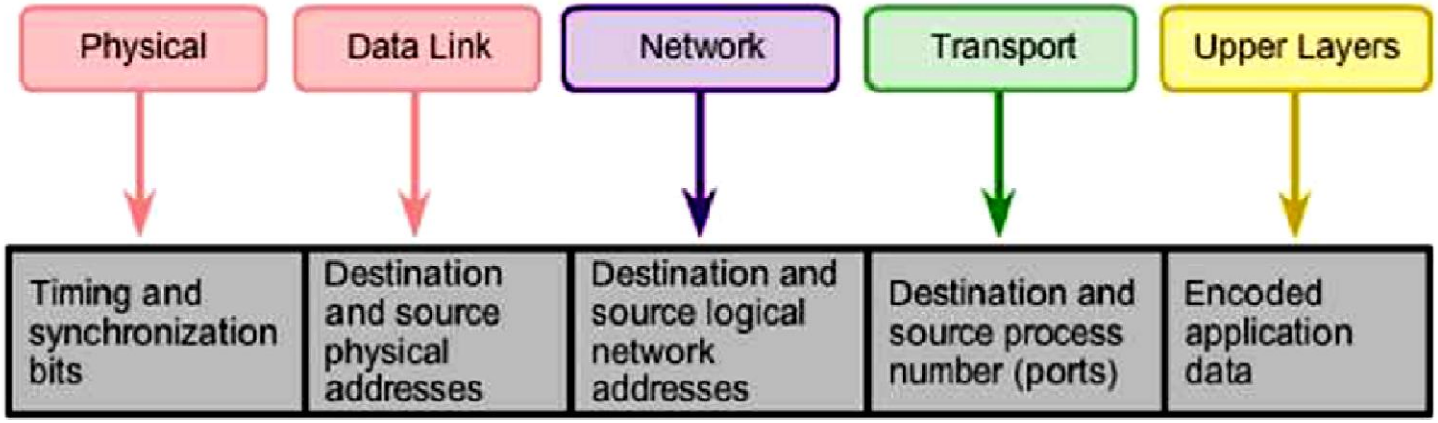
Table Protocol Data Unit Naming Conventions

PDU Name	Layer
Data	Application layer PDU
Segment	Transport layer PDU
Packet	Internetwork layer PDU
Frame	Network access layer PDU
Bits	PDU used for the physical transmission of binary data over media

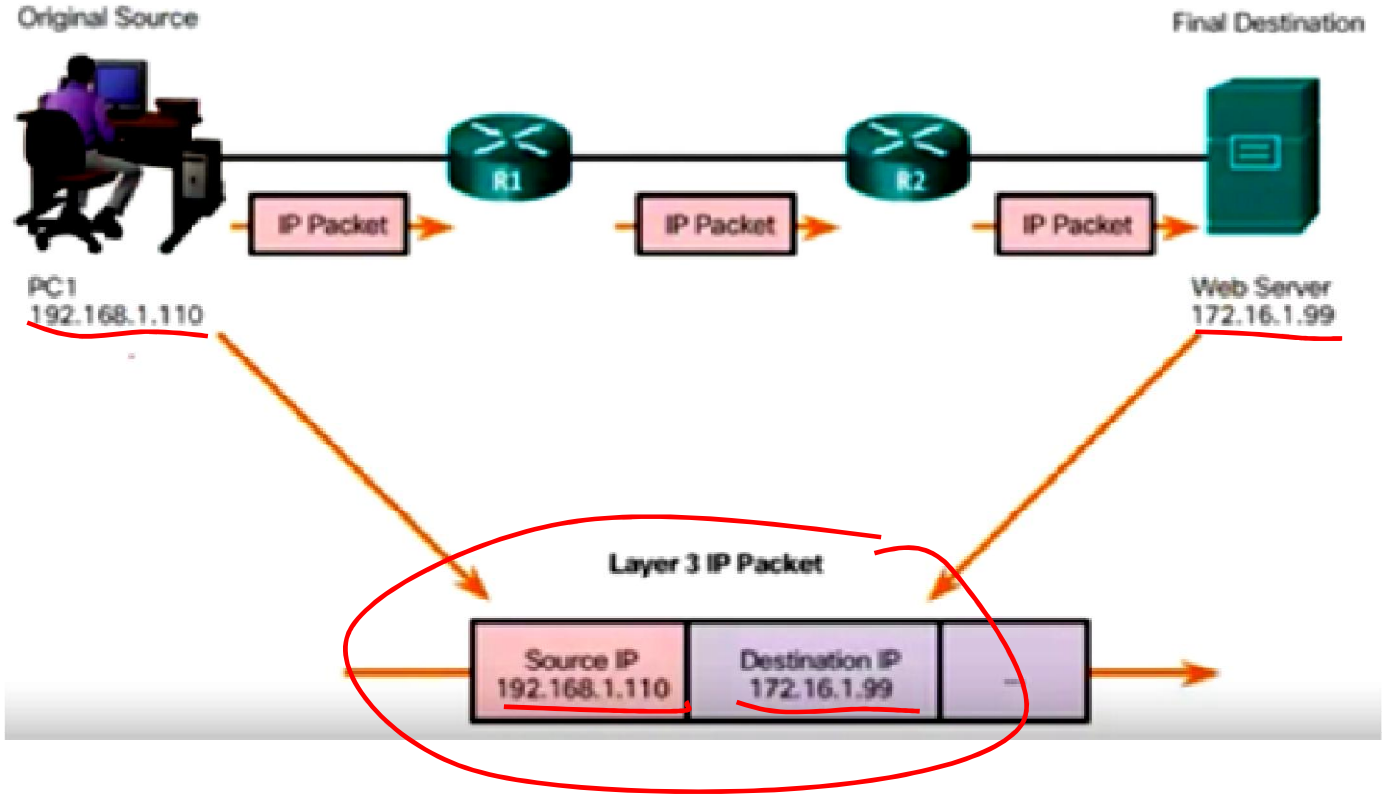


3.5. Network addresses

Addressing of data happens in three different layers of the OSI model. The PDU at each layer adds address information for use by the peer layer at the destination. Figure below depicts the different addressing information added by each layer.



Network layer 3 does not get changed; unless we pass from private network to public network where the source address will be changed.



3.6. Data Link Addresses

Network Address

•Source IP address

•Destination IP address

•Responsible for delivering the IP packet from the original source to the final destination, either on the same network or to a remote network.

Data link Address

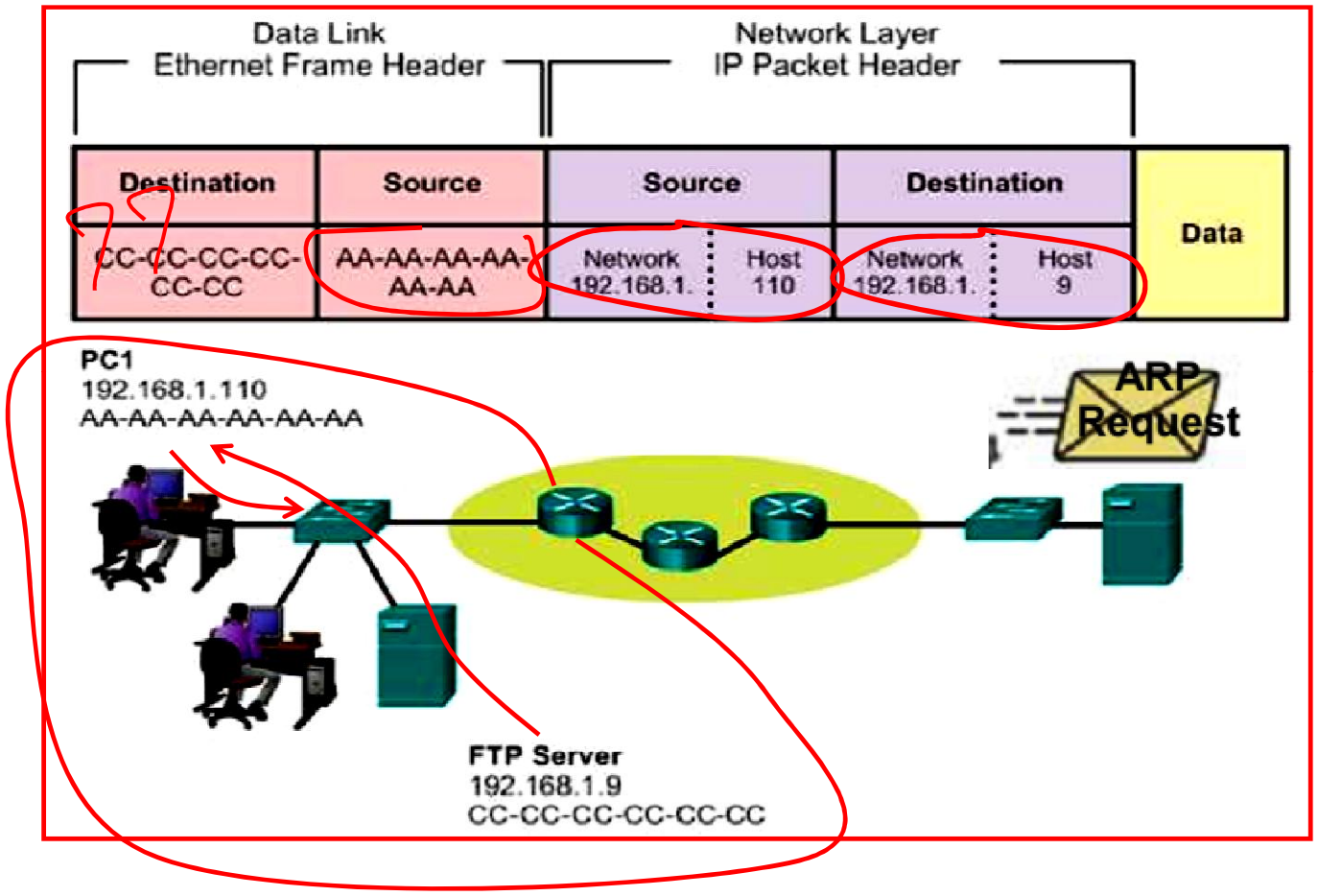
•Source data link address

•Destination data link address

•Responsible for delivering the data link frame from one network interface card (NIC) to another NIC on the same network.

- Introduction
- Rules of Communication
- Network Protocols and Standards
- Moving Data in the Network

3.7. Communicating with Device/Same Network



- Introduction
- Rules of Communication
- Network Protocols and Standards
- Moving Data in the Network

3.8. Communicating with Device/Remote Network