Advanced Communication Networks

Muhammad Taha Jilani

Lecture – 10
(Continued)

TCP/IP Protocols Suite

- **Overview**
  - In 1973, United States *Defense Advanced Research Projects Agency*(*DARPA* or *ARPA*) start development of a full-fledged system of internetworking called *"ARPAnet".*
  - The collection of protocols were used for this internetwork, and there was only one core protocol: TCP (*Transmission Control Program).*
    - It was revised and formally documented in RFC 675, as *Specification of Internet Transmission Control Program* in 1974.
  - In 1977, Postel's (one of the most important pioneers of the Internet and TCP/IP) observation led to the creation of TCP/IP architecture, and the splitting of TCP into: TCP at the transport layer and IP at the network layer; thus the name "TCP/IP".

TCP/IP Protocols Suite

- **Overview**
  - The name “TCP/IP” came about when the original Transmission Control Program (TCP) was split into the Transmission Control Protocol (TCP) and Internet Protocol (IP).
    - The first modern versions of these two key protocols were documented in 1980 as TCP version 4 and IP version 4.
  - TCP/IP quickly became the standard protocol set for running the ARPAnet. In the 1980s, more and more machines and networks were connected to the evolving ARPAnet using TCP/IP protocols, and the TCP/IP Internet was born.

TCP/IP Protocols Suite

- **Why TCP/IP ?**
  - TCP/IP in fact consists of dozens of different protocols, but only a few are the “main” protocols that define the core operation of the suite.
  - The two key protocols are usually considered the most important.
    - The *Internet Protocol (IP)* is the primary OSI network layer (layer three) protocol that provides addressing, datagram routing and other functions in an internetwork.
    - The *Transmission Control Protocol (TCP)* is the primary transport layer (layer four) protocol, and is responsible for connection establishment and management and reliable data transport between software processes on devices.

TCP/IP Protocols Suite

Success of TCP/IP ?

Beside other protocols and even after 40 years, TCP/IP is still widely acceptable protocol in the world. Main factors that contribute it success are

- **Integrated Addressing System:** TCP/IP includes within it a system for identifying and addressing devices on both small and large networks. The addressing system is designed to allow devices to be addressed regardless of the lower-level details. It includes a centralized administration capability for the Internet, to ensure that each device has a unique address.
- **Design For Routing:** TCP/IP is specifically designed to facilitate the routing of information over a network of arbitrary complexity. Due to importance of connecting networks, a number of support protocols are also included in TCP/IP to allow routers to exchange critical information and manage the efficient flow of information from one network to another.

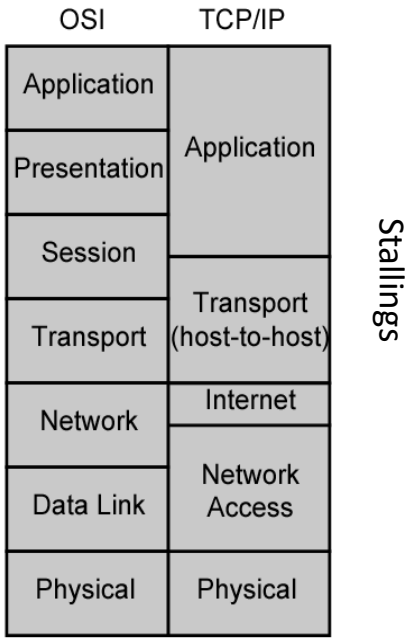
TCP/IP Protocols Suite

Success of TCP/IP ?

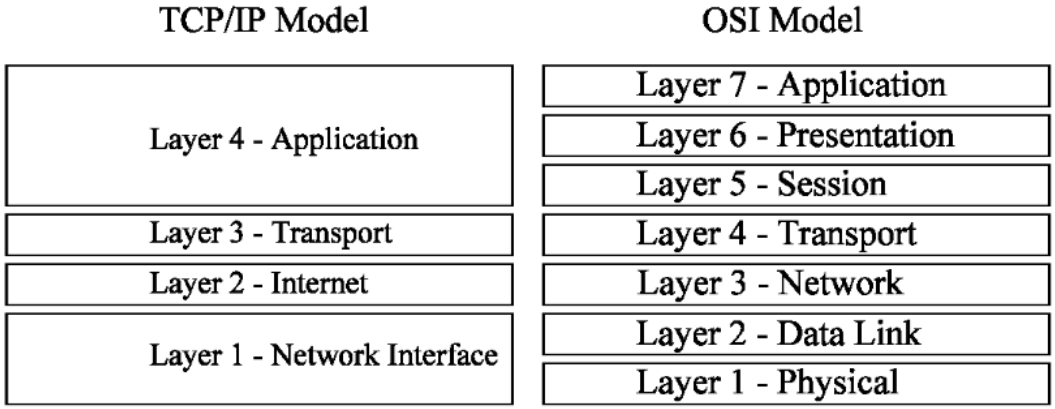
- **Underlying Network Independence:** TCP/IP operates primarily at layers three and above, and includes provisions to allow it to function on almost any lower-layer technology, including LANs, wireless LANs and WANs of various sorts. This flexibility means that one can mix and match a variety of different underlying networks and connect them all using TCP/IP.
- **Scalability:** Over the decades TCP/IP has proven its scalable nature as the Internet has grown from a small network with just a few machines to a huge internetwork with billions of hosts. Changes have been taken periodically to support this growth, but the core of TCP/IP is basically the same as it was in 1978.
- **Open Standards and Development Process:** The TCP/IP standards are not proprietary, but open standards freely available to the public. It allows other to participate in the development of "RFC" process, where anyone with an interest in the TCP/IP protocols is given a chance to provide input into it.

TCP/IP Layer Model

- TCP/IP does not have an official layer structure, but after OSI layers introduction, it is widely compared with OSI model.
- TCP/IP uses its own four-layer architecture (often defined in 5 layers) that corresponds roughly to the OSI Reference Model and provides a framework for the various protocols that comprise the suite.



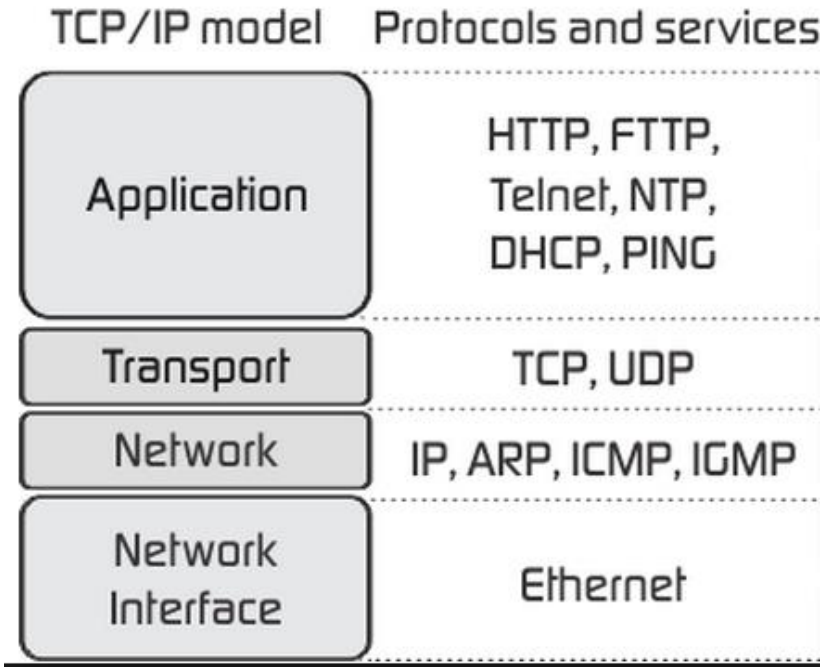
Stallings



Forouzan

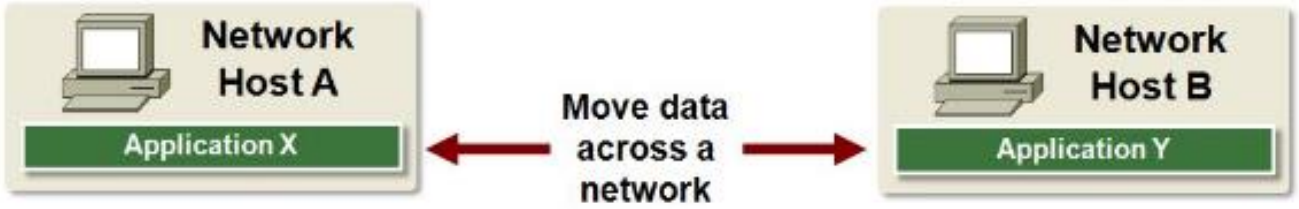
TCP/IP Layer Model

- **TCP/IP vs OSI**
  - Actually TCP/IP reference model has been built on its protocols and this is why it is not so important to assign roles to each layer in TCP/IP; understanding TCP, IP and the application protocols would be enough



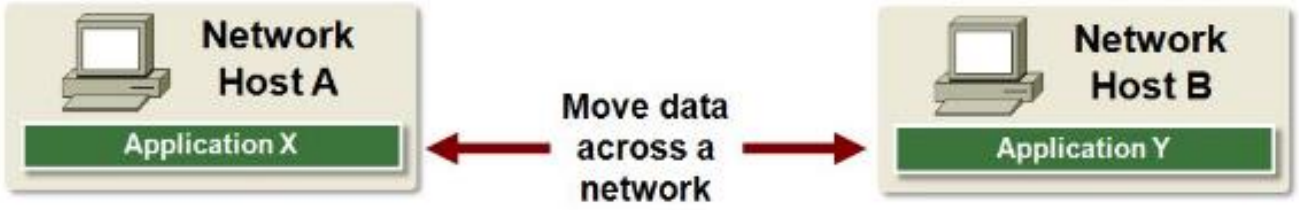
TCP/IP Layer Model

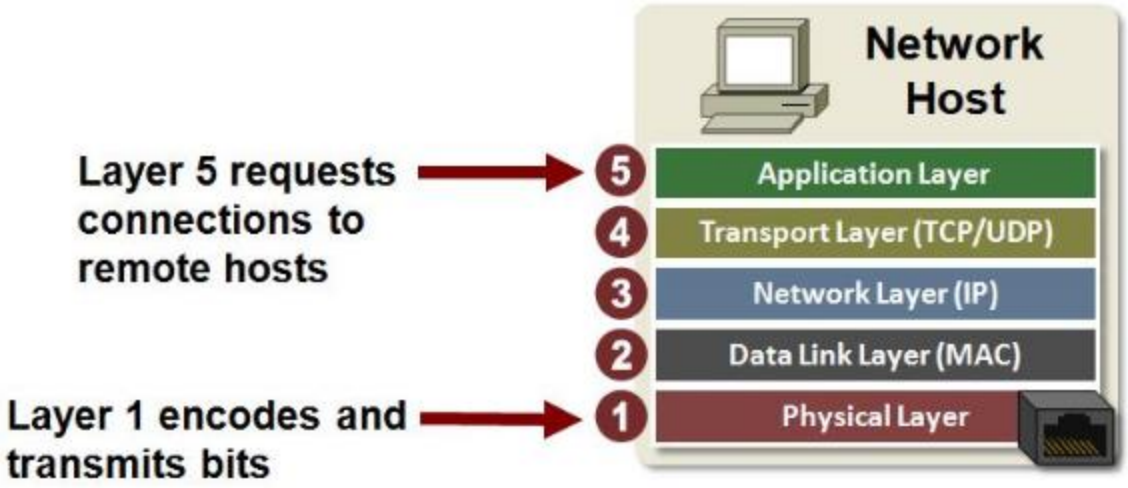
- **Basic Needs for TCP/IP Communication**
  - Some of the applications we use require us to move data from point A to point B across a network. The TCP/IP network provides a framework for transmitting this data, and it requires some basic information from us to move this data.
  - We need to specify if we want the most reliable or fastest transmissions, and we need to specify where we want the data delivered.
  - Sometimes our data is routed based on its IP addresses and sometimes its routed based on its MAC address. The data we send needs both addressing capabilities. This information needs to be sent along with all transmitted data. We also need to physically transmit the data from one location to another.



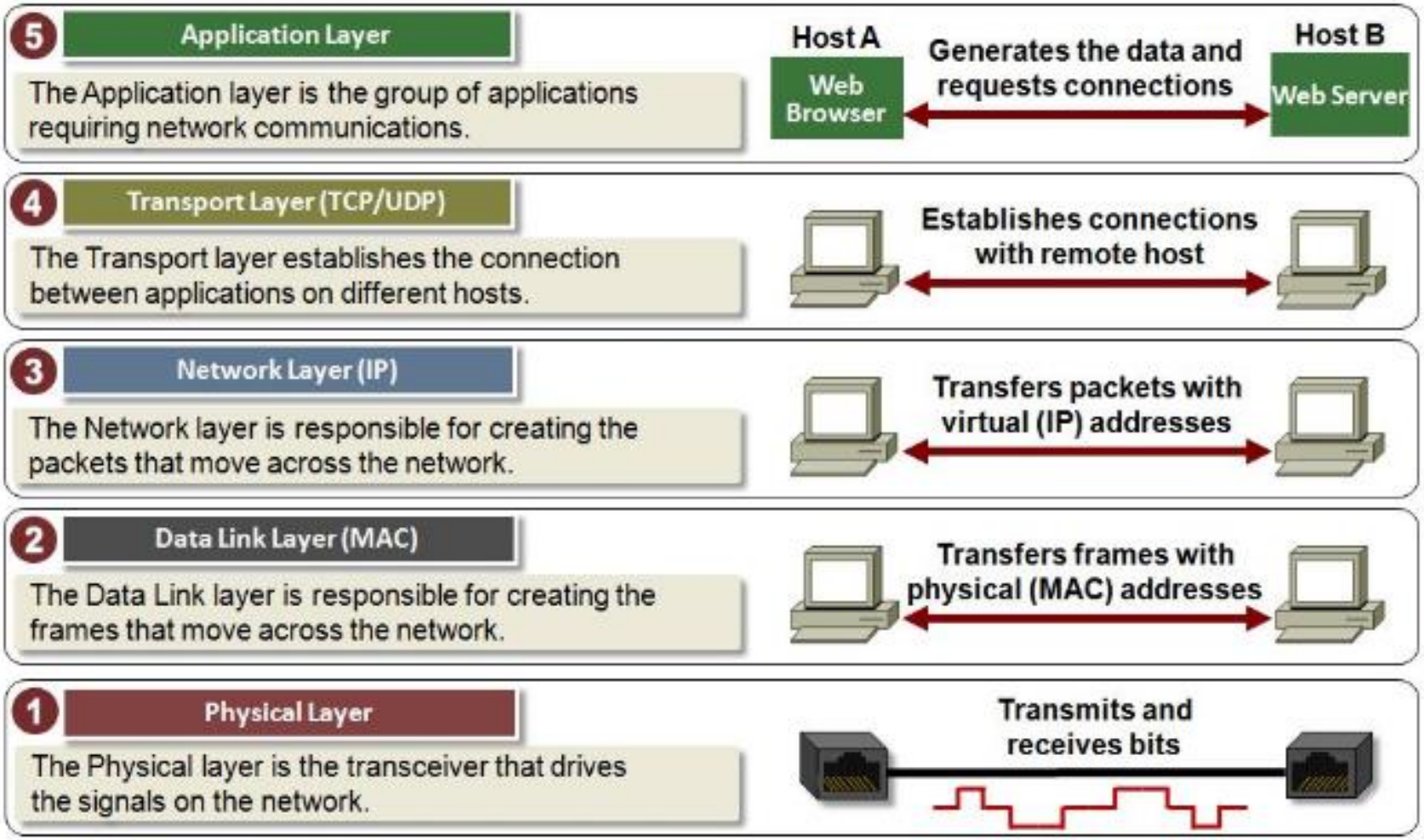
TCP/IP Five Layer Model

- **TCP/IP Communication**



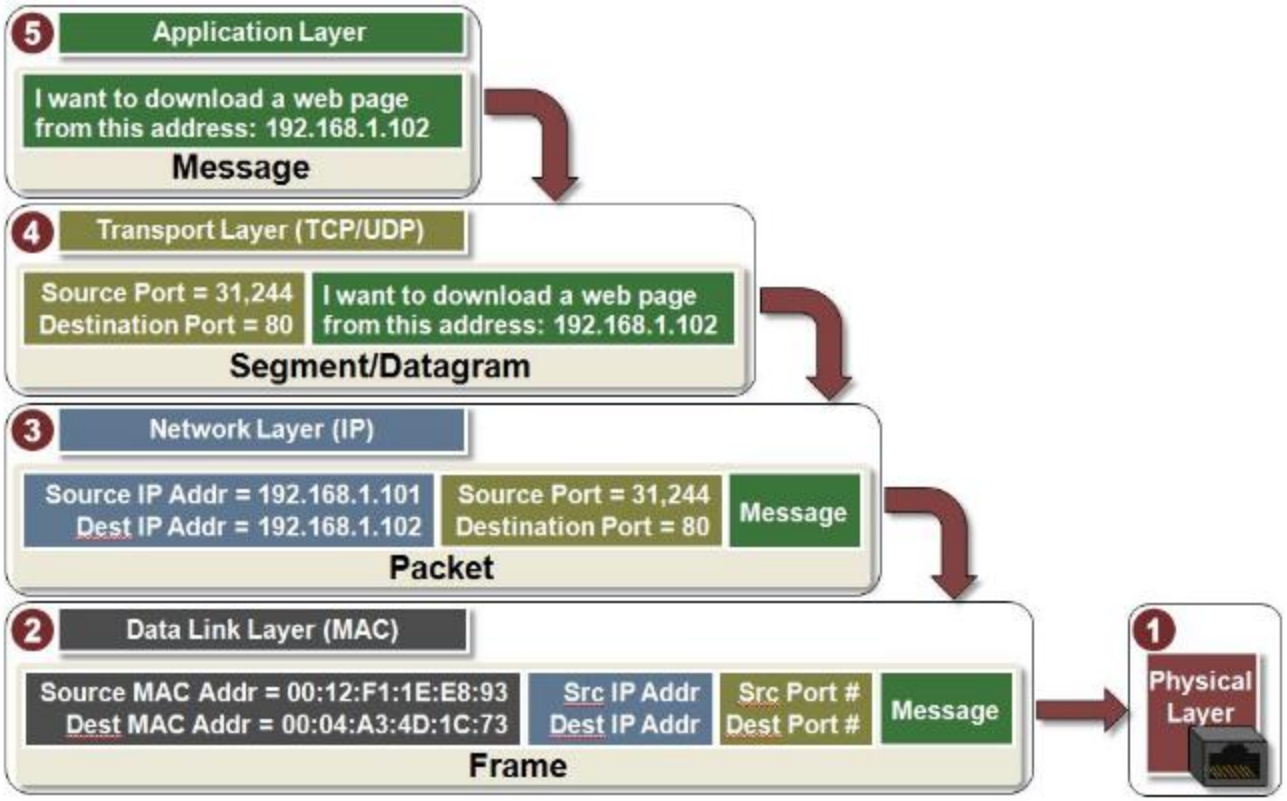


TCP/IP Five Layer Model



TCP/IP Five Layer Model

- **Transmit Data over Layers**



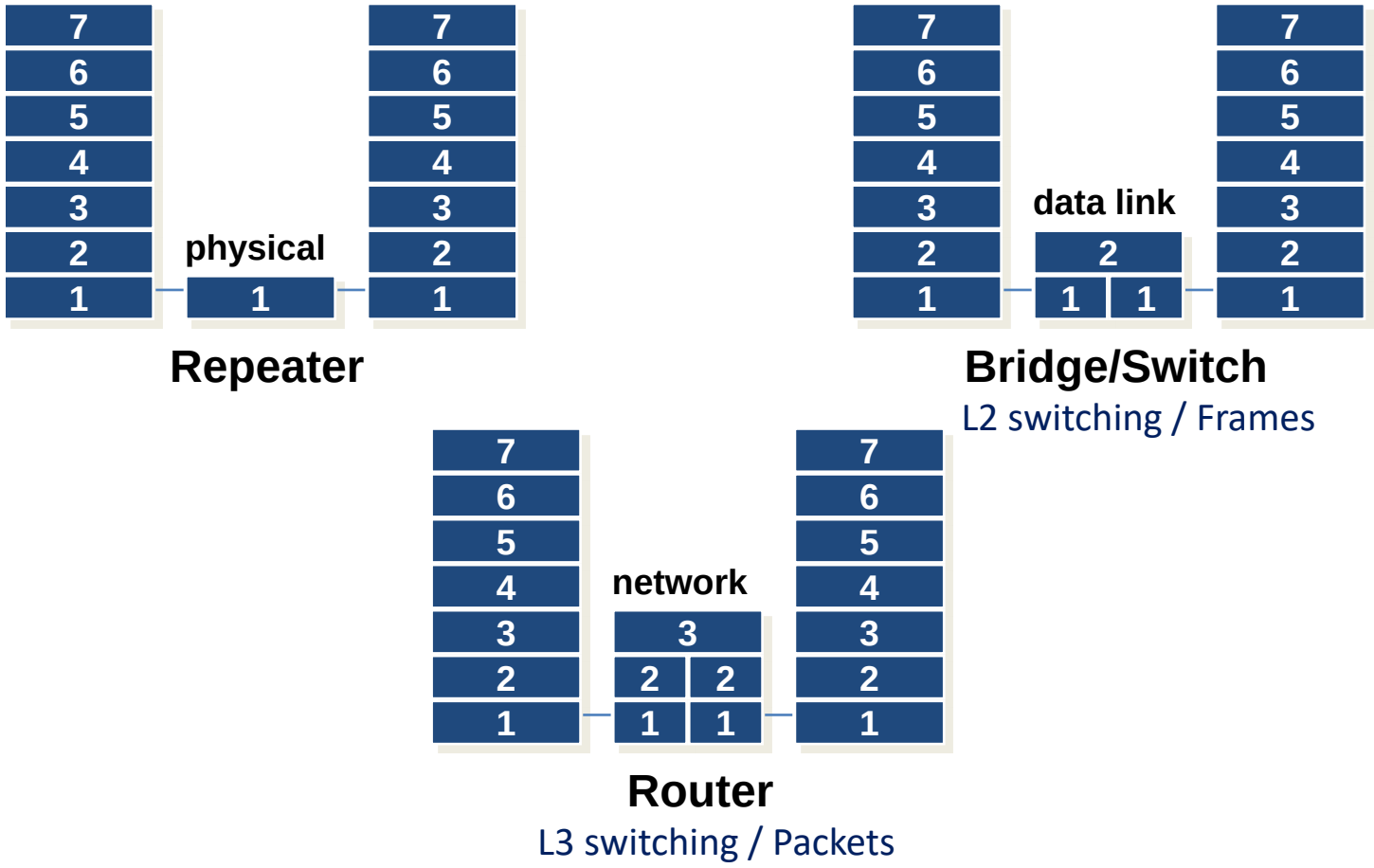
TCP/IP Five Layer Model

- **TCP/IP Layers with corresponding Protocols**

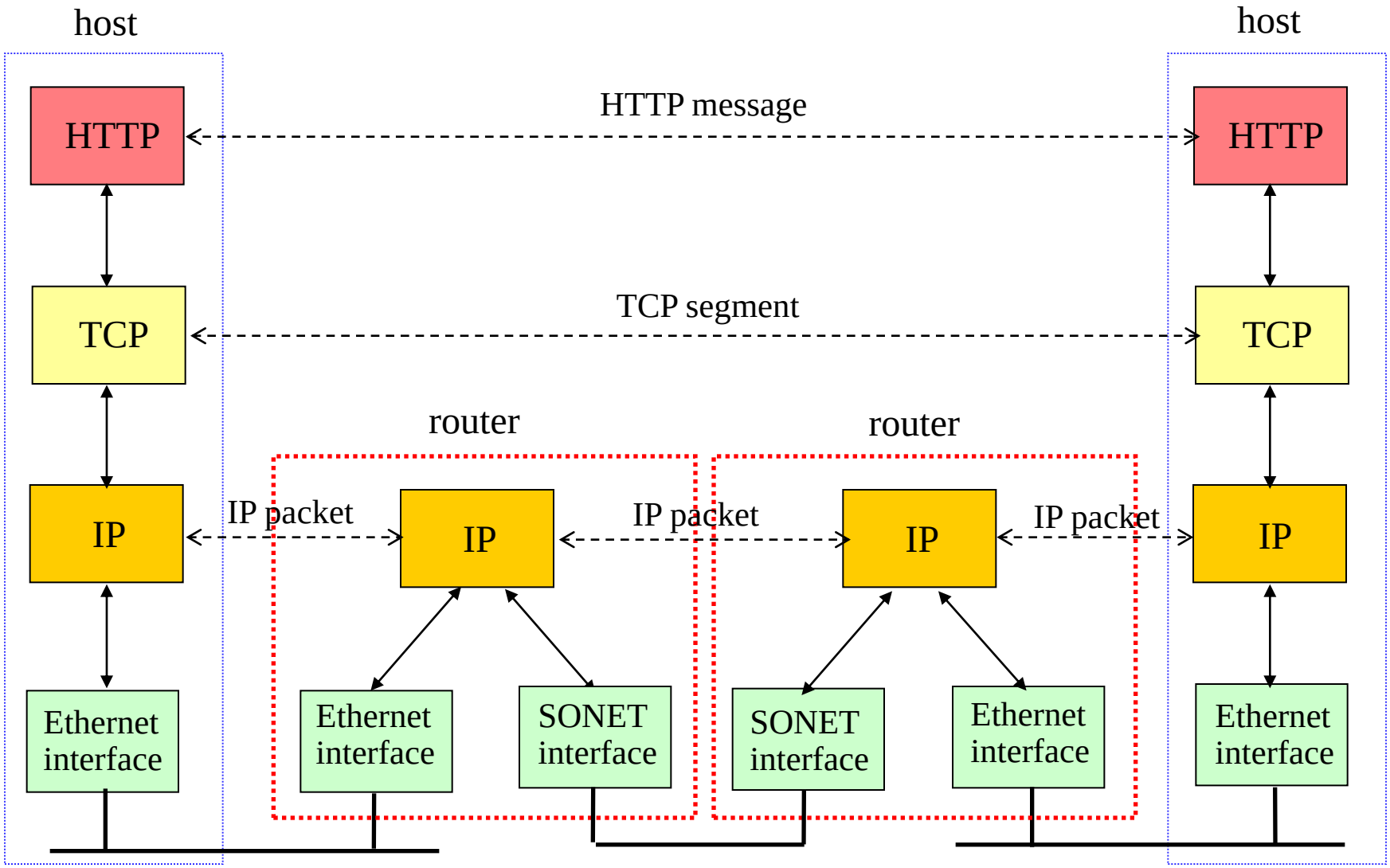
Layer #	Layer Name	Protocol	Protocol Data Unit	Addressing
5	Application	HTTP, SMTP, etc…	Messages	n/a
4	Transport	TCP/UDP	Segments/ Datagrams	Port #s
3	Network or Internet	IP	Packets	IP Address
2	Data Link	Ethernet, Wi-Fi	Frames	MAC Address
1	Physical	10 Base T, 802.11	Bits	n/a

TCP/IP Five Layer Model

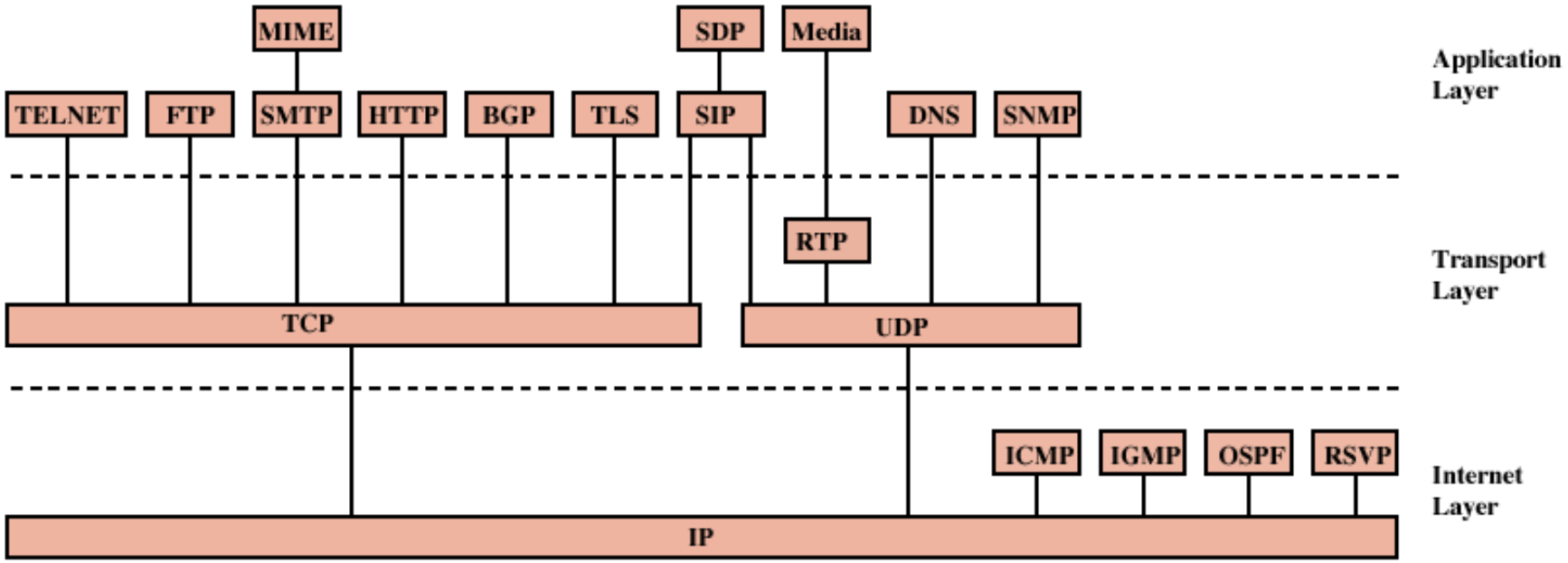
- Level of Internetworking



TCP/IP Five Layer Model

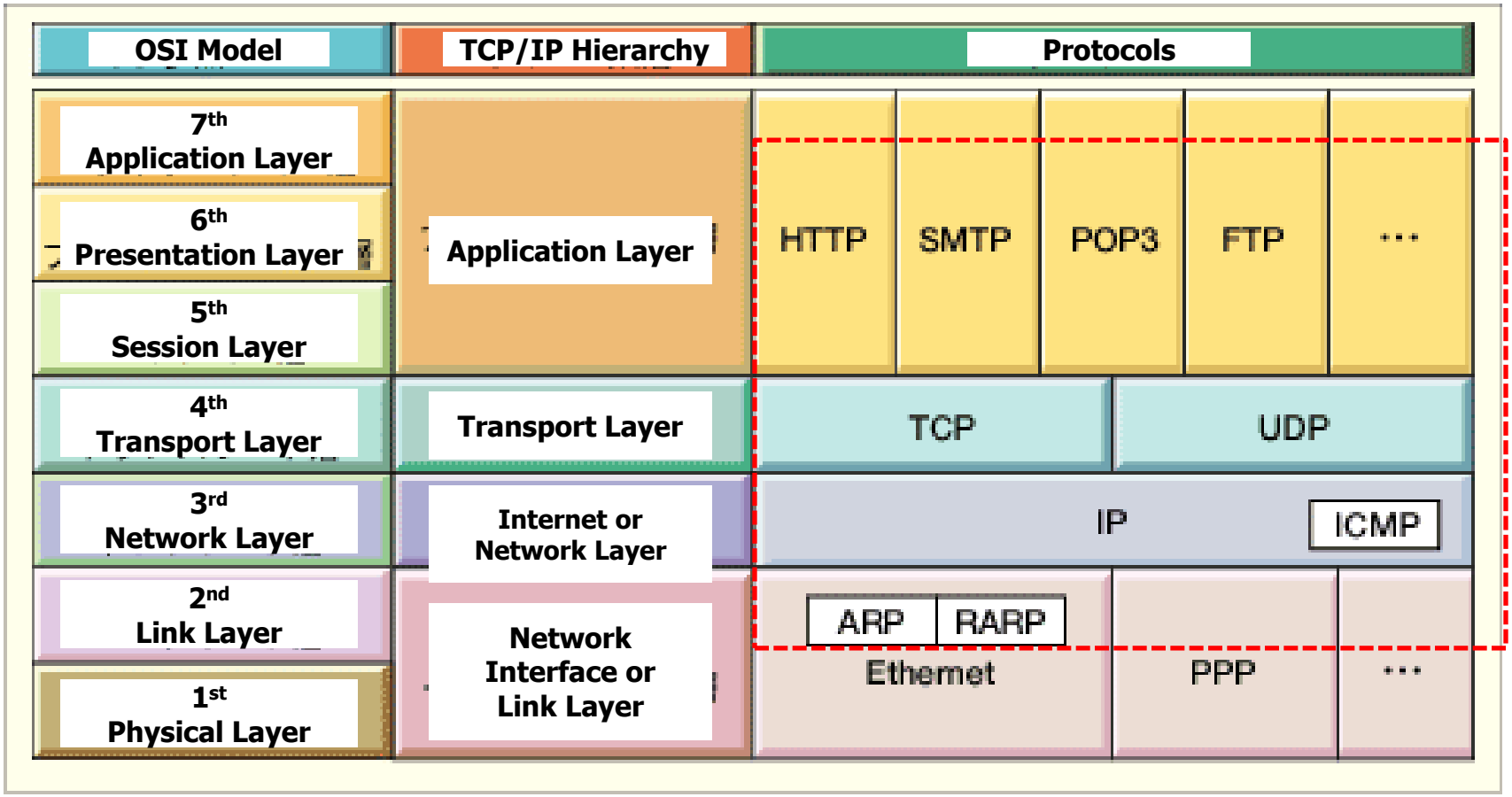


TCP/IP Protocols Suite

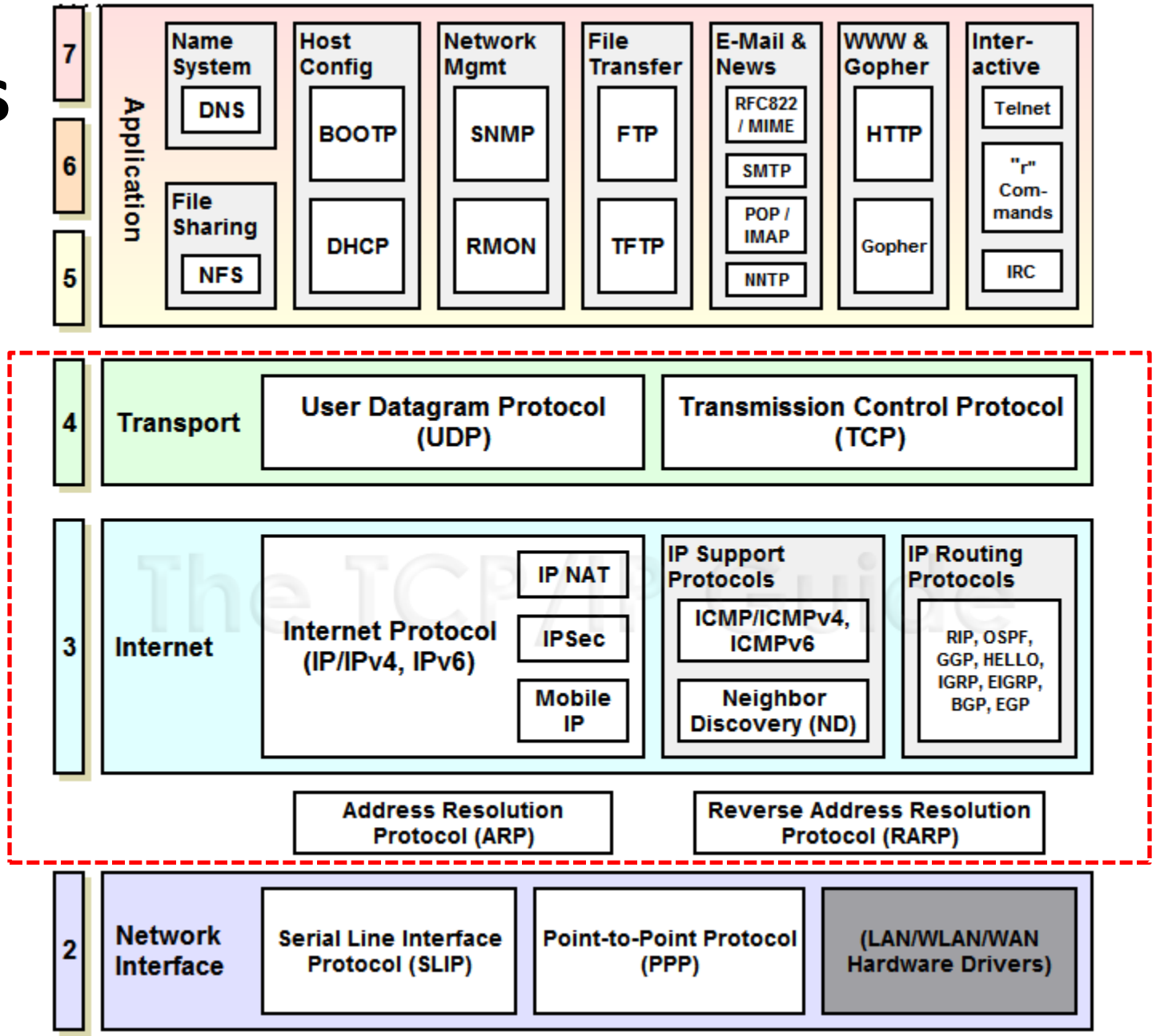


BGP	=	Border Gateway Protocol
DNS	=	Domain Name System
FTP	=	File Transfer Protocol
HTTP	=	Hypertext Transfer Protocol
ICMP	=	Internet Control Message Protocol
IGMP	=	Internet Group Management Protocol
IP	=	Internet Protocol
MIME	=	Multi-Purpose Internet Mail Extension
OSPF	=	Open Shortest Path First
RSVP	=	Resource ReSerVation Protocol
RTP	=	Real-Time Transport Protocol
SDP	=	Session Description Protocol
SIP	=	Session Initiation Protocol
SMTP	=	Simple Mail Transfer Protocol
SNMP	=	Simple Network Management Protocol
TCP	=	Transmission Control Protocol
TLS	=	Transport Layer Security
UDP	=	User Datagram Protocol

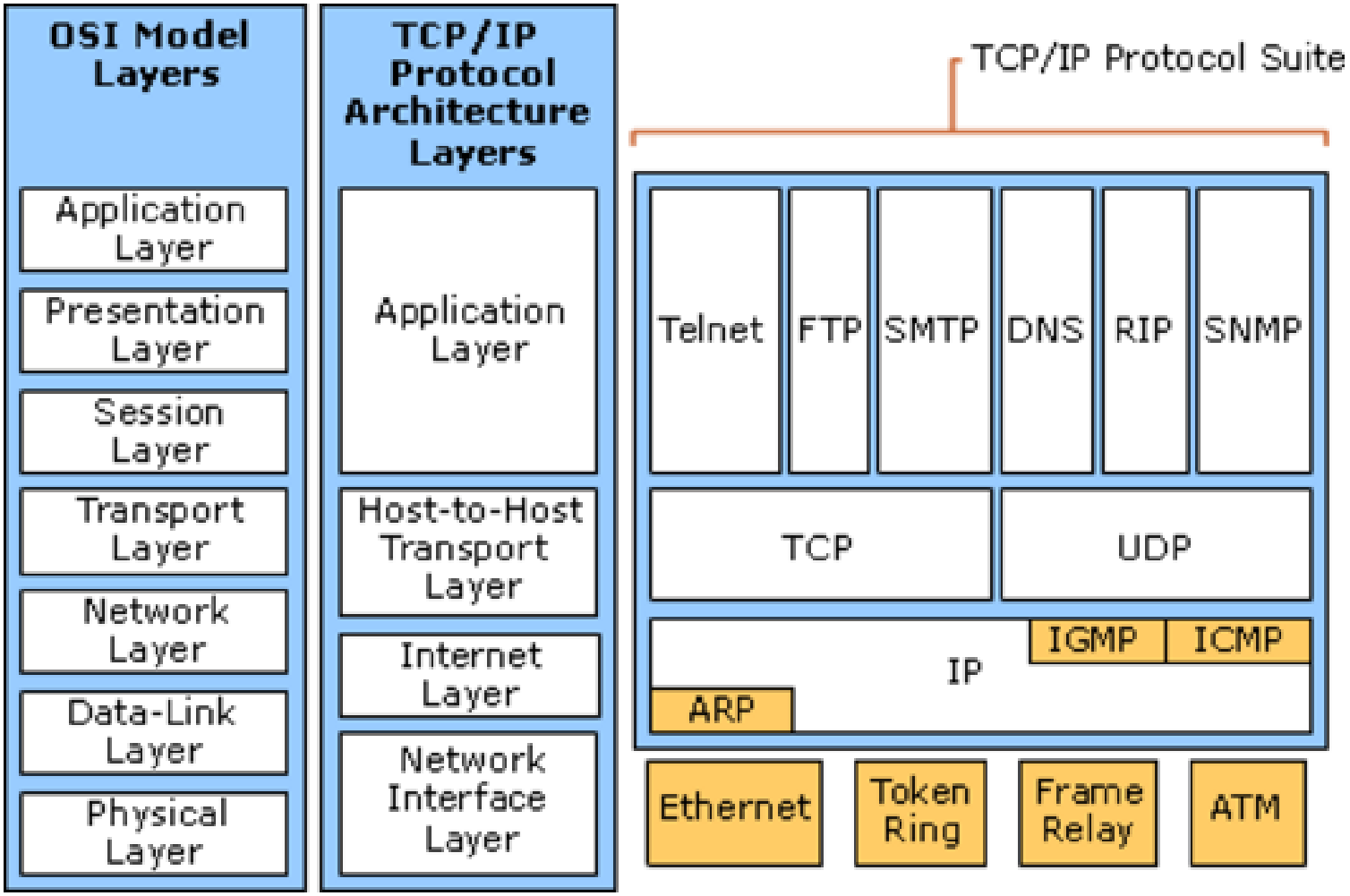
TCP/IP Protocols Suite



TCP/IP Protocols Suite



TCP/IP Protocols Suite



TCP/IP Protocols Suite

Most Common Application Protocols

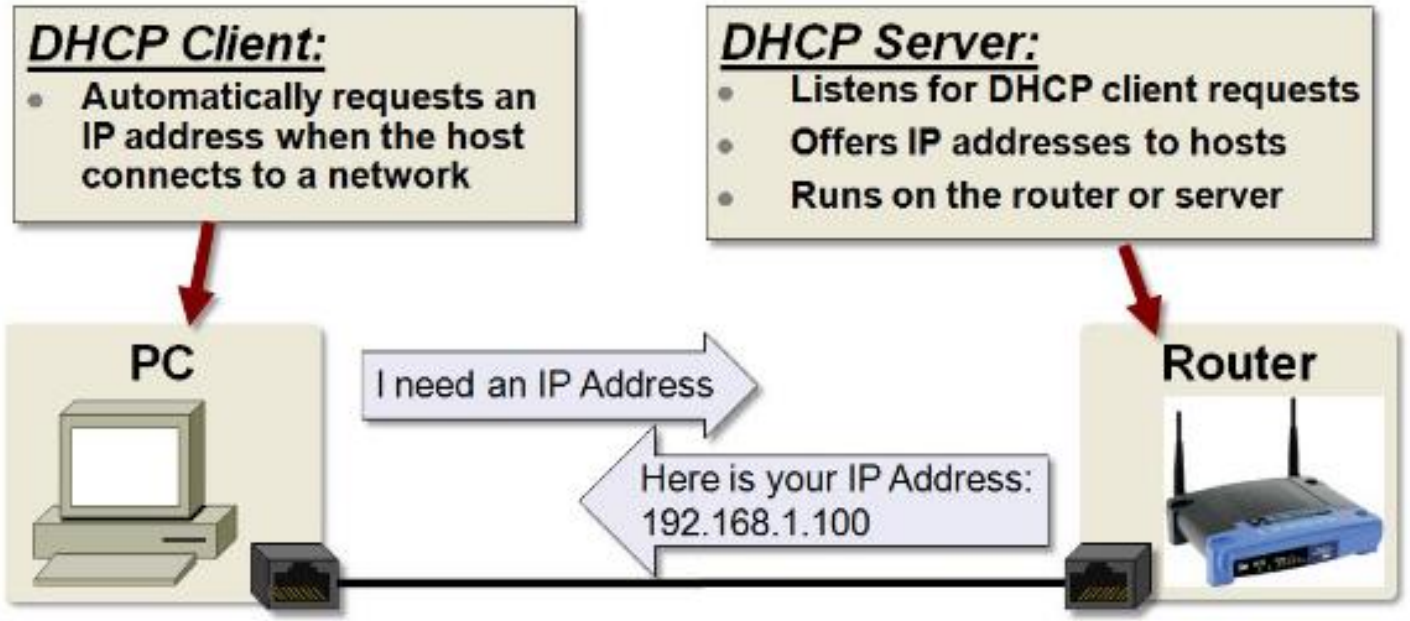
Application	Description
DHCP	Dynamic Host Configuration Protocol assigns IP addresses
DNS	Domain Name System translates website names to IP addresses
HTTP	Hypertext Transfer Protocol used to transfer web pages
NBNS	NetBIOS Name Service translates local host names to IP addresses
SMTP	Simple Mail Transfer Protocol sends email messages
SNMP	Simple Network Management Protocol manages network devices
SNTP	Simple Network Time Protocol provides time of day
Telnet	Bi-directional text communication via a terminal application
TFTP	Trivial File Transfer Protocol used to transfer small amounts of data

Most Common Application Protocols

- **DHCP (Dynamic Host Configuration Protocol)**
  - The dynamic host configuration protocol or DHCP is the application responsible for requesting and offering IP addresses.
  - A DHCP client automatically requests an IP address from a DHCP server when a network is detected. A DHCP server typically runs in a router and offers IP addresses to DHCP clients.

Most Common Application Protocols

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

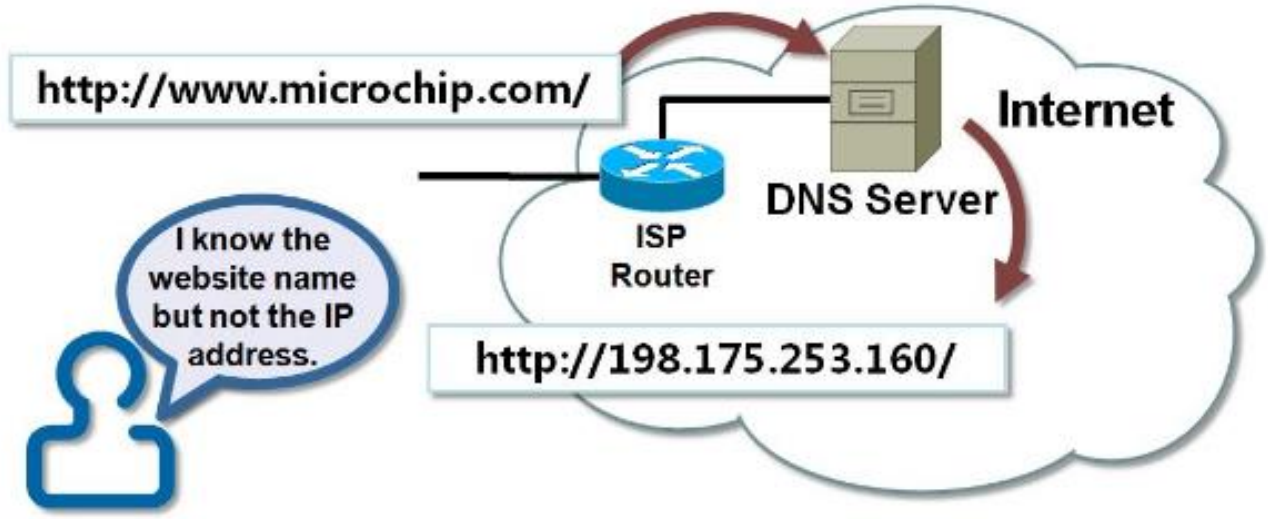


Most Common Application Protocols

- **DNS (Domain Name System)**
  - A Domain Name System (DNS) enables us to browse to a website by providing the website or domain name instead of the website's IP address.
  - It maps domain names to IP addresses. A network host needs the IP address (not the domain or host name) of the web server to generate a Packet.

Most Common Application Protocols

- DNS (Domain Name System)

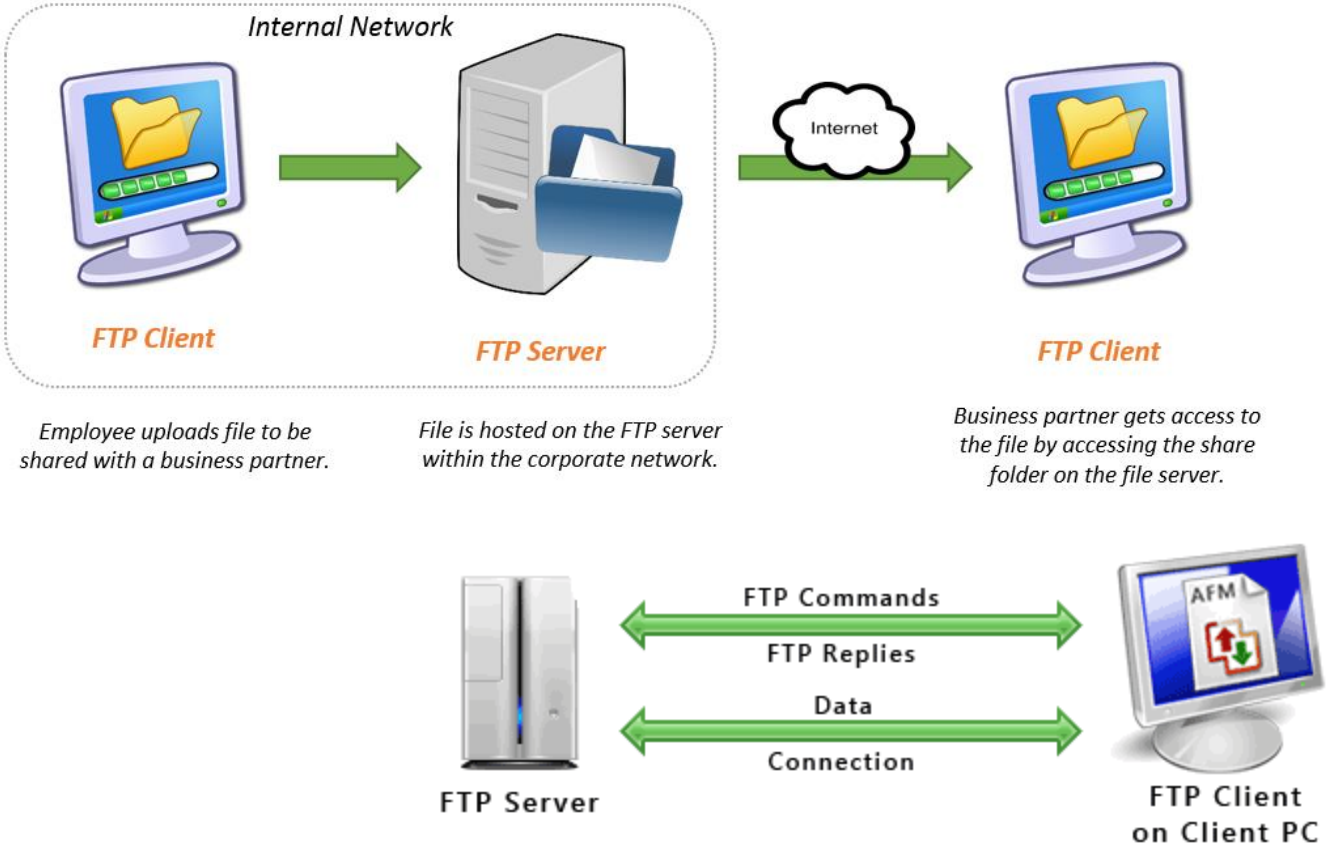


Most Common Application Protocols

- **FTP (File Transfer Protocol)**
  - File Transfer Protocol (FTP) is the commonly used protocol for exchanging files over the Internet. FTP uses the Internet's TCP/IP protocols to enable data transfer.
  - It is a popular protocol for uploading and downloading files, usually those that are too big and would take too long to download via a regular email program as an attachment.
  - FTP is built on a client-server model architecture and uses separate control and data connections between the client and the server.

Most Common Application Protocols

- **FTP (File Transfer Protocol)**

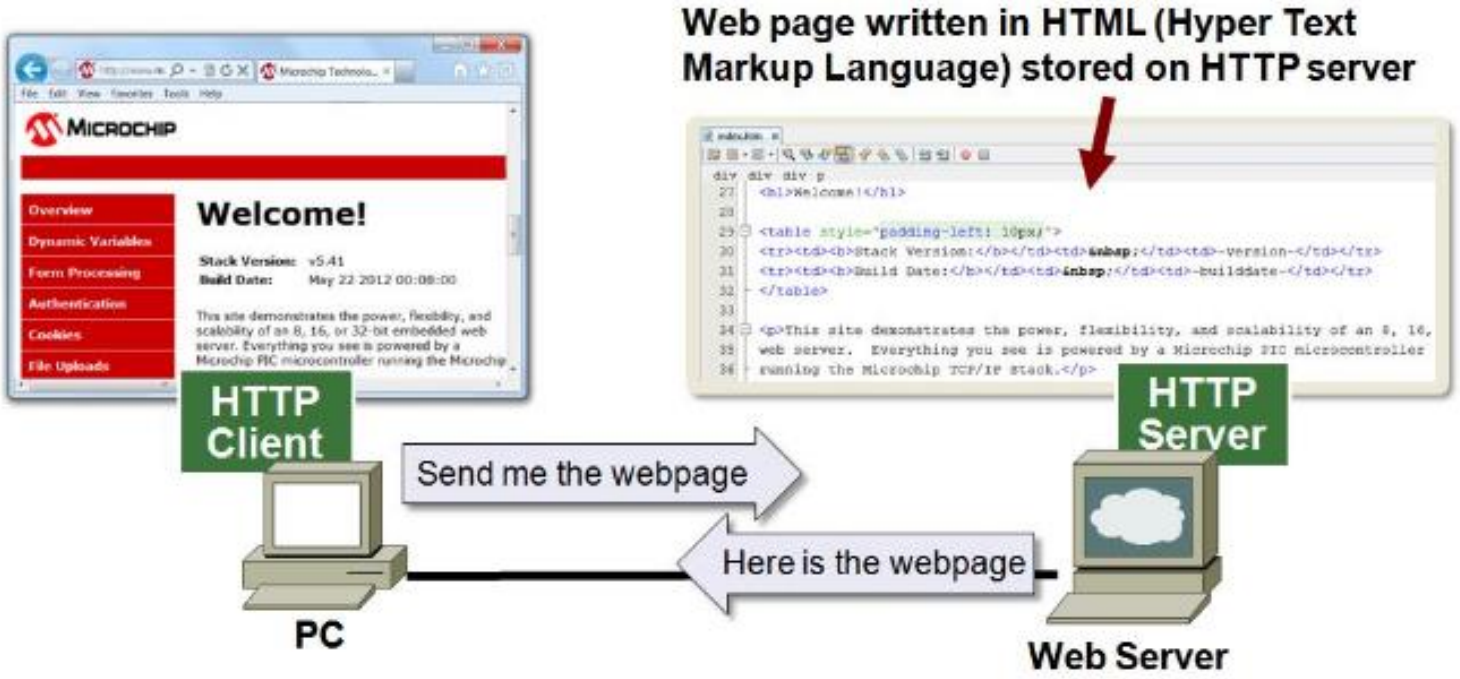


Most Common Application Protocols

- **HTTP (Hypertext Transfer Protocol)**
  - The HyperText Transfer Protocol is the most commonly used TCP/IP application as it transfers web pages from a web server to a web browser.
  - Web pages are written using HTML, which stands for HyperText Markup Language. In other words, the HyperText Transfer Protocol is used to transfer HyperText Markup Language files.
    - World wide web (WWW) is based on HTTP

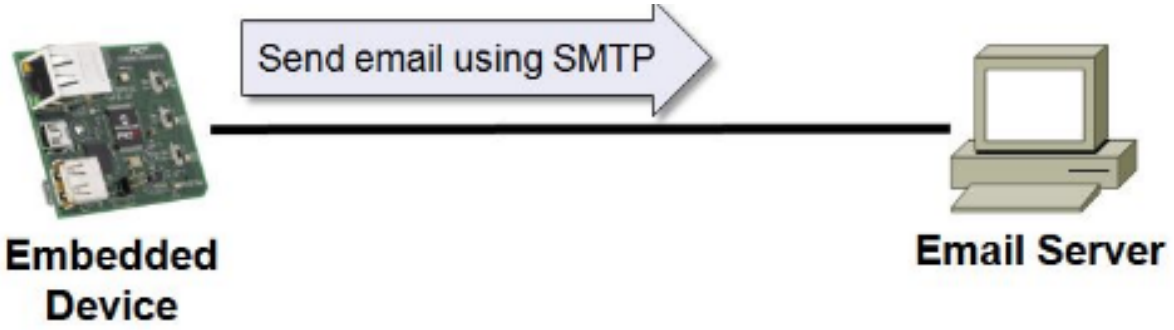
Most Common Application Protocols

- **HTTP (Hypertext Transfer Protocol)**



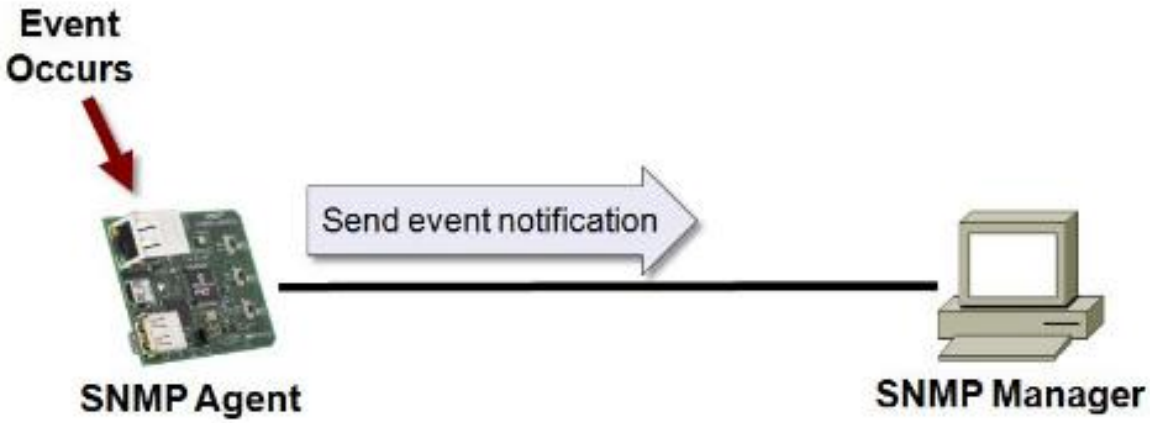
Most Common Application Protocols

- **SMTP (Simple Mail Transfer Protocol)**
  - Your embedded device can be configured to send emails. SMTP or Simple Mail Transfer Protocol would be used for this.



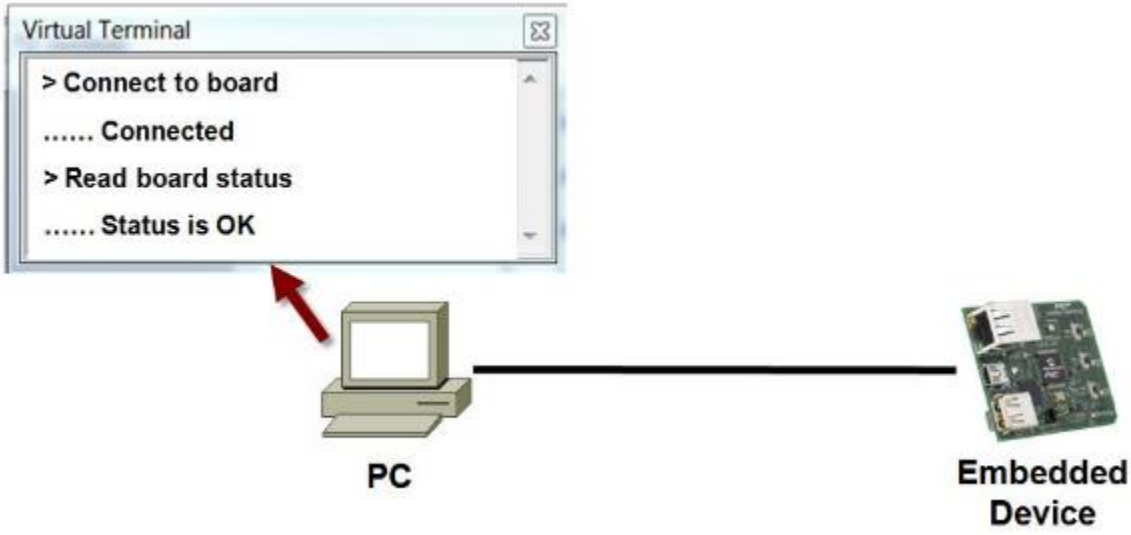
Most Common Application Protocols

- **SNMP (Simple Network Management Protocol)**
  - SNMP stands for Simple Network Management Protocol which manages network devices. It is primarily used to monitor network devices for conditions that may need a users attention.



Most Common Application Protocols

- **Telnet (Bi-directional serial text communication)**
  - Telnet is an application that enables bi-directional text communication via a terminal application like HyperTerm or Tera Term.



Advanced Communication Networks

Muhammad Taha Jilani

Lecture - 11

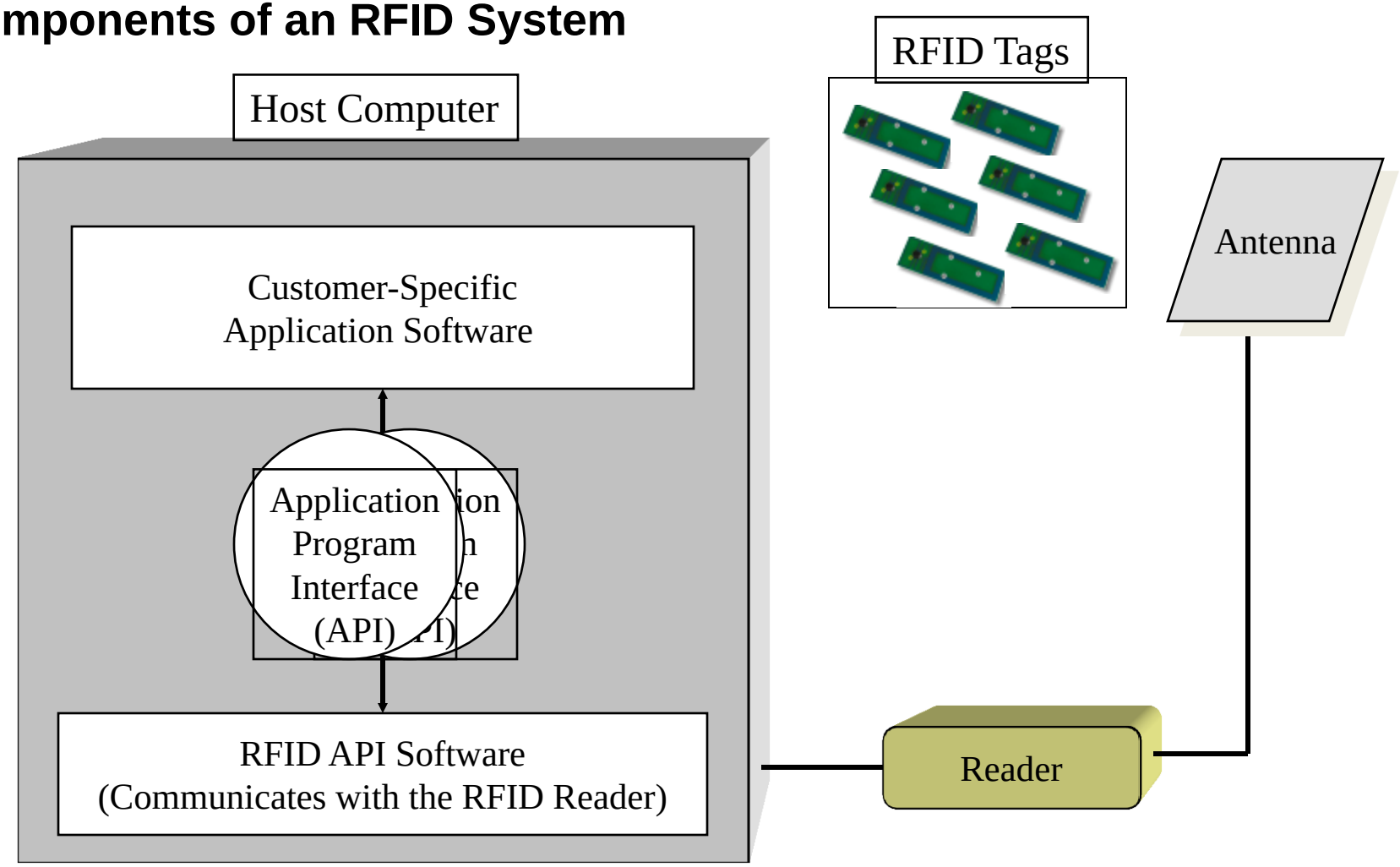
WPAN

Radio Frequency Identification

- Radio Frequency Identification (RFID), is an Automatic Data Capture technology that uses radio-frequency waves to read a movable item to identify, categorize & track.
- It is fast, reliable, and does not require physical line of sight or contact between reader/scanner and the RFID tagged item.

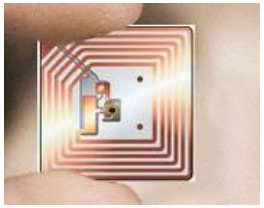
Radio Frequency Identification (RFID)

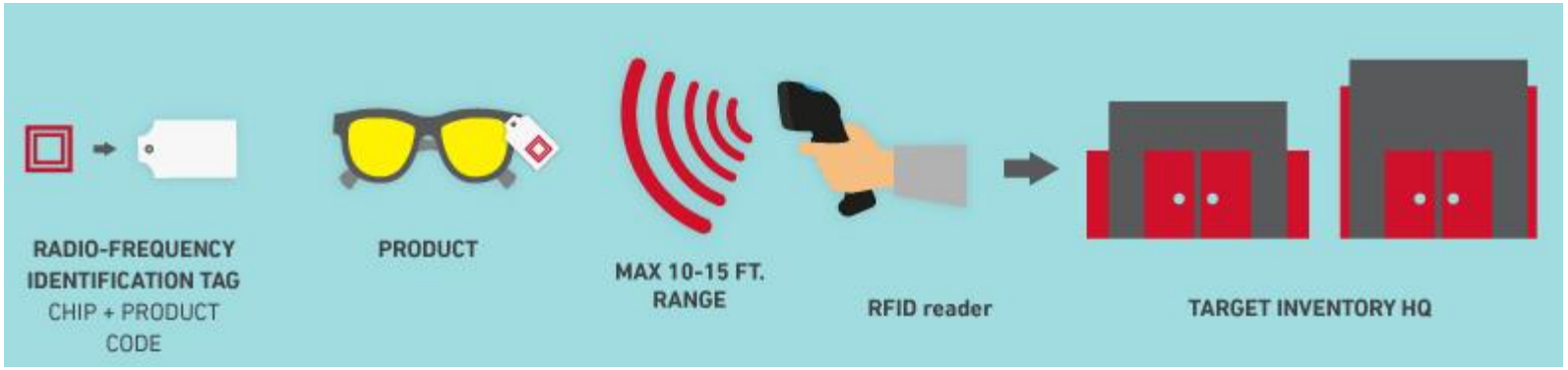
Components of an RFID System



Radio Frequency Identification (RFID)

- Working of RFID
  - Code write onto the Tag
  - Reader/Scanner retrieve that information (manually/automatically)

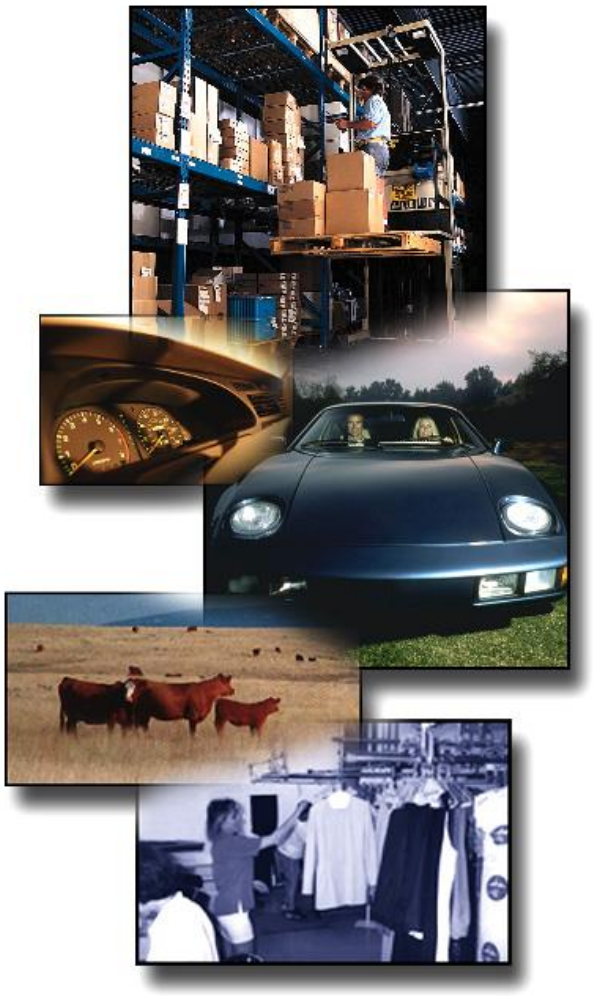




Radio Frequency Identification

RF Tags can be attached to almost anything:

- pallets or cases of product
- vehicles
- company assets or personnel
- items such as apparel, luggage, laundry
- livestock, or pets
- high value electronics such as computers, TVs, camcorders



Radio Frequency Identification

Types of Tags

- Passive Tags
  - No battery
  - Low cost
- Active Tags
  - On-board transceiver
  - Battery – must be replaced
  - Longer range
  - High cost

Radio Frequency Identification

Functionality of Tags

- Read Only :
  - factory programmed
  - usually chipless
  - Tag memory can be factory or field programmed and optionally permanently locked (security)
- Read / Write
  - Data written to the tag left unlocked, can be modified over more than 10,0000 times, allowing the the tag to be reused or updated
  - on-board memory
  - can save data
  - can change ID
  - higher cost

Radio Frequency Identification (RFID)

RFID tags are classified as Class 0 through Class 5, depending on their functionality:

Class 0	UHFl read-only, preprogrammed passive tag
Class 1	UHF or HF; write once, read many (WORM)
Class 2	Passive read-write tags that can be written to at any point in the supply chain
Class 3	Read-write with onboard sensors capable of recording parameters like temperature, pressure, and motion; can be semipassive or active
Class 4	Read-write active tags with integrated transmitters; can communicate with other tags and readers
Class 5	Similar to Class 4 tags but with additional functionality; can provide power to other tags and communicate with devices other than readers

Radio Frequency Identification (RFID)

- Due to flexibility of RFID system, it can be used in several applications however, due to specific nature of application, RFID usually used in following formation
  1. Companion Animals, Livestock and Access Control (low frequency)
  2. Used in Security, Access & Payment Systems (High Frequency)
  3. Used in Supply Chain, Asset Management, Mining, Retail and Livestock (Ultra High Frequency)
  4. Used in Manufacturing & Long Range Asset Management (100-200M) (Active - Battery Operated)

Frequency Ranges

- Low – 100-500 kHz
  - short range, low data rate, cost, & power
- Intermediate – 10-16 MHz
  - medium range and data rate
- High – 850-950 MHz & 2.4-5.8GHz
  - large range, high cost, high data rate
  - needs line of sight

Radio Frequency Identification (RFID)

- RFID Frequency Ranges

Frequency range	Remarks	Allowed Tx Power
< 135 kHz	low frequency, inductive coupling	72 dBµA/m
6.765 - 6.795 MHz	MF Band (ISM), inductive coupling	42 dBµA/m
7.400 – 8.800 MHz	MF Band, used for EAS (electronic article surveillance) only	9 dBµA/m
13.553 -13.567 MHz	**Medium frequency (13.56 MHz, ISM), inductive coupling, wide spread usage for contact less smartcards (ISO 14443, MIFARE, LEGIC, smart labels (ISO 15693, Tag-It, I-Code) and item management (ISO 18000-3).**	**42 dBµA/m**
26.957- 27.283 MHz	MF Band (ISM), inductive coupling, special applications only	42 dBµA/m
433 MHz	UHF (ISM), backscatter coupling, rarely used for RFID as there are more ISM devices working	10 - 100 mW
868 - 870 MHz	UHF (SRD), backscatter coupling	500 mW(Europe)
902 - 928 MHz	UHF (SRD), backscatter coupling	4 W - spread spectrum, (USA/Canada)
2.400 - 2.483 GHz	SHF (ISM), backscatter coupling, several systems, (vehicle identification: 2.446- 2.454 GHz)	4 W - spread spectrum, (USA/Canada), 500 mW (Europe)
5.725 - 5.875 GHz	SHF (ISM), backscatter coupling, rarely used for RFID	4 W USA/Canada, 500 mW Europe

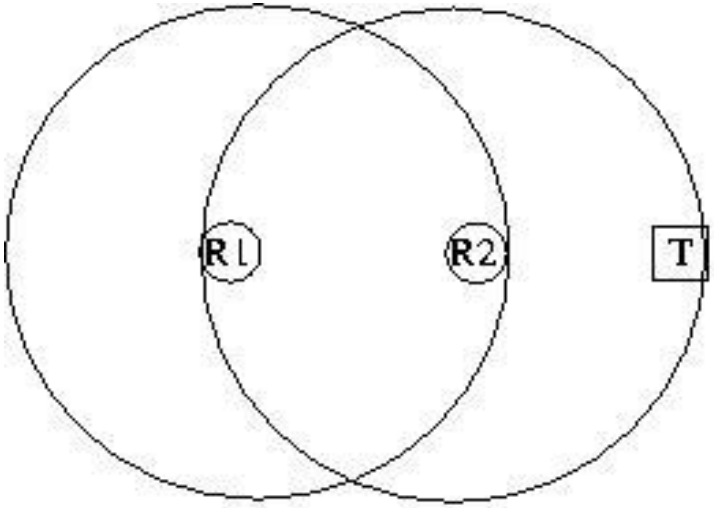
Radio Frequency Identification (RFID)

- To transfer data, it can be modulated by
  - Amplitude Modulation (AM)
  - Frequency Shift Keying (FSK)
  - Phase Shift Keying (PSK)

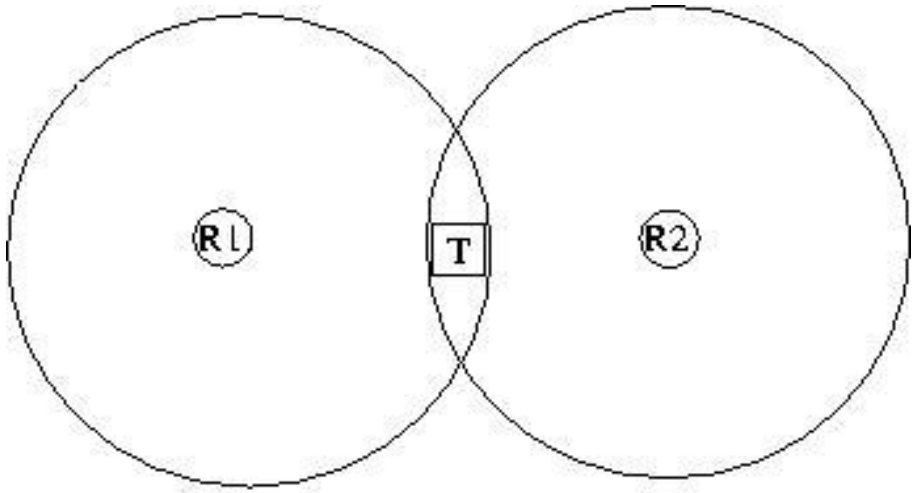
Radio Frequency Identification (RFID)

Reader Collision Problem

- Reader-Reader Interference
- Reader-Tag Interference



Reader to Reader Interference



Reader to Tag Interference

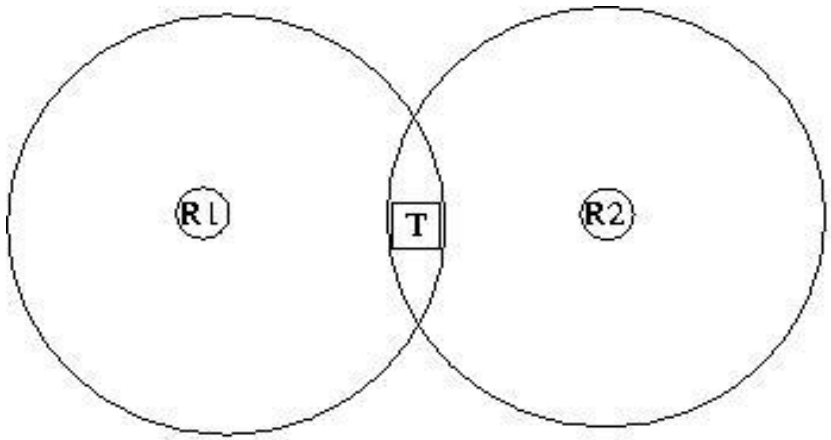
Radio Frequency Identification (RFID)

Reader Collision and Hidden Terminal

- The passive tags are not able to take part in the collision resolution or avoidance

- Consider: RTS-CTS for hidden terminal problem in 802.11
  - RFID: T is not able to send a CTS in response to an RTS from R

- In case multiple readers try to read the same tag, the tag cannot respond selectively to a particular reader



R2 is a hidden terminal for R1 – T communication

Radio Frequency Identification (RFID)

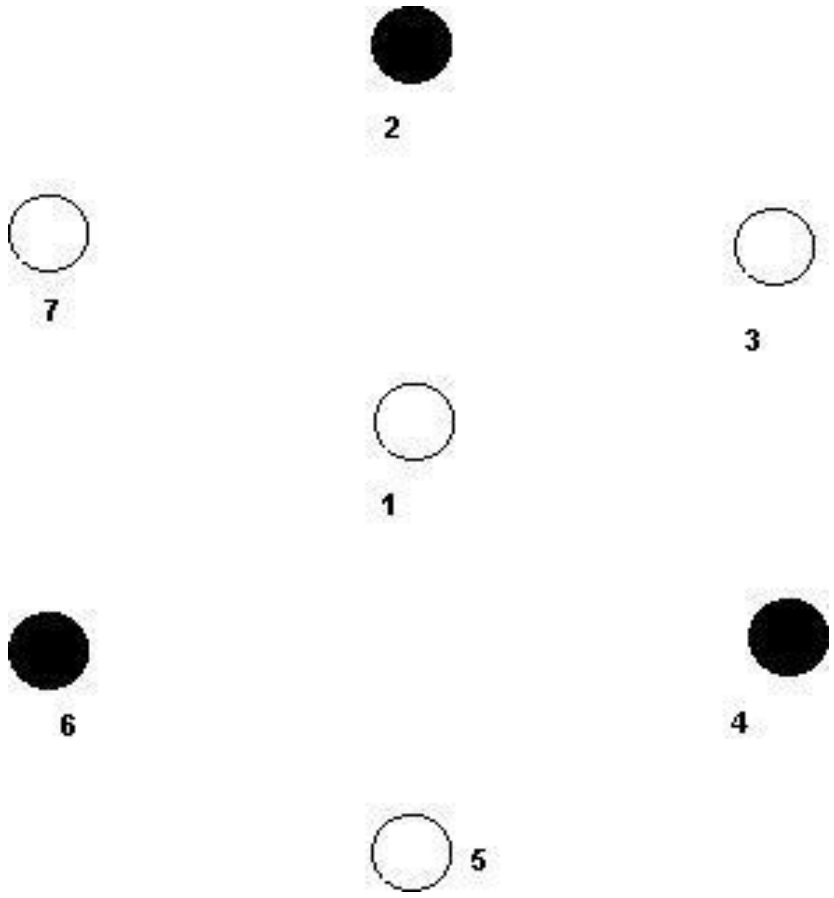
- TDMA based solution
- Assign different time slots and/or frequencies to nearby readers
- Only reader to reader interference
  - Assign different operating frequencies
- Only multiple reader to tag interference
  - Assign different time slots for operation
- Both types of interference
  - First allot different time slots, then frequencies

Radio Frequency Identification (RFID)

Beacon based solution

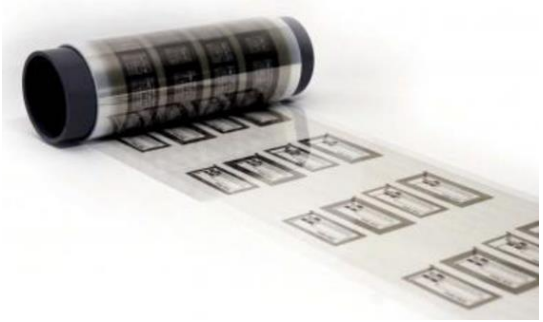
- A reader while reading tag, periodically sends a beacon on the control channel

- Assumptions
  - Separate control channel between readers
  - The range in the control channel is sufficient for a reader to communicate with all the possible readers that might interfere in the data channel



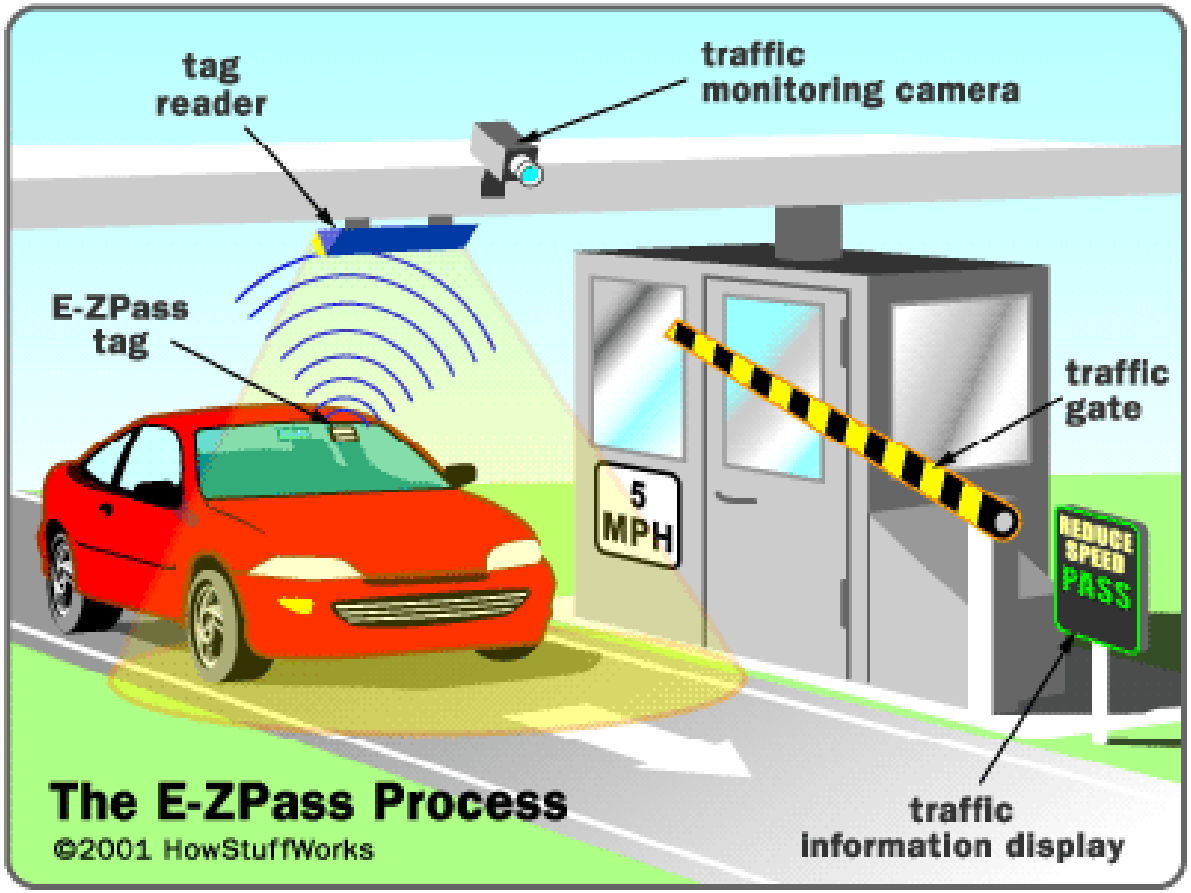
Radio Frequency Identification (RFID)

- Features of RFID
  - Read data without visual access
  - Ability to read data from moving objects
  - Can read at distance, from 3cm to 100 metres
  - Secure the tag data
  - Can also update data in the tag (write)
  - Automated reading of tags (within a industrial apps)
  - Variety of tag form according to the application



Applications

- Automated Toll Collection



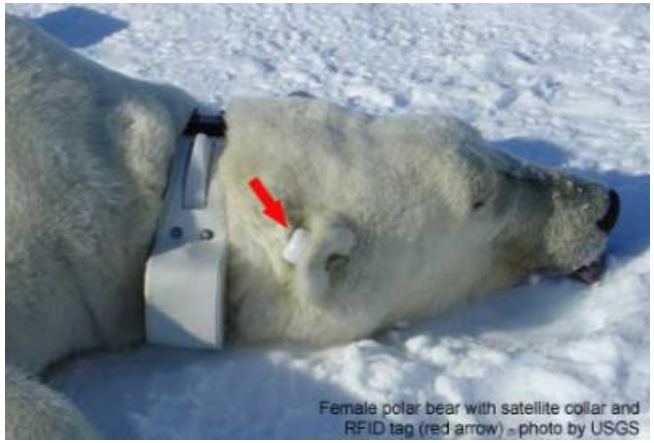
Applications

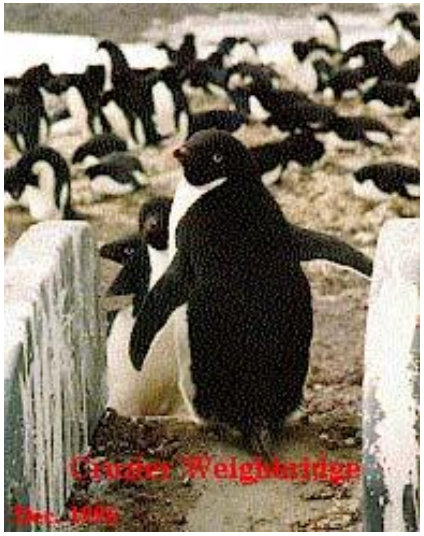
Smart Grocery Store

- Add an RFID tag to all items in the grocery.
- As the cart leaves the store, it passes through an RFID transceiver
- The cart can checkout in seconds.

Applications

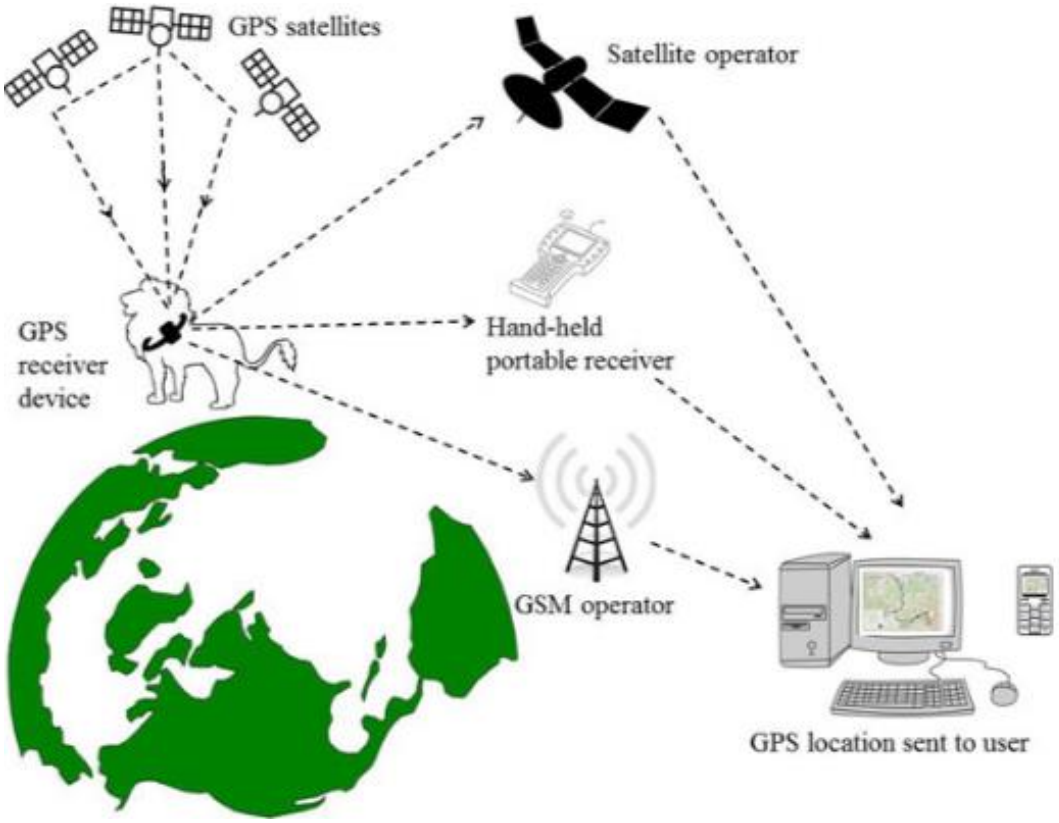
- Wild Life Tracking (For research)





Applications

- Wild Life Tracking (For research)



Alongwith GPS

Applications

- RFID Application
  - RFID Barcode Reader
    - For Inventory management in hyper stores

RFID count is 100 times as fast as a barcode count
Read at a time

TCP/IP PROTOCOL SUIT

(Continued)

TCP/IP Protocols Suite

- Not all systems on a network need to implement all five layers of TCP/IP.
- Devices using the TCP/IP protocol stack fall into two general categories:
  - *host* or *end system* (ES)
  - *intermediate node/system* (IS)- that is often a router
- Intermediate nodes usually only involve the first three layers (PHY-to-NET)
- Each layer has an *interface* with above/below layers, and it provides defined services, but these services are not standardized and vary widely by operating system.
- TCP/IP is designed to be comprehensive and flexible (that's the reason for its 40 years of success), even layers can be split when necessary, and new service interfaces defined.

TCP/IP Protocols Suite

- **Transport Protocols - Application Needs?**

Data loss

- Some applications (e.g., audio) can tolerate some loss
- Other applications (e.g., file transfer, telnet) require 100% reliable data transfer

Timing

- Some applications (e.g., Internet telephony, interactive games) require low delay to be “effective”

Bandwidth

- Some applications require a minimum amount of bandwidth to be “effective”
- Other applications (“elastic apps”) will make use of whatever bandwidth they get

TCP/IP Protocols Suite

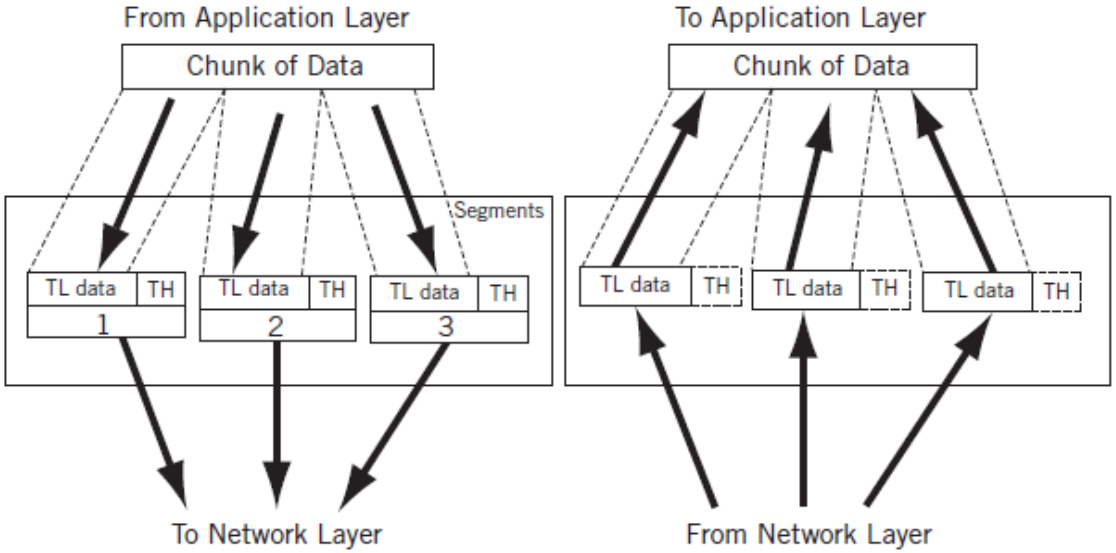
- Transport Service Requirements of Common Applications

Application	Data loss	Bandwidth	Time Sensitive
file transfer	no loss	elastic	no
e-mail	no loss	elastic	no
web documents	no loss	elastic	no
real-time audio/ video	loss-tolerant	audio: 5Kb-1Mb video:10Kb-5Mb	yes, 100's msec
stored audio/video	loss-tolerant	same as above	yes, few secs
interactive games	loss-tolerant	few Kbps	yes, 100's msec
financial apps	no loss	elastic	yes and no

Transport layer Protocols

Most Common Transport Protocols

- The Transport layer (also known as the Host-to-Host Transport layer) provide transport services between Application and Network layes.
- The core protocols of the Transport layer are
  - User Datagram Protocol (UDP)
  - Transmission Control Protocol (TCP)



Transport layer Protocols

- **User Datagram Protocol (UDP)**
  - UDP provides a one-to-one or one-to-many,
    - connectionless (no session information is kept by hosts),
    - unreliable (no guarantees of any QoS parameters, not even delivery)communications service.
  - UDP is used when the amount of data to be transferred is small (such as data that fits into a single packet), when you do not want the overhead of establishing a TCP connection, or when the applications or upper layer protocols provide reliable delivery.

Transport layer Protocols

- **User Datagram Protocol (UDP)**
  - A layer on the top of IP layer
  - Adds Packet length + Checksum (opt.)
    - A small guard against corrupted packets
  - Also source and destination *ports*
    - Ports are used to associate a packet with a specific application at each end
  - Still unreliable:
    - Duplication, loss, out-of-orderness possible

Optional in IPv4, but mandatory with IPv6

Transport layer Protocols

- **User Datagram Protocol (UDP)**
  - UDP provides application multiplexing (via port numbers) and integrity verification (via checksum) of the header and payload.

Transport layer Protocols

User Datagram Protocol (UDP)

- **Applications**
  - UDP is used by many common network applications, including
    - DNS,
    - IPTV streaming media applications,
    - voice over IP (VoIP),
    - Trivial File Transfer Protocol (TFTP),
    - Online games.
  - UDP is required for multicast applications.

Transport layer Protocols

Interaction between Client-Server while transporting segments involves Sockets/Ports

Sockets, or Ports

- Sockets, or ports, are a very low level software, that allows computers to talk to one another
- For each client–server interaction, there is a socket on each host at the endpoints of the network.
- The sockets at each end uniquely identify that particular client–server interaction, although the same sockets can be used for subsequent interactions.
- Sockets are usually written in IPv4 and IPv6 by adding a colon (:) to the IP address
  - 10.10.12.77:17
  - [FC00:490:f100:1000::1]:80

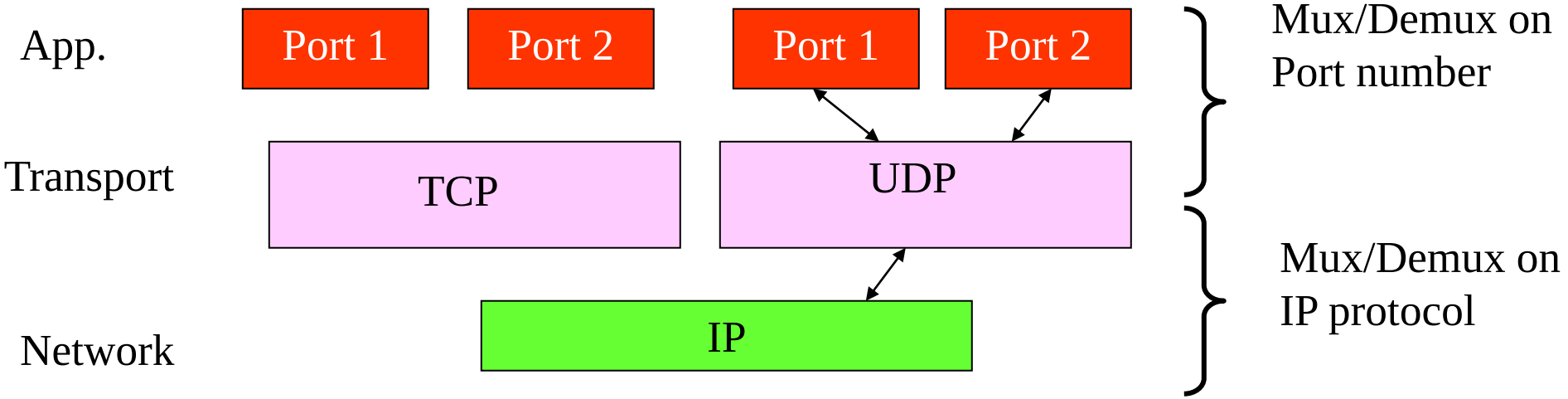
Transport layer Protocols

Sockets, or Ports

- When you send information from one computer to another, you send it to a port on the receiving computer
  - If the computer is “listening” on that port, it receives the information
  - In order for the computer to “make sense” of the information, it must know what protocol is being used
- Common port numbers are 80 (for web pages), 23 (for telnet) and 25 and 110 (for email)
- Port numbers above 1024 are available for other kinds of communication between different programs

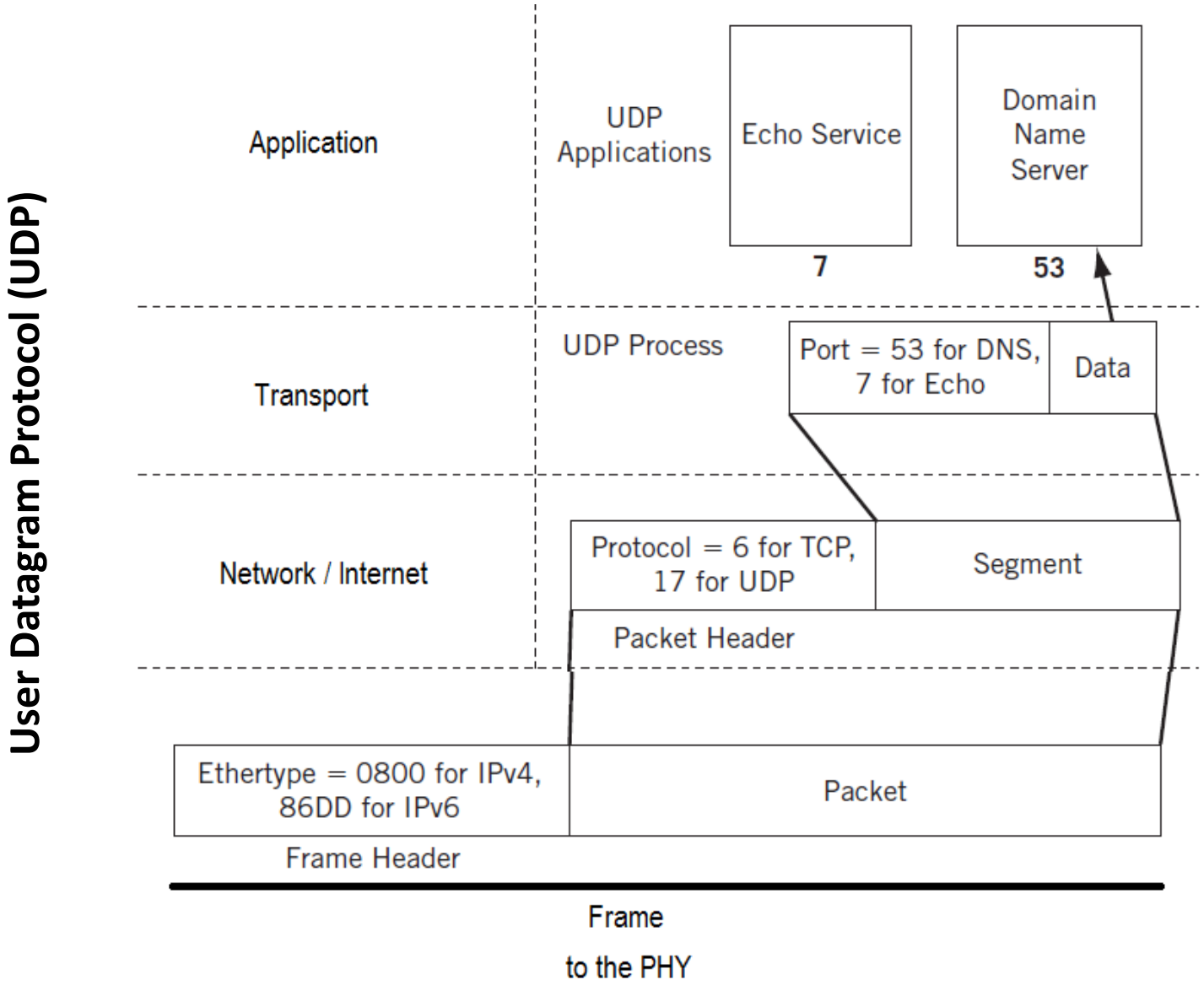
Transport layer Protocols

- **User Datagram Protocol (UDP)**



- Provides unreliable, connectionless on top of IP
- Minimal overhead, high performance
  - No setup/teardown, 1 datagram at a time
- Application responsible for reliability
  - Includes datagram loss, duplication, delay, out-of-sequence, multiplexing, loss of connectivity

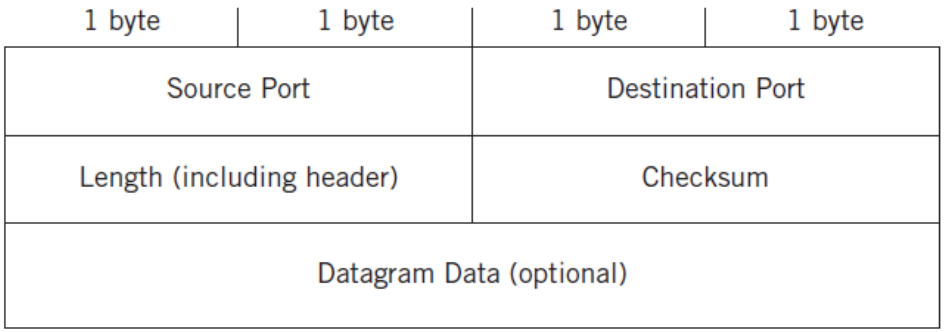
Transport layer Protocols



Transport layer Protocols

- **UDP Header**
- The header added to messages by the Transport layer includes more than just the source and destination port numbers.

UDP packets, called user datagrams, have a fixed-size header of 8 bytes.



Field	**Purpose**
Source Port	16-bit port number identifying originating application
Destination Port	16-bit port number identifying destination application
Length	Length of UDP datagram (UDP header + data) The minimum length is 8 (the header alone), and the maximum value is 65,353.
Checksum	Checksum of UDP header and data

Transport layer Protocols

Most Common Transport Protocols

- **Transmission Control Protocol (TCP)**
  - TCP is as complex as UDP is simple, but with same concept as both are end-to-end protocols.
  - But the major difference between UDP and TCP is that TCP is connection oriented.
  - TCP provides a one-to-one, connection-oriented, reliable communications service. TCP handles the establishment of a TCP connection, the sequencing and acknowledgment of packets sent, and the recovery of packets lost during transmission.

Transport layer Protocols

- **Transmission Control Protocol (TCP)**
  - Major Internet applications such as the World Wide Web, email, remote administration, and file transfer rely on TCP.
  - TCP protocol operations may be divided into three phases. Connections must be properly established in a multi-step handshake process (*connection establishment*) before entering the *data transfer* phase. After data transmission is completed, the *connection termination* closes established virtual circuits and releases all allocated resources

Transport layer Protocols

Most Common Transport Protocols

- **TCP Implementation**
  - Connections are established between client to server and back, using a *three-way handshake,* within these connection
    - Data is divided up into packets by the operating system
    - Packets are numbered, and received packets are acknowledged
    - Connections are explicitly closed
      - (or may abnormally terminate)

Transport layer Protocols

- **Client–server interaction with TCP three-way handshake**
  - TCP uses unique terminology for the connection process, a single bit called the SYN (synchronization) bit is used to indicate a connection request.
    - This single bit is still embedded in a complete 20-byte (usually) TCP header, and other information, such as the initial sequence number (ISN) used to track segments, is sent to the other host.
  - Connections and data segments are acknowledged with the ACK bit,
  - A request to terminate a connection is made with the FIN (final) bit.

Transport layer Protocols

- **Client–server interaction with TCP three-way handshake**

How TCP is reliable?