IT 2nd material

Network

بِسْمِ ٱللَّهِ ٱلرَّحْمَٰنِ ٱلرَّحِيمِ

Lecture 2

Chapter 5:

PROTOCOLS

NETWORK PROTOCOL

A protocol is a set of rules for communication between computers on a network. These rules are guidelines that regulate and govern the following characteristics of a network.

- Allowed physical topologies

- Access method

- Cables type

The essential elements of a protocol are semantics, syntax, and timing.

Syntax:

It refers to syntax, data structure, or format, which is the order in which they occur. For example, a simple protocol might expect the first eight bits of data to be the sender's address, the second eight bits which are the destination address, and the rest of the stream to be the message itself.

Semantics:

It refers to the semantic meaning of each bit section. How a pattern is interpreted and the actions to take based on that interpretation.

Protocol stack:

Hosts connected to network utility programs provide a user with an application such as email, file transfer, and access to Web applications.

The collection of protocols that define the various interfaces between all the layers is called a protocol stack.

Types of Protocols:

There are many standard protocols. Standard protocols have their advantages and disadvantages, the only interesting aspect of the protocols, if you want to communicate with other computers is that their computer or device must support the right. Protocols are implemented in either hardware or software.

Popular protocols:

Address Resolution Protocol:

On the physical level, routers and hosts are identified by their physical address, which is a local address. For communication with the same network, the physical address can meet the target. Communication between different networks, it is necessary both the physical address (MAC) and logical (IP), the user should be able to assign a logical address corresponding to a physical address and vice versa.

Two protocols are used:

ARP maps the logical address to a physical address.

RARP assigns the physical address to a logical address.

1- Address Resolution Protocol (ARP)

Address Resolution Protocol (ARP) contacts a physical address with its IP address.

-Each time a server (router) needs to determine the physical address of another host (router) on the network, It broadcasts an ARP query packet containing the physical address of the IP receiver network.
-All devices on the network and routers receive the packet checks for the IP address.
-The recipient buried identifies your IP address and responds with an ARP response packet including its IP and physical address.
- The sender can send all packets ordained for this receiver.

2- Reverse Address Resolution Protocol (RARP)

All devices and the routers are assigned a single logical address, which is required to create the IP datagram.
- This address is usually stored in a configuration file, which is stored on the hard disk This reverse address resolution protocol (RARP) is used to determine the logical address when the physical address is known.
- A device started first getting the physical address of the NIC. The device creates an RARP request packet and transmitted it over the network.
- Another device on the network work as a server and have all the IP address responds with a RARP response packet. This package includes the IP address of the sender.

ARP: Finds the MAC Address when the IP Address is known.

RARP: Finds the IP Address when the MAC Address is known.

Internet Control Message Protocol (ICMP)

Internet Control Message Protocol (ICMP) is an extension of the Internet Protocol that supports packets containing error messages, control, and information.

There are two types of messages ICMP request messages and error reporting.

User Datagram Protocol (UDP)

User datagram protocol (UDP) is a transport layer connectionless protocol that uses port numbers to make available process-to-process communication.

It enables process-to-process communication using **port numbers**.

Unlike TCP, UDP does not establish a connection before sending data, making it faster but less reliable.

It operates at **Layer 4** of the OSI model (Transport Layer).

UDP Header Structure:

1. **Source Port Number** (16 bits): Identifies the sender's port.
2. **Destination Port Number** (16 bits): Identifies the receiver's port.
3. **Total Length** (16 bits): Specifies the size of the entire datagram (header + data).
4. **Checksum** (16 bits): Ensures data integrity during transmission. *(يُستخدم Checksum للتحقق من أن البيانات لم تتلف أثناء الإرسال.)*

How UDP Works:

1. The application data is divided into smaller units called **datagrams**.
2. Each datagram is encapsulated with a UDP header containing source and destination port numbers.
3. The **IP address** of the sender is included in the datagram for proper routing.
4. Datagrams are sent individually over the network without establishing a connection.

Characteristics:

- **Connectionless:** No handshake between sender and receiver. *(يعني أن البيانات تُرسل مباشرة بدون فتح قناة اتصال مخصصة)*
- **No Acknowledgment:** The receiver does not confirm whether data was received.
- **No Sequencing:** Packets may arrive out of order.
- **Lightweight:** Less overhead compared to TCP, making it faster.
- **Unreliable:** Does not guarantee data delivery or order.

Applications:

- **Audio/Video Streaming:** Prioritizes real-time delivery over reliability.
- **Online Gaming:** Reduces latency for a better gaming experience.
- **DNS Lookups:** Fast communication with minimal data.

Comparison with TCP:

Feature	TCP	UDP
Connection Type	Connection-oriented	Connectionless
Reliability	Reliable	Unreliable
Flow Control	Yes	No
Acknowledgment	Yes	No
Use Case Examples	File transfer, Email	Streaming, Gaming

Internetwork packet exchange / sequenced packet exchange

IPX and SPX:

- **IPX**: Stands for *Internetwork Packet Exchange*, and it operates at the **network layer** (Layer 3) of the OSI model. It is used to enable communication between devices within a network, allowing data transfer between client and server in Novell NetWare.
- **SPX**: Stands for *Sequenced Packet Exchange*, and it works at the **transport layer** (Layer 4). SPX is a connection-oriented protocol that ensures data is sent in a reliable, ordered manner.

Packet Structures:

- **802.3 Ethernet Packet Structure**: Contains fields like:
  - *Destination Node*: The receiving device.
  - *Source Node*: The sending device.
  - *Length*: The length of the data portion of the packet.
  - *Data*: The actual data being transmitted.
  - *Pad*: Padding to ensure the packet is the correct size for the network.
- **IPX Packet Structure**: Includes fields such as:
  - *Destination Network (2 bytes)*: The network address of the destination device.
  - *Source Network*: The network address of the sending device.
  - *Transport Control*: Controls the transport layer communication.
  - *Checksum*: Ensures the integrity of the data (إذا كان هناك خطأ في البيانات، يمكن التحقق باستخدام الـ Checksum).
  - *Destination Node*: The destination device's address.
  - *Source Node*: The source device's address.
  - *Frame Check Sequence (CRC)*: A method for detecting errors in the packet.

- *Source Socket and Destination Socket*: Identifies the specific application or process communicating.

Data Link Control (DLC)

Data link control protocols (DLC) are transfer protocols used in the data link layer. **DLC protocol is both synchronous and asynchronous**.

Types of protocols:

- **Synchronous protocols**: Synchronization exists between the sender and receiver during data transmission. Examples: **HDLC** and **SDLC**.
- **Asynchronous protocols**: No synchronization between the sender and receiver during data transmission.

Synchronous Protocols:

- **HDLC (High Data Link Control)**:
  - Uses **bit-oriented frames**, meaning data is transmitted as a series of bits.
  - Ensures **error-free data transmission** in the correct order.
  - Can work in **half-duplex** (one-way at a time) or **full-duplex** (two-way communication) modes.
- **SDLC (Synchronous Data Link Control)**:
  - Uses **a frame format similar to HDLC**.
  - Was mainly used for **connecting computers to mainframes**.

Current Use:

- **HP** uses **DLC protocols** for network printers and continues to support older versions of **Windows**, like **Windows XP**.

- These protocols are mostly needed for older printers, not modern devices.

HTTP (Hypertext Transfer Protocol)

is the protocol used for transferring data over the web between clients (typically web browsers) and servers. It operates at the **application layer** of the **OSI model** and is essential for retrieving web pages, sending forms, and fetching resources like images or documents.

An HTTP client requests by establishing a TCP connection to a specific port on the remote host (usually 80 or 8080).

1. The Hypertext Transfer Protocol (HTTP) is a protocol used for transmitting and receiving web based information over the internet.

2. HTTP operates at the application layer of the OSI model and is the foundation of data communication for the World Wide Web.

3. HTTP follows a client-server model, where a client (typically a web browser) sends requests to a server, and the server responds with the requested data or performs the requested action.

4. HTTP uses a request-response paradigm, where the client sends an HTTP request message to the server, specifying the desired action (such as retrieving a webpage or submitting a form).

5. The server processes the request and sends back an HTTP response message containing the requested data, along with a status code indicating the success or failure of the request.

6. HTTP relies on Uniform Resource Identifiers (URIs) or more commonly known as URLs (Uniform Resource Locators) to identify and locate resources on the web.

7. HTTP supports various methods or verbs, such as GET, POST, PUT, DELETE, which define the type of action to be performed on the server.

8. HTTP is a stateless protocol, meaning that each request from the client is independent and does not maintain any memory of previous requests.

9. To enable stateful interactions, HTTP introduced cookies, which are small pieces of data stored on the client-side and sent with each subsequent request to maintain session information.

10. HTTP can be secured using the Hypertext Transfer Protocol Secure (HTTPS), which adds an additional layer of encryption through the use of SSL/TLS protocols, ensuring secure transmission of data.

11. HTTP supports various content types, including text, images, audio, video, and more, allowing for the transfer of a wide range of data formats.

12. HTTP headers provide additional information about the request or response, such as content type, caching directives, and authentication credentials.

13. HTTP supports caching, allowing clients to store and reuse previously fetched resources, reducing the need for repeated requests to the server.

14. HTTP supports redirection, allowing servers to redirect clients to a different URL or resource based on certain conditions or rules.

15. The continuous development and standardization of HTTP have led to various versions, with HTTP/1.1 and HTTP/2 being the most widely used versions, each introducing improvements in performance, security, and efficiency.

POP3 (Post Office Protocol)

POP3 (Post Office Protocol 3) is a standard protocol for receiving email.

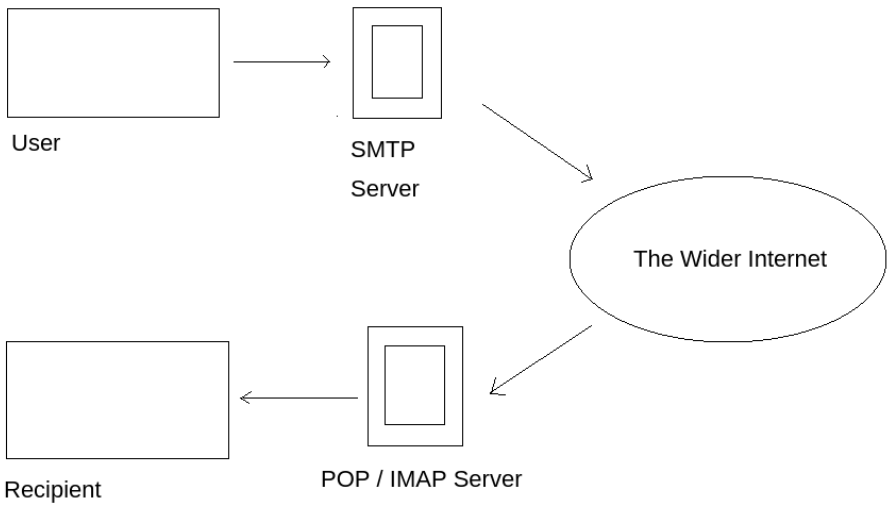
Periodically, you can receive an email and check your mailbox on the server and download any mail, probably via **POP3**.

This standard protocol is built into most popular email products such as **Eudora** and **140 Outlook Express**. Also, it incorporated into the **Netscape** and **Microsoft Internet Explorer** browsers.

IMAP (The Internet Message Access Protocol)

IMAP works in application layer protocol. That it is used to access e-mails on remote servers**. POP3 and IMAP** protocols are the two most common e-mails used.

IMAP allows users to access their messages immediately on their systems.



SMTP (Simple Mail Transfer Protocol)

The Simple Mail Transfer Protocol is a protocol for sending email messages between servers. Most email systems and email clients use SMTP to send messages from one server to another.

connection is easily verified by the Telnet utility. Default SMTP uses TCP **port 25**

FTP (File Transfer Protocol)

FTP or file transfer protocol is used to transfer data (upload/download) from one computer to another over the Internet or computer network. FTP is a communication protocol commonly used for transferring files over the Internet.

1. FTP (File Transfer Protocol) is a widely used network protocol that allows for the transfer of files between computers on a network.

2. It operates on **the client-server model**, where the client initiates the connection to the server and requests file transfers.

3. FTP uses two separate channels for communication: the control channel, which handles commands and responses between the client and server, and the data channel, which is responsible for transferring the actual files.

4. It supports various **authentication** methods, including username and password, as well as anonymous access for public file repositories.

5. FTP supports both ASCII and binary data transfer modes, enabling the transfer of text-based files as well as binary files like images or executables.

6. It provides features such as **directory listing**, **file renaming**, and **file deletion**, **allowing users to manage files on the server remotely**.

7. While FTP is widely supported, it has some security vulnerabilities, **such as transmitting data in plain text,** making it recommended to use secure alternatives like **FTPS** (FTP over SSL) or **SFTP** (SSH File Transfer Protocol) for encrypted file transfers.

IP (Internet Protocol)

An Internet protocol (IP) is a unique identifier or address of each computer or communications network device and the Internet.

Each network device participating computer as a router, computers, printers, fax machines, and Internet switch can have its unique IP address. Each Internet domain must have a unique IP address or a shared IP address.

DHCP (Dynamic Host Configuration Protocol)

DHCP or Dynamic Host Configuration Protocol is a set of rules used by a communication device such as a router adapter, or computer network, allowing the device to request and obtain an IP address of a server that has one list so many directions.

DHCP is a protocol for network equipment to obtain IP addresses and other settings such as a gateway, DNS, and subnet mask of the DHCP server.

DHCP ensures that all IP addresses are unique

DHCP works in four phases, known as DORA:

1. Discover
2. Observe
3. Request
4. Authorize

ARCNET

ARCNET is a technology of local area network with a token bus system to manage the trunk line between workstations. If a device in a network, wants to send a message, a token, which is set to 1 is inserted. A target device reads the message and the token is set to O so that the frame can be used by another device.

FDDI

Fiber Distributed Data Interface (FDDI) provides a standard for data transmission in a local area network that can extend a range of 200 kilometers.

The FDDI-ring network protocol is used as a base. The FDDI local area network can support a large number of users and can cover a wide geographic area. An FDDI network contains two token rings and

the main ring has a capacity of 100 Mbit Is. FDDI is an ANSI standard network and can support 500 stations at 2 Kilometers.

X.25

X.25 is a set of standard protocols for wide area networks using a telephone line or ISDN system. The X.25 standard was approved by CC/TT now ITU in 1976.

TFTP

TFTP is an Internet software utility for transferring files. It's easier than File Transfer Protocol (FTP), but has less capability.

It is used when required for user authentication and directory visibility. TFTP uses the User Datagram Protocol (UDP) and Transmission Control Protocol (TCP).

TFTP Message Types

RRQ ----------:>Request To Read a File

WRQ ---------- :>Request To Write a File

DATA ----------:>COntains a block of file data

ACK ----------:>Used by peer to acknowledge each block of DATA
ERROR ----------:>Used by peer to indicate erroneous operations

SNMP

Simple Network Management Protocol (SNMP) is the TCP I IP set. SNMP is used to manage the network of 156 complex network-connected devices.

PPTP

The point-to-point tunneling protocol is used in virtual private networks. PPP works by ordinary session PPP. PPTP is a method for implementing VPNs.

ATM

ATM is a network protocol that handles data at a speed of 155 Mbps. ATM works by transmitting all data into small packets of a fixed size; while other protocols transfer variable length packets. ATM is compatible with a variety of media such as video, CD, and image. ATM can be used a **star** topology, operating **with fiber optic and twisted pair.**

ATM can be used to connect two or more local area networks. It is also commonly used by Internet service providers to take advantage of free high-speed Internet access.

Frame Specifications

The two main categories of frame types **are Ethernet** and **Token Ring**. There are four different types of Ethernet frames. The most popular form of Ethernet is the only way that the equipment is a common transmission channel, described in the IEEE 802.3 standards.

TCP/IP

Transmission Control Protocol / Internet Protocol (TCP/IP) is the communication protocol tor the Internet.

It can be used for communication on a private network such as the Internet or extranet. It performs various functions such as:

- Multiplexing

- Error recovery

- Flow control

- Connection establishment

- Termination and segmentation.

TCP/IP is a suite of communication protocols used to send data across networks, including the internet. It consists of two main layers:

1. **Transmission Control Protocol (TCP)**: Manages the assembling of data into smaller packets, which are transmitted over the network. Upon reaching the destination, the TCP layer reassembles these packets into the original message.
2. **Internet Protocol (IP)**: Handles addressing and routing of packets, ensuring they reach the correct destination. Routers use the IP address to forward the packets, and the data might travel through different routes.

TCP/IP operates using a **client-server** model, where a client (user) requests data or services, and a server provides them. It is considered "stateless," meaning each client request is independent.

Applications that use TCP/IP include **HTTP** (for web browsing), **FTP** (file transfer), **SMTP** (email), and **Telnet** (remote login). These protocols, along with others, form a "suite" that enables communication over the internet.

Layers of TCP/IP:

- **Application Layer**: Handles end-user communication (e.g., HTTP, FTP).
- **Transport Layer**: Manages data transfer between devices, ensuring reliability (e.g., TCP, UDP).
- **Internet Layer**: Handles packet routing and addressing (e.g., IP).
- **Network Access Layer**: Manages physical network connections (e.g., Ethernet, Wi-Fi).

TCP/IP is foundational for the internet, allowing diverse devices to communicate effectively across networks. It is often compared to the

OSI model, which has seven layers. TCP/IP's four layers are more practical for real-world applications, while OSI is a conceptual framework.

Comparison between OSI and TCP/IP Models:

- **OSI** has 7 layers, while **TCP/IP** has 4 layers.
- OSI guarantees packet delivery at the transport layer; TCP/IP does not.
- OSI is more flexible and general, whereas TCP/IP is specific to protocols.

The **network access layer** in TCP/IP uses methods like **CSMA/CD** (Carrier Sense Multiple Access with Collision Detection) in Ethernet networks, where devices check if the medium is free before sending data. If data collisions occur, the system waits and retransmits the data after a brief delay.