Introduction to Network and Security

1-1 Definitions

Network explained as an arrangement of intersecting horizontal and vertical lines.

"A spider constructs a complex network of several different kinds of threads"

Data network is a digital telecommunications network which allows nodes to share resources. On the other hand, a computer network is a set of connected computers. Computers on a network are called nodes.

The connection between computers can be done via cabling, most commonly the Ethernet cable, or wirelessly through radio waves. connected computers can share resources, like access to the Internet; printers; file servers and others.

The model for understanding the network working is OSI model

1-2 Open Systems Interconnection (OSI) Model مهم جدا

The Open Systems Interconnection (OSI) model defines a networking framework to implement protocols in layers, with control passing data from one layer to the next. It is primarily used today as a teaching tool. It conceptually divides network architecture into 7 layers in a logical progression. The lower layers deal with electrical signals, chunks of binary data, and routing of these data across networks. Higher levels cover

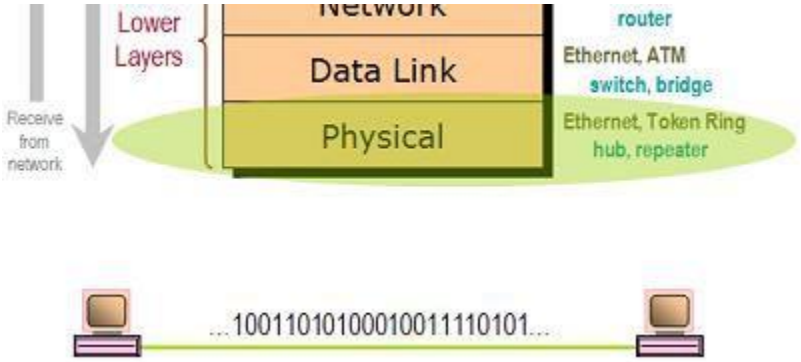
network requests and responses, representation of data, and network protocols as seen from a user's point of view.

The OSI model was originally created as a standard architecture for building network systems, many popular network technologies today reflect the layered design of OSI.

Layer 1 Physical Layer

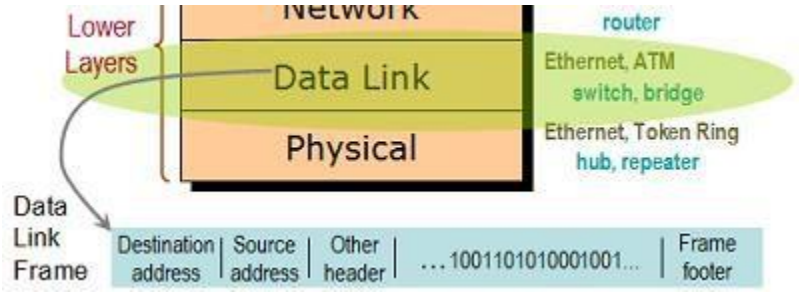
At Layer 1, the Physical layer of the OSI model is responsible for transmission of digital data bits from the Physical layer of the sender device (source) over network communications media to the Physical layer of the receiver device (destination).

Examples of Layer 1 technologies include Ethernet cables; token ring networks. Additionally, hubs and other repeaters are standard network devices that function as cable connectors at the Physical layer.



Data Link Layer مهمة

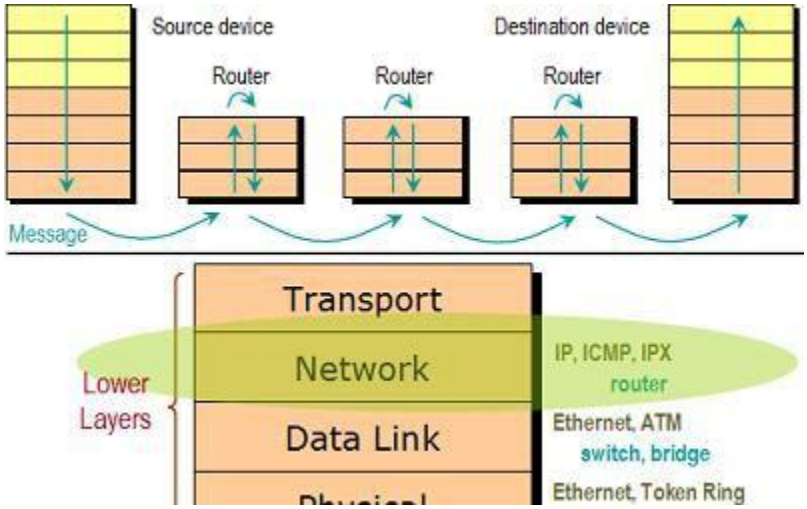
When obtaining data from the Physical layer, **the Data Link layer checks for physical transmission errors and packages bits into data "frames".** The Data Link layer also manages physical addressing schemes such as MAC addresses for Ethernet networks, controlling access of any various network devices to the physical medium. Because the Data Link layer is the most complex layer in the OSI model, it is often divided into two parts, the "Media Access Control" sub layer and the "Logical Link Control" sub layer.



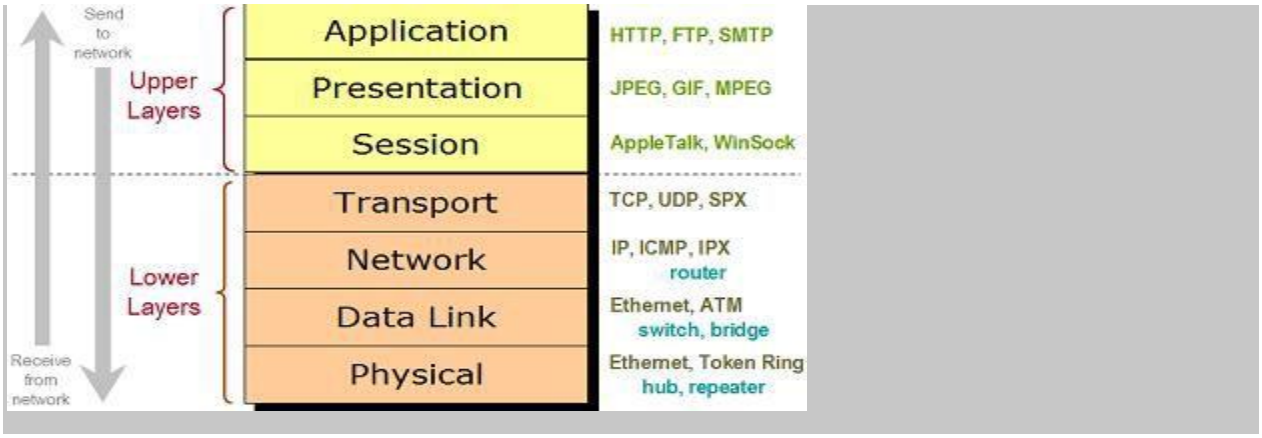
Network Layer

The Network layer adds the concept of routing above the Data Link layer. **When data arrives at the Network layer, the source and destination addresses contained inside each frame are examined to determine if the data has reached its final destination. If the data has reached the final** destination**, this Layer 3 formats the data into packets delivered up to the Transport layer. Otherwise, the Network layer updates the destination address and pushes the frame back down to the lower layers**.

To support routing, the Network layer maintains logical addresses such as IP addresses for devices on the network. **The Network layer also manages the mapping between these logical addresses and physical addresses**. In IP networking, this mapping is accomplished through the Address Resolution Protocol (ARP).



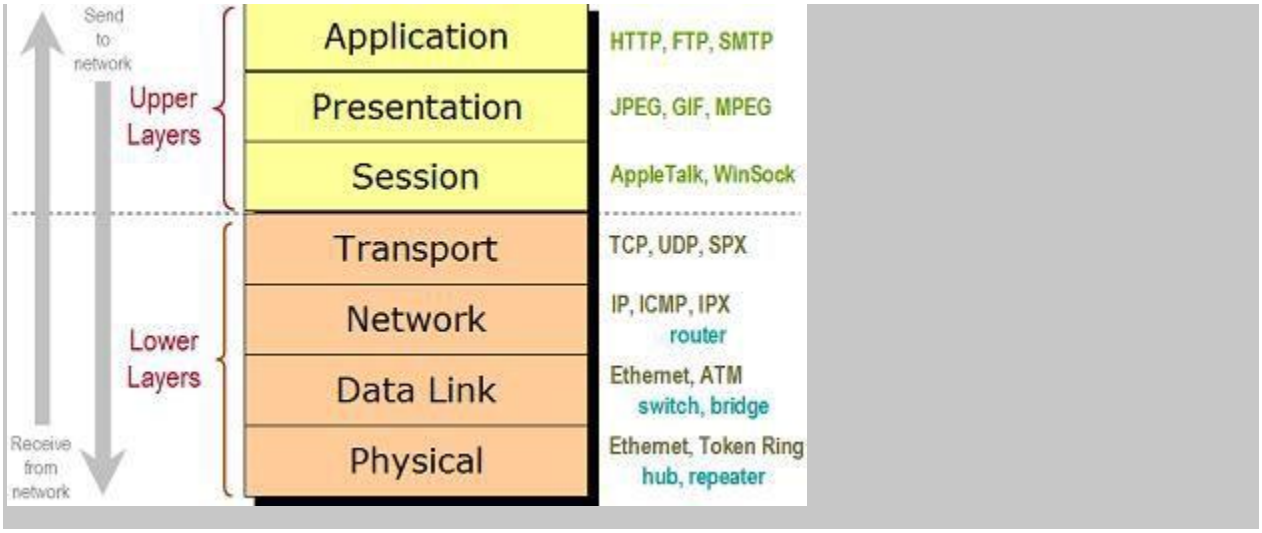
Transport Layer



The Transport Layer delivers data across network connections. **TCP is the most common example of a Transport Layer**

4 network protocol. Different transport protocols may support a range of optional capabilities including error recovery, flow control, and support for re-transmission.

Session Layer



The Session Layer manages the sequence and flow of events that initiate and tear down network connections حدوث انقطاع في الشبكة. At Layer 5, it is built to support multiple types of connections that can be created dynamically and run over individual networks.

Presentation Layer

The presentation layer has three primary functions:

- Coding and conversion of application layer data to ensure that data from the source device can be interpreted by the appropriate application on the destination device

- Compression of the data in a manner that can be decompressed by the destination device
- Encryption of the data for transmission and decryption of data upon

receipt by the destination.

Application Layer

The Application layer supplies network services to end-user applications. Network services are typically protocols that work with user's data. For example, in a Web browser application, the Application layer protocol HTTP packages the data needed to send and receive Web page content. This Layer 7 provides data to (and obtains data from) the Presentation layer.

1-3 Computer Security

The NIST (National Institute of Standard and Technology) *Computer Security Handbook* [NIST95] defines the term *computer security* as "The protection afforded الممنوحة to an automated information system in order to attain لتحقيق the applicable objectives of preserving the integrity, availability, and confidentiality of information system resources (includes hardware, software, firmware, information/data, and telecommunications).

This definition introduces three key objectives that are at the heart of computer security:

1- **Confidentiality:** This term covers two related concepts:

A- **Data confidentiality:** Assures that private or confidential information is not made available or disclosed to unauthorized individuals.

B- **Privacy:** Assures that individuals control what information related to them, it may be collected and stored by others which may be disclosed.

The main characteristics for Confidentiality is:

Preserving authorized restrictions on information access and disclosure, including protecting personal privacy and proprietary information المعلومات التي تملكها .

A loss of confidentiality is the unauthorized disclosure of information.

2- **Integrity:** This term covers two related concepts:

A- **Data integrity:** Assures that information and programs are changed only in authorized manner.

B- **System integrity:** Assures that a system performs its intended function in unimpaired manner بدون أي حالة من الضعف, free from deliberate or inadvertent unauthorized manipulation.

The characteristics of Integrity: Guarding against improper information modification or destruction, including ensuring information nonrepudiation and authenticity.

A loss of integrity is the unauthorized modification or destruction of information.

3- **Availability:** Assures that systems are working properly and service is not denied to authorized users.

The Characteristics of Availability: Ensuring timely في الوقت المناسبand reliable access to and use of information.

A loss of availability is the disruption of access to or use of information system.

Although the use of the CIA tried to define security objectives, some specialists in the security field feel that additional concepts are needed to present a complete picture. Two of the most commonly mentioned are as follows:

• **Authenticity:** The property of being genuine and being able to be verified and trusted; confidence in the validity of a transmission a message or message originator, **this means verifying that users are who they say they are** and each input arriving at the system came from a trusted source.

• **Accountability:** The security goal (aim) is to generate the requirements for actions of an entity to be traced uniquely. Simply it means that the system must be able to find who/whom are responsible for such security incident/ accident. **This supports nonrepudiation, deterrence** ردع ،درء, **intrusion detection and prevention, and after that an action of recovery and legal action must be taken.**

Because truly secure systems are not yet an achievable goal, we must be able to trace a security breach to a responsible party. **Systems must keep**

records of their activities to permit later forensic analysis to trace security breaches or to aid in *transaction disputes* نزاع التعاملات.

1-4 the Challenges of Computer Security

Computer and network security both are complex. Some of the reasons follow:

1. Security is not as simple as it might first appear to the novice المبتدئ . The requirements seem to be straightforward; indeed, most of the major requirements for security services can be given self-explanatory, one-word labels: confidentiality, authentication, nonrepudiation, or integrity. **But the mechanisms used to meet those requirements can be quite complex.**

2. **In developing a particular security mechanism or algorithm, one must always consider potential attacks on those security features.** In many cases, successful attacks are designed by looking at the problem in a completely different way, therefore exploiting an unexpected weakness in the mechanism happening most times.

3. **Because of point 2, the procedures used for providing particular services are often counterintuitive حدسية.** Typically, a security mechanism is a complex and not obvious from the statement of a particular requirement that such elaborate measures are needed وجود مقياس واضح.

4. **Having designed various security mechanisms, it is necessary to decide where to use them, the major two positions are:**

A- physical placement (e.g. at what points in a network are certain security mechanisms needed).

C- logical sense (e.g., at what layer or layers of an architecture such as TCP/IP [Transmission Control Protocol/Internet Protocol] should mechanisms be placed).

5. **Security mechanisms typically involve more than a particular algorithm or protocol.** They also require that participants be in possession of some secret information (e.g., an encryption key), which raises questions about the creation, distribution, and protection of that secret information. There also may be a reliance on communications protocols whose behavior may complicate the task of developing the security mechanism. For example, if the proper functioning of the security mechanism requires setting time limits on the transit time of a message from sender to receiver, then any protocol or network that introduces variable, unpredictable delays may render تجعل such time limits meaningless.

6. **Computer and network security is essentially a battle of wits (مواهب او دهاء) between a perpetrator who tries to find holes and the designer and administrator who tries to close them.** The great advantage that the attacker has is that he or she need only find a single weakness, while the designer must find and eliminate all weaknesses to achieve perfect security.

7. **There is a natural tendency ميل طبيعي on the part of users and system managers to perceive لاحظ او يدرك little benefit from security investment until a security failure occurs.**

8. **Security requires regular or continues monitoring,** but this is difficult in today's short-term, overloaded environment.

9. Security is still too often an afterthought ابعد ما تكون عن to be incorporated into a system, after the design it is complete rather than being an integral part of the design process.

10. Many users and security administrators see strong security as an impediment عائق to efficient and user-friendly operation of an information system or use of information.

1-5 The OSI Security Architecture (Ref#1 p 12)

ITU (International Telecommunication United) -T3 Recommendation X.800, (*Security Architecture for OSI*), defines the OSI security architecture, it is useful to managers as a way of organizing the task of providing security.

Furthermore, because this architecture was developed as an international standard, computer and communications vendors have developed security features for their products and services that relate to this structured definition of services and mechanisms.

The OSI security architecture focuses on security attacks, mechanisms, and services. These can be defined briefly as

• **Security attack**: Any action that compromises the security of information owned by an organization.

• **Security mechanism**: A process (or a device incorporating such a process) that is designed to detect, prevent, or recover from a security attack.

• Security service: A processing or communication service that enhances the security of the data processing systems and the information transfers belong to organization. The services are intended to counter تواجه او تضع في

الحسبان security attacks, and they make use of one or more security mechanisms to provide the service.

Other security glossary provides definitions taken from RFC 4949,

Threat: A potential for violation of security, which exists when there is a circumstance, capability, action, or event that could breach security and cause harm. In other word, a threat is a possible danger that might exploits a vulnerability in security system.

Attack: An assaults الاعتداءات on security system that derives from an intelligent threat; “an intelligent act” is a deliberate attempt (especially in the sense of a method or technique) to evade تتجنب security services and violate the security policy of a system.

Q1 What is the difference between Privacy and Confidentiality?

Q2 what is the goal for accountability?

Q3, who has the great chance to beat the other, why?