

HCIA Security

Prepared by Dr. Abdelrhman Ahmed

Lecture 2

جامعة الجميع الذكية

تسعى لتكون الكيان الأول الذي يتبنى مبدأ المجتمع التعليمي
التعاوني ويقدم العلم مقابل العمل لتنمية وبناء المجتمعات.

Basic Network Concepts

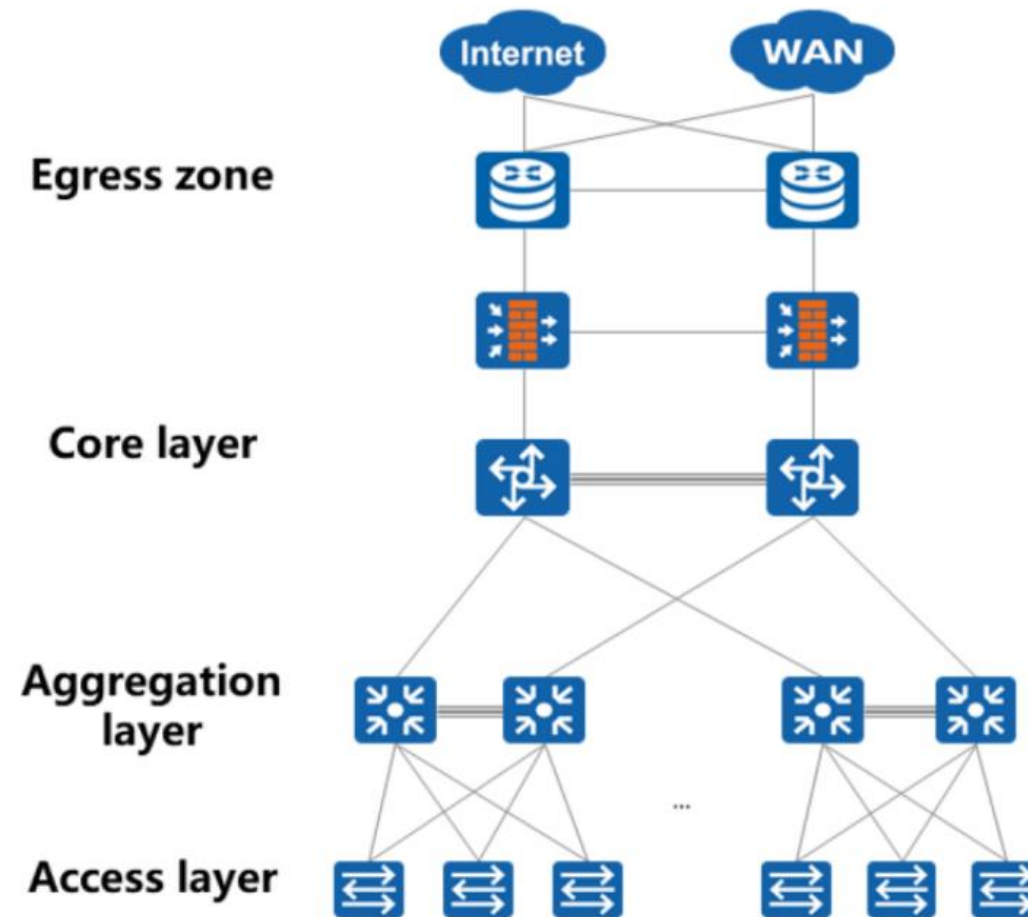


جامعة الجميع الذكية
EVERYONE'S SMART UNIVERSITY

- To understand security technologies, you first need to learn about basic network concepts, such as basic communication principles, network components, and common network protocols. With knowledge of these basic concepts, you can better understand network security threats and deploy security defense policies.

- Upon completion of this course, you will be able to:
 - Describe the working principles of TCP/IP protocols.
 - Describe the working principles of common protocols.
 - Describe possible security threats to common protocols.

Architecture of a Typical Campus Network



Architecture of a Typical Campus Network

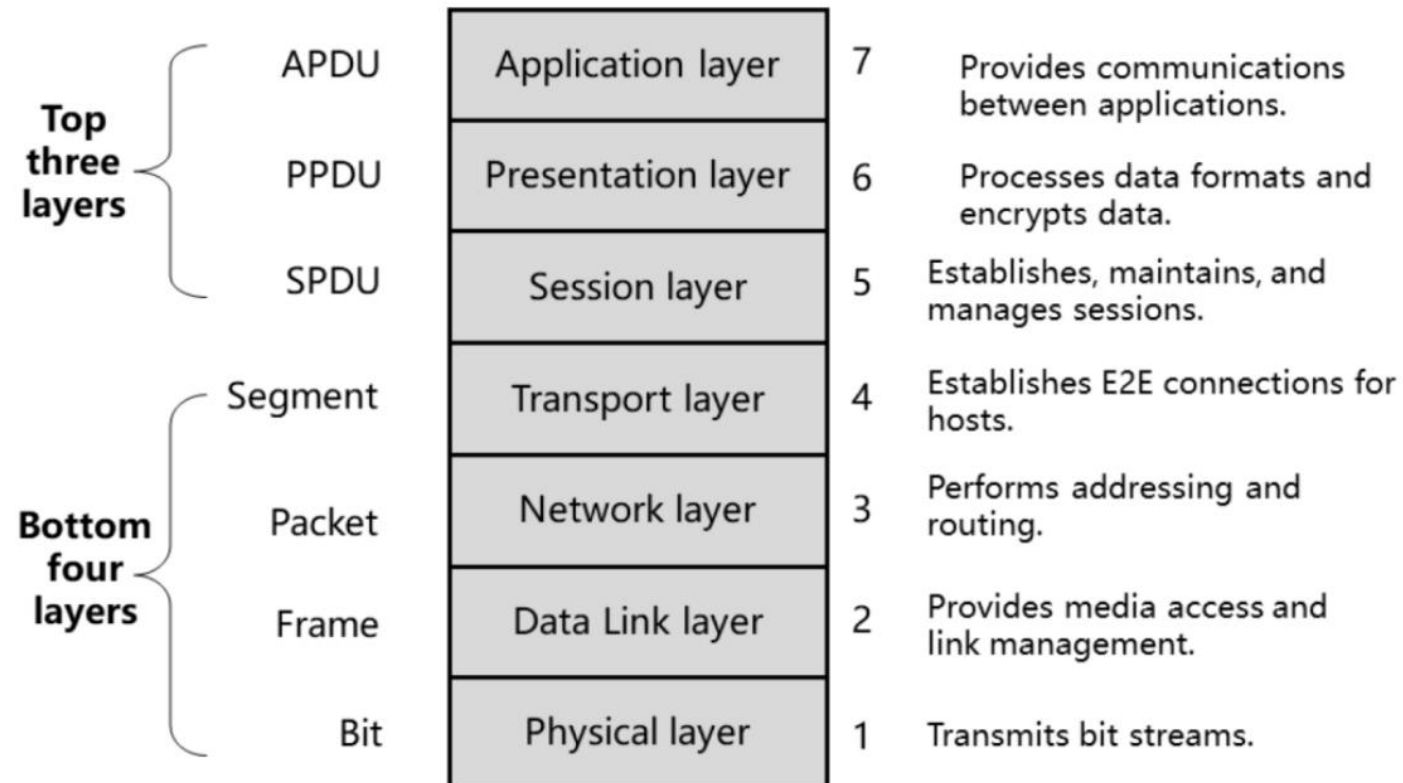
- In medium to large networks, a modular design is usually used to split network functions. Within each module, consideration must be given to the flexibility and scalability of the network structure. Generally, a hierarchical architecture is used, for example, in a campus network that needs to provide access services for a large number of users.
- Traditional networks contain the core, aggregation, and access layers. The core layer provides high-speed data channels, the aggregation layer converges traffic and control policies, and the access layer offers various access modes to devices.

- Objectives
- Design principles
- Advantages

- **OSI model: Open System Interconnect Reference Model**
 - The OSI model is designed to overcome the interconnection difficulties and low efficiency issues associated with using various protocols by defining an open and interconnected network..
- The OSI reference model forms the basis for computer network communications. Its design complies with the following principles:
 - There are clear boundaries between layers to facilitate understanding.
 - Each layer implements specific functions and does not affect each other.
 - Each layer is a service provider and a service user. Specifically, each layer provides services to its upper layer and uses services provided by its lower layer..
 - The division of layers encourages the development of standardized protocols.
 - There are sufficient layers to ensure that functions of each layer do not overlap.

- The OSI reference model has the following advantages:
 - Simplifies network operations.
 - Provides standard interfaces that support plug-and-play and are compatible with different vendors.
 - Enables vendors to design interoperable network devices and accelerate the development of data communications networks.
 - Prevents a change in one area of a network from affecting other areas. Therefore, each area can be updated quickly and independently.
 - Simplifies network issues for easier learning and operations.

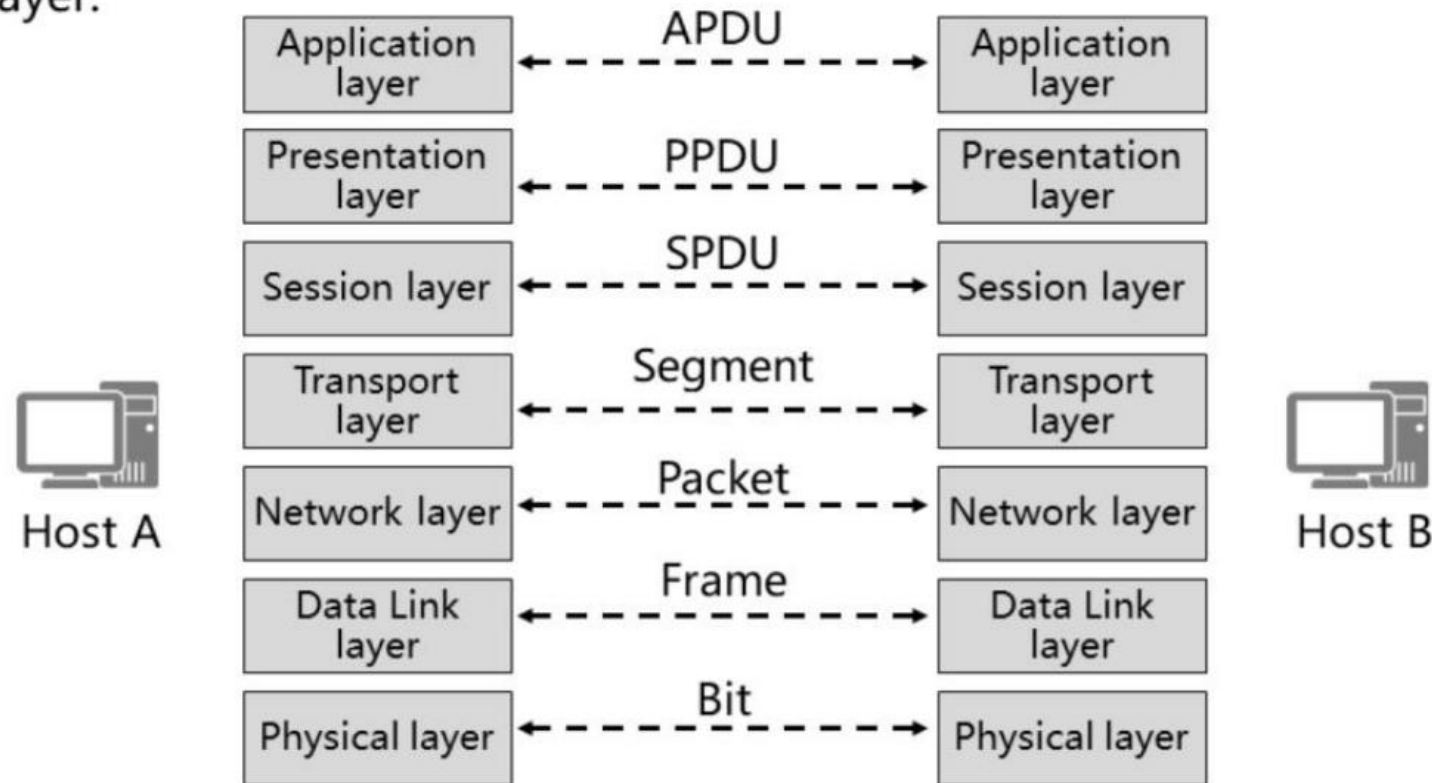
7 Layers of the OSI Model



- In the OSI model, units of data are collectively called Protocol Data Units (PDU). However, each PDU is called a different name according to the layer at which it is sent:
 - Application layer (layer 7): data is called an Application Protocol Data Unit (APDU)
 - Presentation layer (layer 6): data is called a Presentation Protocol Data Unit (PPDU)
 - Session layer (layer 5): data is called a Session Protocol Data Unit (SPDU)
 - Transport layer (layer 4): data is called a segment
 - Network layer (layer 3): data is called a packet
 - Data link layer (layer 2): data is called a frame
 - Physical layer: data is called bit stream.
- Each layer of the OSI model encapsulates data to ensure that the data can reach the destination accurately and can be accepted and executed by the terminal host. A node encapsulates the data to be transmitted by using a specific protocol header for transmission. When data is processed at a layer, packets are also added to the tail of the data , which is also called encapsulation.

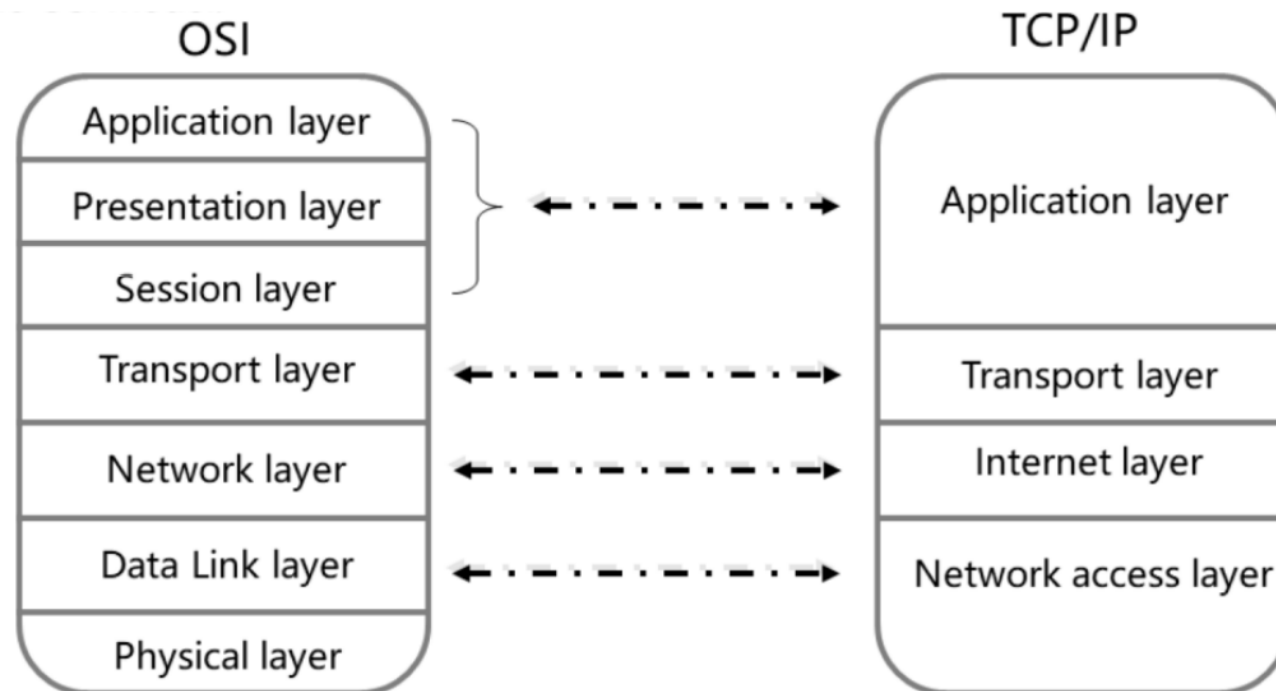
Peer Layer Communications

- Each layer uses the services provided by the lower layer to communicate with the peer layer.



Mapping Between TCP/IP and OSI

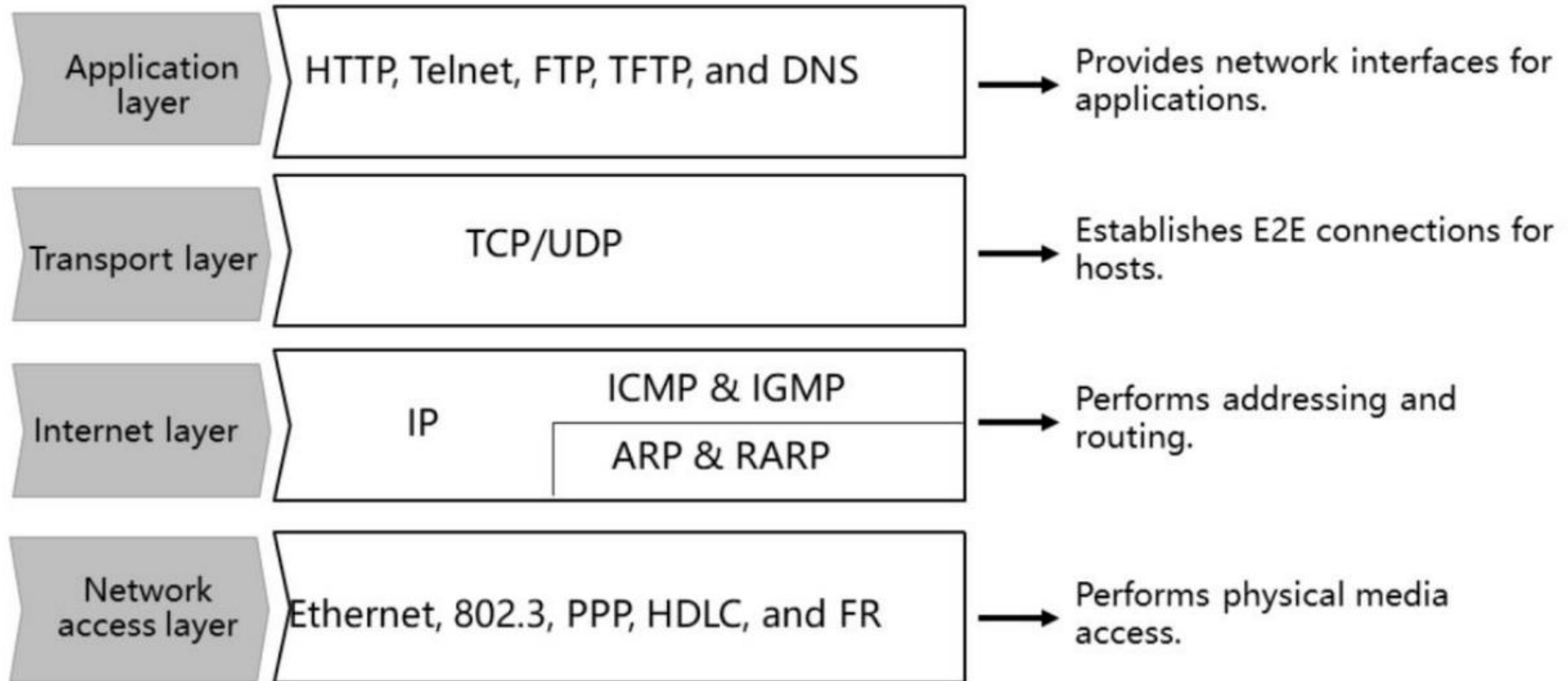
The TCP/IP protocol stack has a simple hierarchical design and a clear mapping relationship with the OSI model.



Mapping Between TCP/IP and OSI

- The Transfer Control Protocol/internet Protocol (TCP/IP) model is widely used due to its openness and usability. The TCP/IP protocol stack is implemented as standard protocols.
- The TCP/IP model is divided into four layers (from bottom to top): link layer, internet layer, transport layer, and application layer. Some documents define a model with five layers, where the link layer is split into a link layer and a physical layer (equivalent to layers 1 and 2 in the OSI model).

Functions of Each Layer of the TCP/IP



Functions of Each Layer of the TCP/IP

Each layer of the TCP/IP protocol stack has corresponding protocols, which are achieved to generate network applications. Some protocols cannot be defined in a hierarchical manner. For example, ICMP, IGMP, ARP, and RARP are deployed at the same layer as the IP protocol at the Network layer. However, in some scenarios, ICMP and IGMP may be placed on the upper layer of the IP protocol, and ARP and RARP are placed at the lower layer of the IP protocol.

- **Application layer**

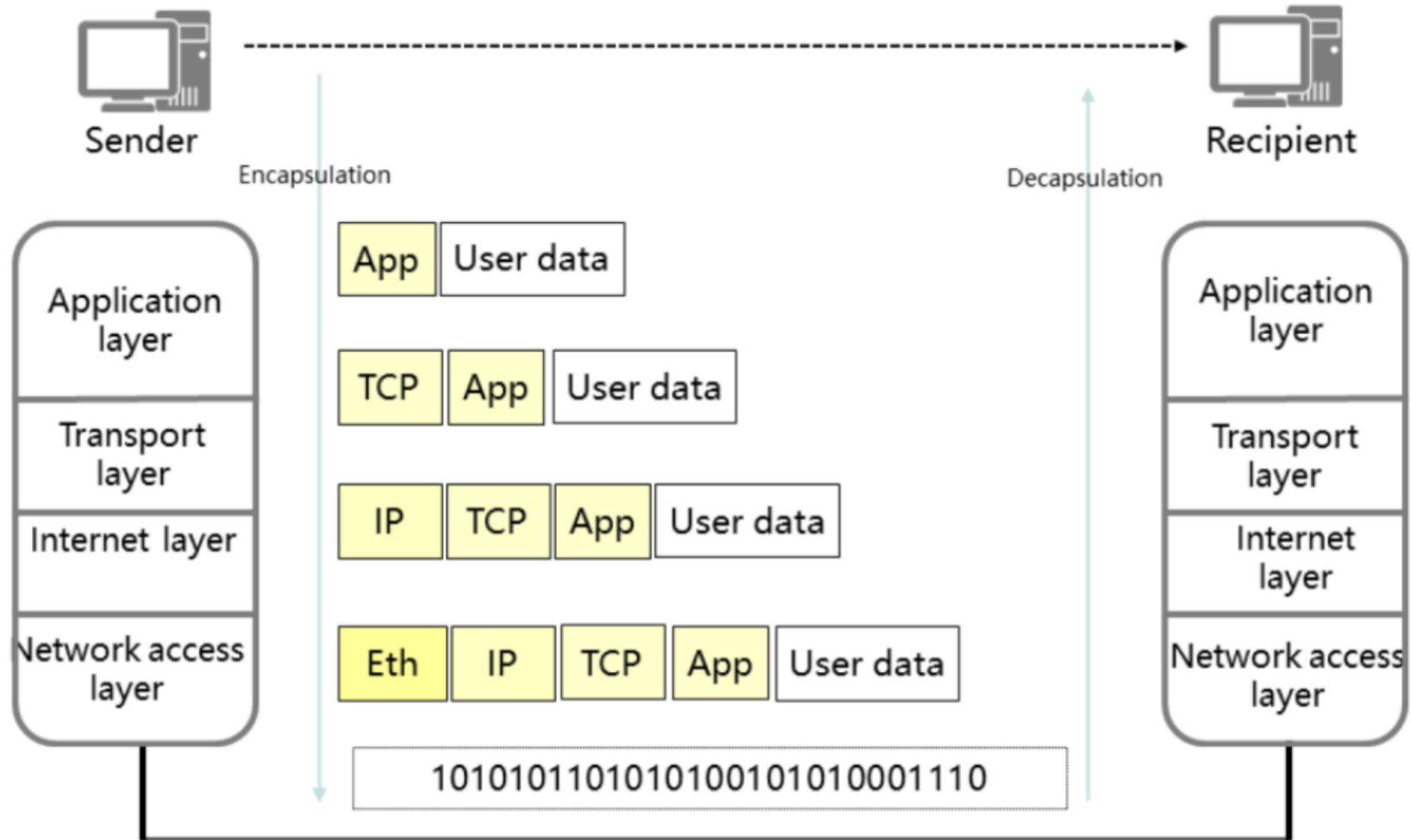
- ☐ **Hypertext Transfer Protocol (HTTP):** It is used to access various pages on the web server.
- ☐ **File Transfer Protocol (FTP):** It is used to transfer data from one host to another.
- ☐ **Domain Name System (DNS):** It is used to convert the domain name of the host to an IP address.

Transport layer

- ☐ **TCP:** Provides reliable connection-oriented communications services for applications and applies to applications that require responses.
- ☐ **User Datagram Protocol (UDP):** Provides connectionless communications and does not guarantee reliable transmission of data packets. It is suitable for transmitting a small amount of data at a time, and the application layer is responsible for reliability.



Encapsulation and Decapsulation Processes of the TCP/IP



Functions of Each Layer of the TCP/IP

- The sender submits the user data to the application, which then sends the data to the destination. The data encapsulation process is as follows:
 - The user data is first transmitted to the application layer, and the application layer information is added.
 - After the application layer processing is complete, the data is transmitted to the transport layer. The transport layer information, such as TCP or UDP (the application layer protocol specifies whether to use TCP or UDP) is then added.
 - After the processing at the transport layer is complete, the data is transmitted to the Internet layer. The Internet layer information (such as IP address) is then added.
- After the data is processed at the Internet layer, the data is transmitted to the network access layer. The network access layer information (such as Ethernet, 802.3, PPP, and HDLC) is added. Then, the data is transmitted to the destination as a bit stream. Processing differs based on different devices

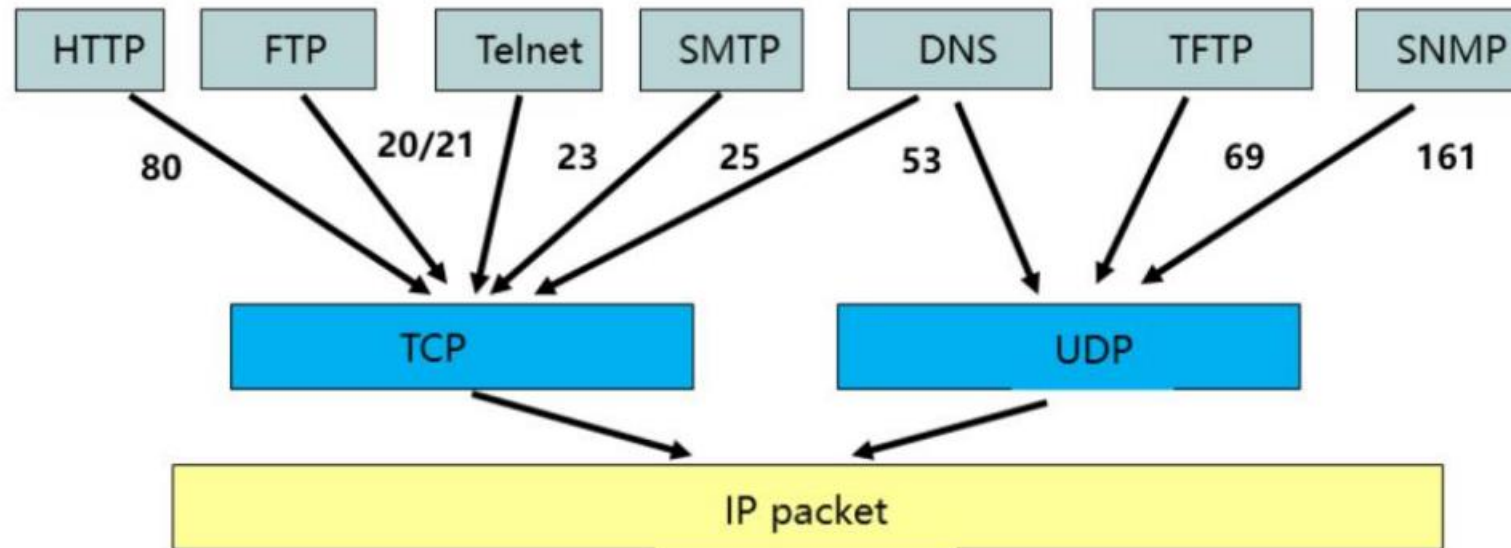


Functions of Each Layer of the TCP/IP

After the user data arrives at the destination, the decapsulation process is performed as follows:

- ❑ Data packets are sent to the network access layer. After the network access layer receives data packets, the data link layer information is removed after packet resolution, and Internet layer information (such as IP address) is obtained.
 - ❑ After the Internet layer receives data packets, the Internet layer information is removed after packet resolution, and upper-layer protocols (such as TCP) is obtained.
 - ❑ After the transport layer receives data packets, the transport layer information is removed after packet resolution, and upper-layer protocols (such as HTTP) is obtained.
 - ❑ After the application layer receives data packets, the application layer information is removed after packet resolution. The data displayed is the same as that received from the host.
- The application layer and transport layer provide end-to-end services. The Internet layer and network access layer provide segment-to-segment services

Quintuple



Quintuple

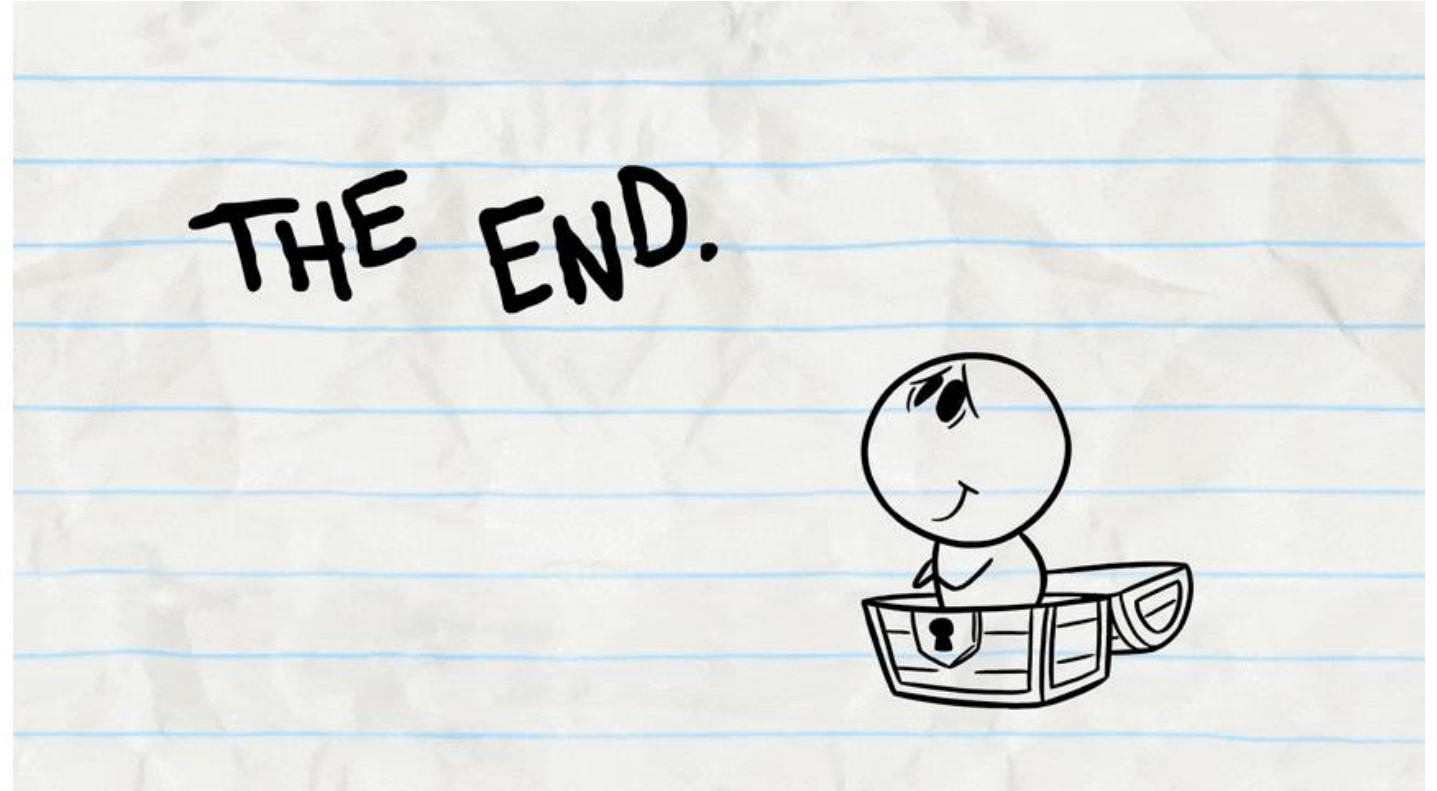
- Source IP address + destination IP address + protocol + source port + destination port

- **Quintuple structure:** Source IP address, destination IP address, protocol in use (for example, 6 indicates TCP, and 17 indicates UDP), source port, and destination port.
- **Destination port:** Generally, well-known application services have standard ports, such as HTTP, FTP, and Telnet. Because some applications are not popular, the applications are usually defined by development vendors to ensure that the service ports registered on the same server are unique.
- **Source port:** Generally, common application services, such as HTTP, FTP, and Telnet, are assigned well-known port numbers (in the range from 0 to 1023). However, some operating systems may use greater port numbers as their initial ports. Because source ports are unpredictable, they are seldom involved in the ACL policy.
- **A quintuple is a concept.** So that an application server can respond to service requests, it must register the port numbers and protocol (TCP or UDP) for the services it hosts. By using the quintuple, the application server can respond to any concurrent service request while ensuring that each link is unique in the system.

The End

Please feel free to contact me anytime if you have any questions

Abdelrhman Ahmed Refaat:
abdelrhmanahmedrefaat@gmail.com



جامعة الجميع الذكية
EVERYONE'S SMART UNIVERSITY