Lecture 12

Communication Fundamentals in Computer Networks

M. Adnan Quaium

Assistant Professor
Department of Electrical and Electronic Engineering
Ahsanullah University of Science and Technology
Room – 4A07
Email – adnan.eee@aust.edu
URL- http://adnan.quaium.com/aust/cse4295

The Internet and the TCP/IP Layer Model

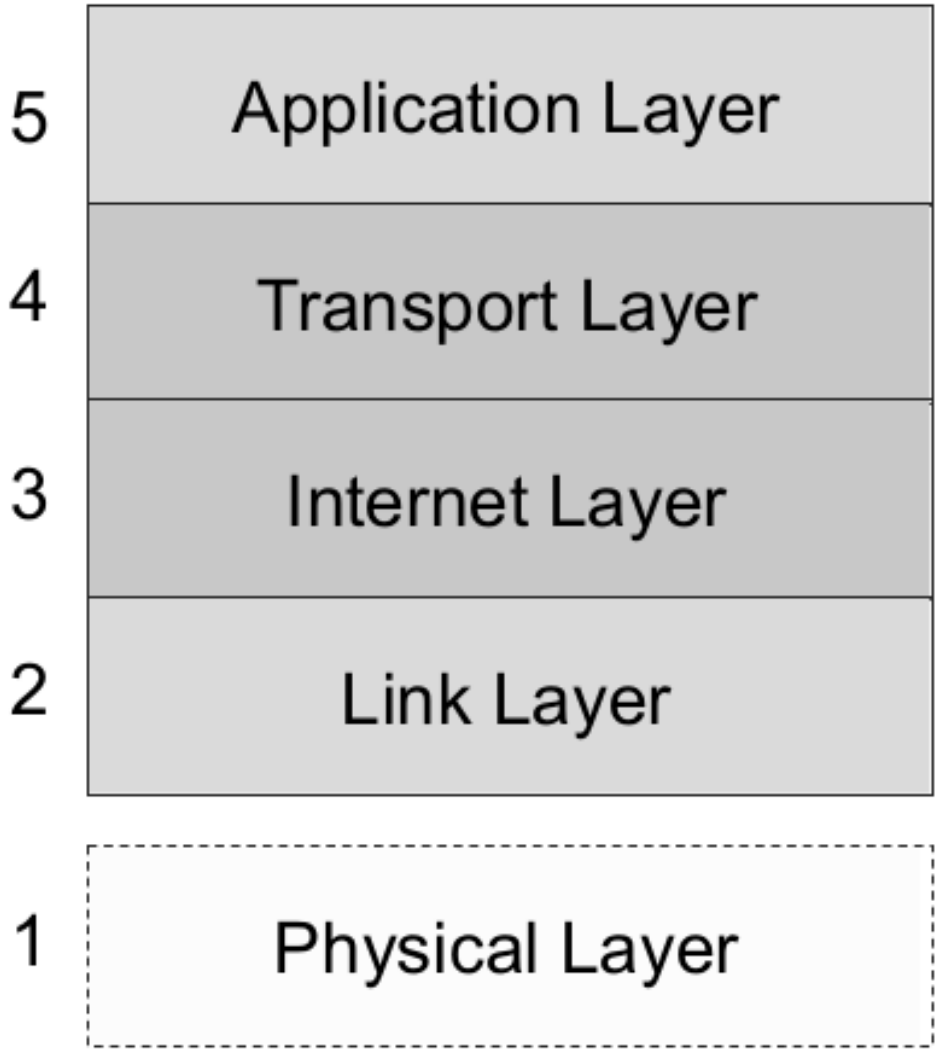


Fig. 3.21 The TCP/IP Reference Model consists of four layers (2-5); together with the network hardware layer (1) the model is referred to as the hybrid TCP/IP reference model.

The Internet and the TCP/IP Layer Model

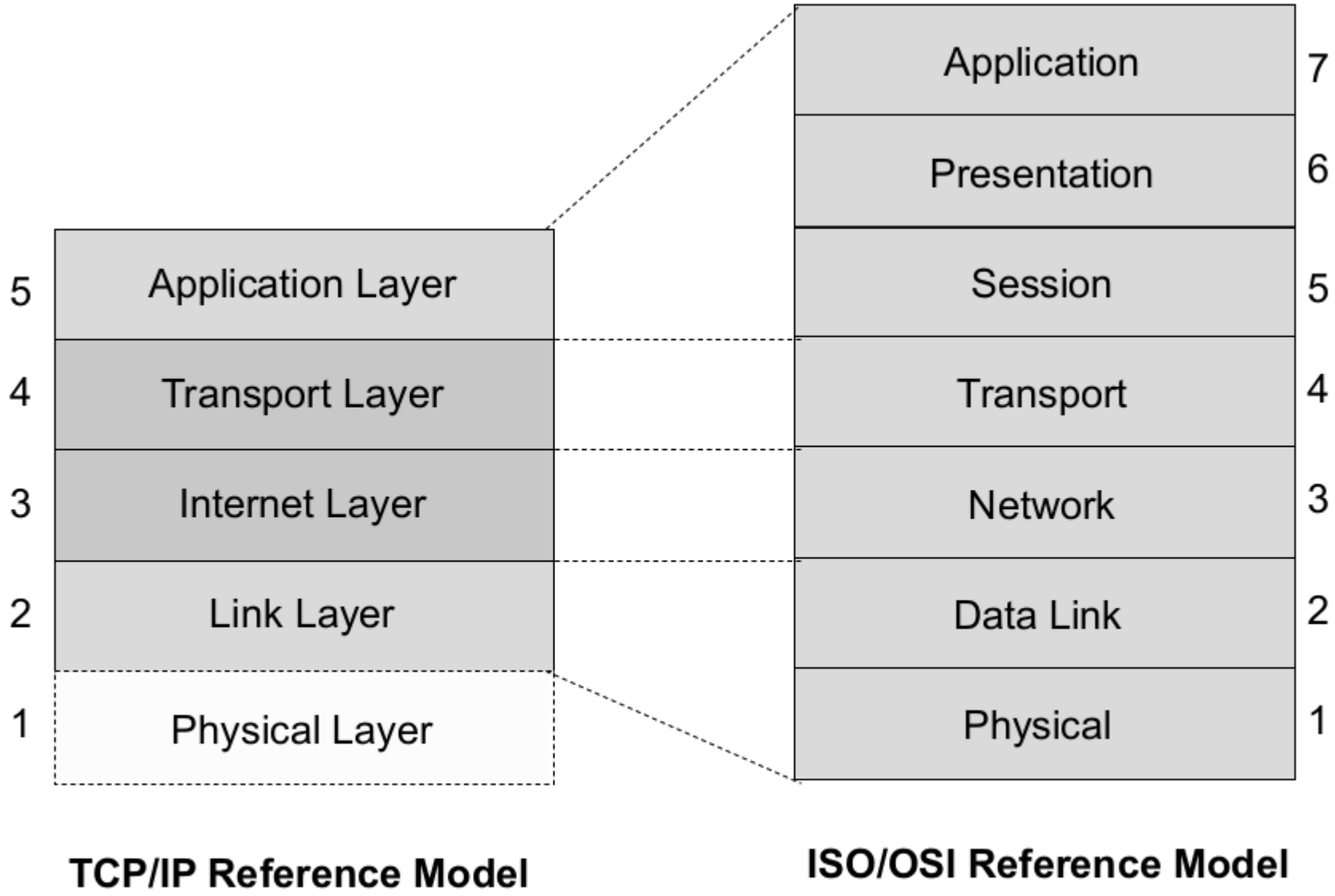
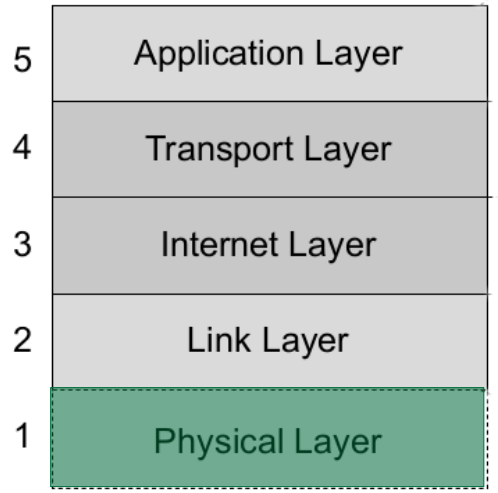


Fig. 3.22 Comparison of the TCP/IP and the ISO/OSI reference models.

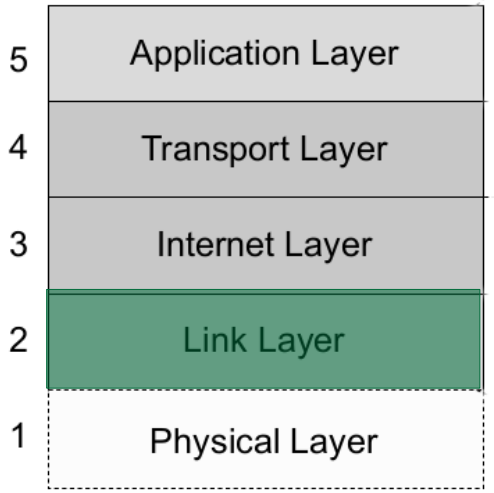
TCP/IP Layer Model



Physical layer is a communication hardware descriptive layer (hardware/physical layer).

TCP/IP Layer Model

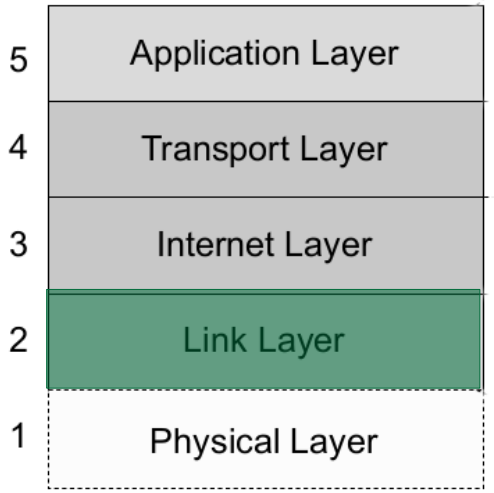
The main task of the link layer involves the secure transmission of individual data packets between two adjacent end systems.



- Bit sequences are grouped together into fixed units (data packets) and provided with the extra information necessary for transmission, e.g., checksums for simple error detection.
- Two types of services :
  - In *unsecured service*, data packets that are recognized as defective are eliminated. The request for retransmission first takes place at a higher layer of the protocol stack.
  - A *secure service*, in contrast, accepts the request for retransmission itself.

TCP/IP Layer Model

In local area networks (LANs), this layer is normally divided into two more sub-layers:



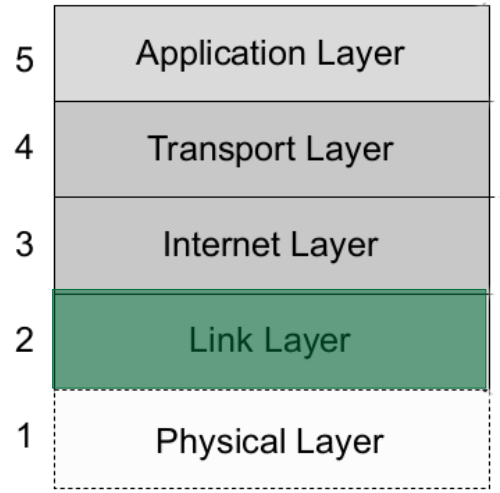
Media Access Control (MAC)

- This sub-layer controls access to the transmission system, which is shared by (many) other computer systems.

Logical Link Control (LLC)

- This sub-layer regulates the followings:
  - Flow control (to avoid overload at the receiver),
  - Error handling (error detection and error correction),
  - Transmission control (link management; orderly and error-free transmission) and
  - Data packet synchronization (assuring that the beginning and the end of a data packet are detectable).

TCP/IP Layer Model

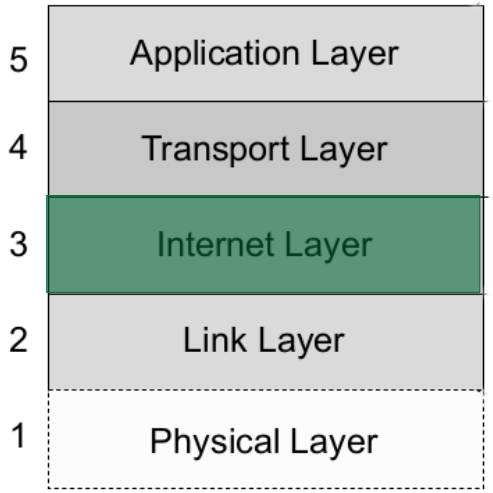


Protocols at layer 2 of the TCP/IP protocol family are:

- Ethernet, Token Ring or FDDI,
- ARP und RARP (Address Resolution Protocol and Reverse Address Resolution Protocol), SLIP (Serial Line Interface Protocol) and
- PPP (Point to Point Protocol).

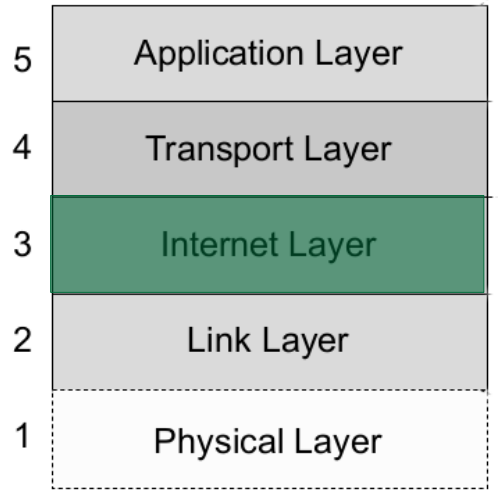
TCP/IP Layer Model

The main task of the internet layer is to enable data communication between two end systems at different ends of the communication network.



- *An addressing scheme* must be used that is valid across the borders of individual physical networks.
- The data packets to be sent must each be provided with the addresses of the sender and the receiver so they can be delivered correctly.
- It is responsible for *fragmentation* and *defragmentation* of the so-called IP datagrams.
- It has protocol mechanisms for *relaying messages across intermediate systems* to the designated receiver.
- IP is an *unreliable protocol* because it does not have mechanisms for dealing with data loss.

TCP/IP Layer Model

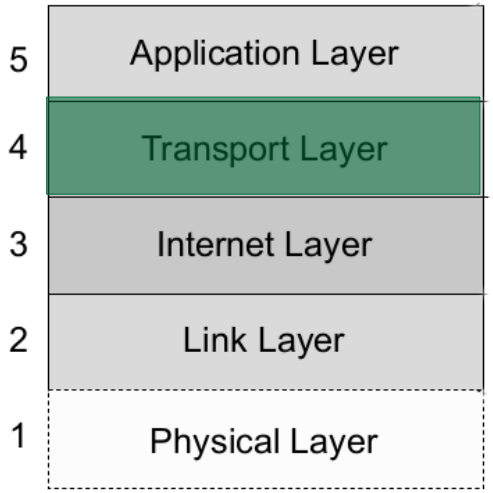


Protocols at layer 3 of the TCP/IP protocol family are:

- ICMP protocol (Internet Control Message Protocol)
- IGMP (Internet Group Management Protocol)
- RSVP (Resource Reservation Protocol)
- ST 2+ (Internet Stream Protocol, Version 2)
- OSPF (Open Shortest Path First)
- BGP (Border Gateway Protocol)

TCP/IP Layer Model

The primary task of transport layer is to establish a communication link between two application programs that are located on different computers in the network.

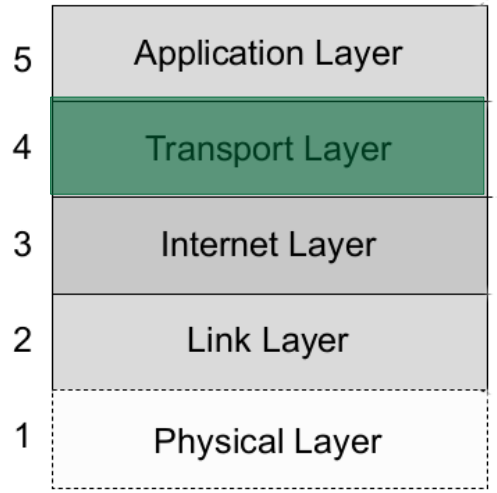


- A *flow control* is carried out on the transport layer. This ensures that overload situations are avoided as much as possible.
- There also exists an *acknowledgement mechanism* by which the receiver can confirm correctly sent data packets or re-request defective ones.
- The transport layer is capable of transporting *packets of any length* (streams).
  - *A long message is divided into segments; these segments are transmitted separately and then reassembled at the receiver.*

TCP/IP Layer Model

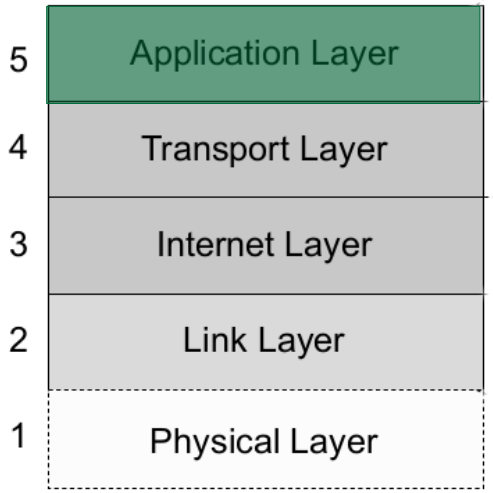
Protocols at layer 4 of the TCP/IP protocol family are:

- TCP (Transport Control Protocol)
- UDP protocol (Universal Datagram Protocol)
- VMTP (Versatile Message Transaction Protocol)
- NETBLT (Network Block Transfer Protocol)
- MTP (Multicast Transport Protocol)
- RDP (Reliable Data Protocol)
- RIP (Routing Information Protocol)
- SSL (Secure Socket Layer)
- TLS (Transport Layer Security)



TCP/IP Layer Model

The Application layer basically serves as the interface for the actual application programs that want to communicate via the network.

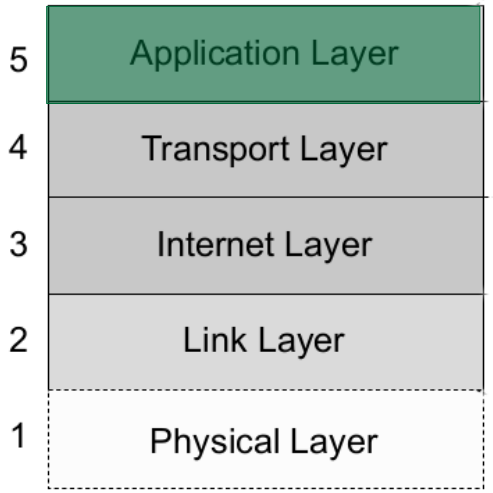


- The services offered at the application layer have a high level of abstraction.
  - *This means that it is possible to shield the user, or communicating application, from the communication details regulated on the lower protocol layers for the most part.*

TCP/IP Layer Model

The application layer of the TCP/IP protocol family includes the following protocols:

- TELNET
- FTP (File Transfer Protocol)
- SMTP (Simple Mail Transfer Protocol)
- HTTP (Hypertext Transport Protocol)
- RPC (Remote Procedure Call)
- DNS (Domain Name Service)
- PGP (Pretty Good Privacy)
- SNMP (Simple Network Management Protocol)
- RTP (Realtime Transport Protocol)



Protocol Functions

Protocols at different layers frequently offer the same functionality. These shared functionalities are called *protocol functions* or *protocol mechanisms*.

Basic protocol functions

- **Data transfer:** It is possible to *define priority data traffic* in data transmission. Priority data can even overtake ordinary data that has been sent. If a data packet is correctly received it is possible to establish a special *acknowledgment procedure* to signal successful data transfer.

- **Connection management:** *The establishment and termination* of a data connection is one of the fundamental tasks of network communication. The protocol mechanism must therefore be capable of handling *late, lost or duplicated data packets*. Consecutive sequence numbers are thus assigned to data packets.

Protocol Functions

Error handling

- **Error detection:** Different checksum procedures or parity bits can be implemented in error detection.
- **Retransmission:** If a data packet is identified as defective, it can be requested again from the sender.
- **Time monitoring:** If the time a data packet needs through the network exceeds a specified, maximum limit, it is considered “lost“ and subsequently retransmitted (timeout).
- **Error correction:** By providing the information to be transmitted with sufficient redundancy, it is possible to ensure an automatic correction of transmission error.

Protocol Functions

Length adjustment

- Due to technical and organizational constraints, the length of data packets is always limited.
- However, the message to be transmitted is often longer than the predetermined data format allows.
  - *When this happens, the message must be broken down before transfer into size-appropriate, separate parts or packets (fragmentation).*
  - *Once having arrived at the receiver, the data packets fragments are then assembled again into the original message (defragmentation).*
- At the same time, it is also possible that messages are shorter than the prescribed data packet length.
  - *In this case, the data packets are then expanded with so-called padding bits (bit stuffing)*

Protocol Functions

Transmission adjustment

- **Multiplexing:** If a connection channel has a significantly higher transmission capacity than the individual connected computing systems, then connections to multiple computing systems can be mapped to one connection with a high transmission capacity.

- **Inverse multiplexing:** If a computing system connected to the network has a higher transmission capacity than the available data connection, via the inverse multiplexing mechanism, the connection to the computing system can be mapped simultaneously as multiple data connections.

Protocol Functions

User-based protocol mechanisms

- **Connection classes:** Network services can deliver their performance in different quality levels – so-called service classes.
- **Rights management:** The use of certain system services or special data connections can be user-related or time-limited.
- **Quality of service management:** When establishing a connection, the initiator of the intended communication can express the wish for certain quality of service parameters, e.g., a specific minimum throughput.