Networks

1. Transmission Media

1.1 Wireless Media

- Microwave

- radio

- light

- satellite

1.2 Wired

- Twisted-pair (copper)

- Coaxial cable

- fibre optics

- powerline

2. Network Topology

These describe the physical or logical connections in a network.

- *Bus*
  Devices share a single communication line (the bus). All information is sent to all the devices and devices ignore data not addressed to them. A major disadvantage is there is a single point of failure for the entire network. Early coaxial ethernet often used a bus topology.

- *Ring*
  Devices are connected in a circular fashion. Data transmits around the circle in one direction until it reaches its destination. *Token Ring* is one implementation.

- *Star*
  Devices are connected to a central hub. Twisted pair ethernet is generally configured in a star topology as each device connects to a central hub.

- *Mesh*
  Each device is connected to every other device (full mesh) or at least a number of devices (partial mesh). Multiple routes provides redundancy. They may be formed dynamically or preconfigured.

- *Ad Hoc*
  An ad hoc network is a decentralized <u>wireless</u> network that is typically formed dynamically as devices come into proximity with each other. There is no need for fixed infrastructure (i.e.: a wireless access point), and connections are established on-the-fly. Each device in the network can act as both a client and a router, relaying data for other devices in the network. These networks may be used where pre-existing network infrastructure may be unreliable: for emergency or military operations, or in underdeveloped areas. It is left to the reader to consider why one of the biggest concerns with an ad hoc network is security.

3. Network Models

This describes the overall design and structure of a computer network, including how the components of the network interact.

- *Client-Server*
  Client-server networks have a dedicated central server that controls the network, and a number of clients that connect to the server. A client-server network can have more than one server, each performing a specific function. Functions may include data storage and access, internet connection management, etc.

- *Peer-to-Peer*
  These networks do not have a central server controlling the network. Instead, all the computers in the network are connected to one another and may share resources such as files, applications, and programs. Each computer can either be a client, and request services, or a server, and provide services. Each computer is called a peer and has the same capabilities and access rights, and no peer has control over another.

4. Network Protocols

A network communication protocol is an established set of rules that determine how data is transmitted between different devices in the same network.

These protocols define the syntax, semantics, authentication, synchronization, and error detection in both analog and digital communications.

Essentially, it allows connected devices to communicate with each other, regardless of any differences in their internal processes, structure, or design. Network protocols are typically created according to industry standards by various networking or information technology organizations. There are thousands of different network protocols, but they all perform one of three primary actions: Communication, Network management, and Security.

Ethernet, Infrared, Wireless, **ZigBee**, Bluetooth, GSM and 3G/4G/5G (cellular)

Voice Over IP (VOIP), **Session Initiation Protocol (SIP)**

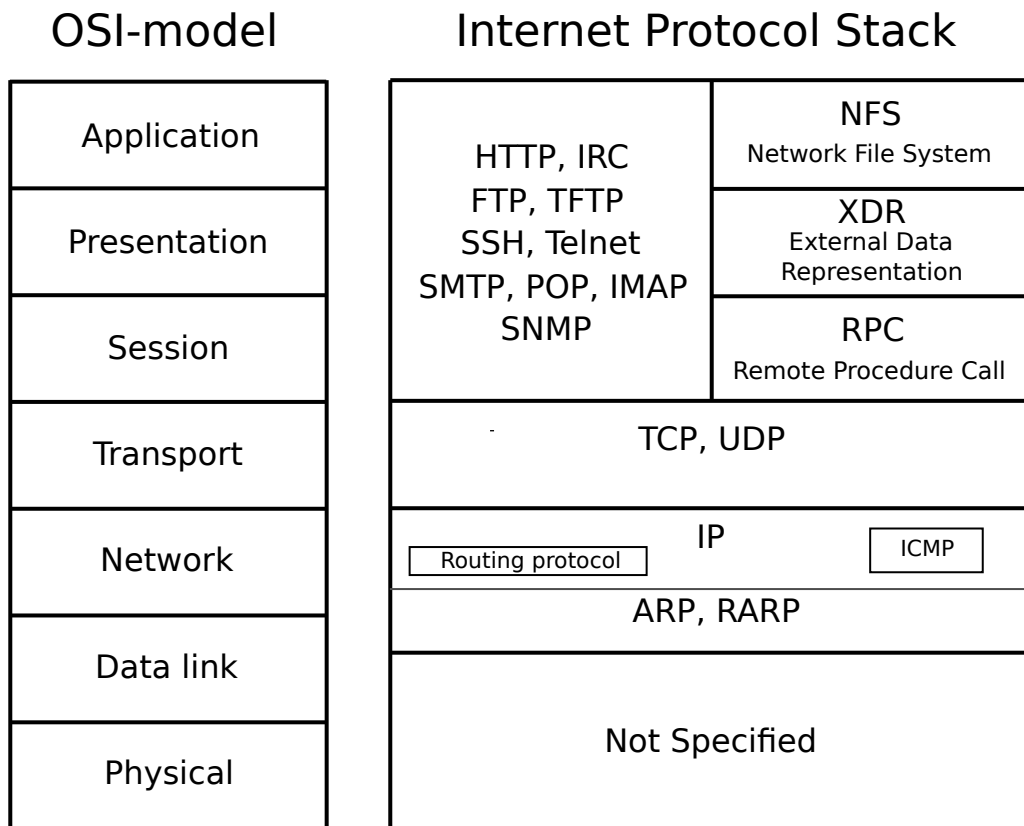# 5. Network Architecture Conceptual Frameworks

These are sometimes referred to as protocol stacks.

5.1 OSI Model

Theoretical way to layer a network. In reality, it is sometimes difficult to find technologies that cleanly separate the boundaries, especially at the higher layers.

- *1 – **Physical layer***: Transmits individual bits from one node to the next. An example is LVDS that may use a single differential signal to recover clock and data.

- *2 – **Data Link layer***: Frames the data and performs physical addressing between devices in the immediate vicinity (i.e.: the local network). In modern networks, this layer ensures error-free data transfer. An example is Ethernet, which is a protocol that defines both the physical and data link layer.

- *3 – **Network layer***: performs logical addressing to send data end-to-end in a network.

- *4 – **Transport layer***: maintains the flow control and reliable data transfer (error checking and recovery of data). An example is TCP (Transmission Control Protocol), which is a *connection-oriented* protocol. Note that UDP is considered layer 4 even though it does not implement flow control nor have reliable data transfer.

- *5 – **Session layer***: establishes, manages, and terminates connections between applications. In the TCP/IP stack, this is implemented by the application.

- *6 – **Presentation layer***: provides independence from difference in data representation, translating from application to network format and back.

- *7 – **Application layer***: provides services for an application to ensure effective communication with another application. An example is HTTP (Hypertext Transfer Protocol) used for hypermedia documents, such as HTML.

5.2 TCP/IP

OSI-model / Internet Protocol Stack diagram

OSI-model	Internet Protocol Stack
Application	HTTP, IRC FTP, TFTP SSH, Telnet SMTP, POP, IMAP SNMP — NFS (Network File System) / XDR (External Data Representation) / RPC (Remote Procedure Call)
Presentation	
Session	
Transport	TCP, UDP
Network	IP — Routing protocol / ICMP — ARP, RARP
Data link	Not Specified
Physical	

IPv4, IPv6

Static vs Dynamic IP addresses and DHCP

Media Access Control (MAC) addresses

6. Network Components

Repeater, bridge, hub, switch, gateway, router

Modem, network interface card (NIC), wireless access point

Server

- ***Tethering***
  Tethering typically involves a mobile device, such as a smartphone, sharing its cellular data connection with another device, such as a laptop or tablet, via a wired (USB) or wireless (Bluetooth or Wi-Fi) connection.

7. Network Metrics

Speed, bandwidth, throughput, latency

Error rate, packet loss, jitter

Availability, scalability

8. Network Security

Malware (viruses, spyware)

Unauthorized access (hacking), inside attacks, social engineering, phishing, pharming, DDoS – Distributed Denial of Service, ransomware

Countermeasures to each threat above (biometrics, two-factor authentication, encryption, physical security, ...)