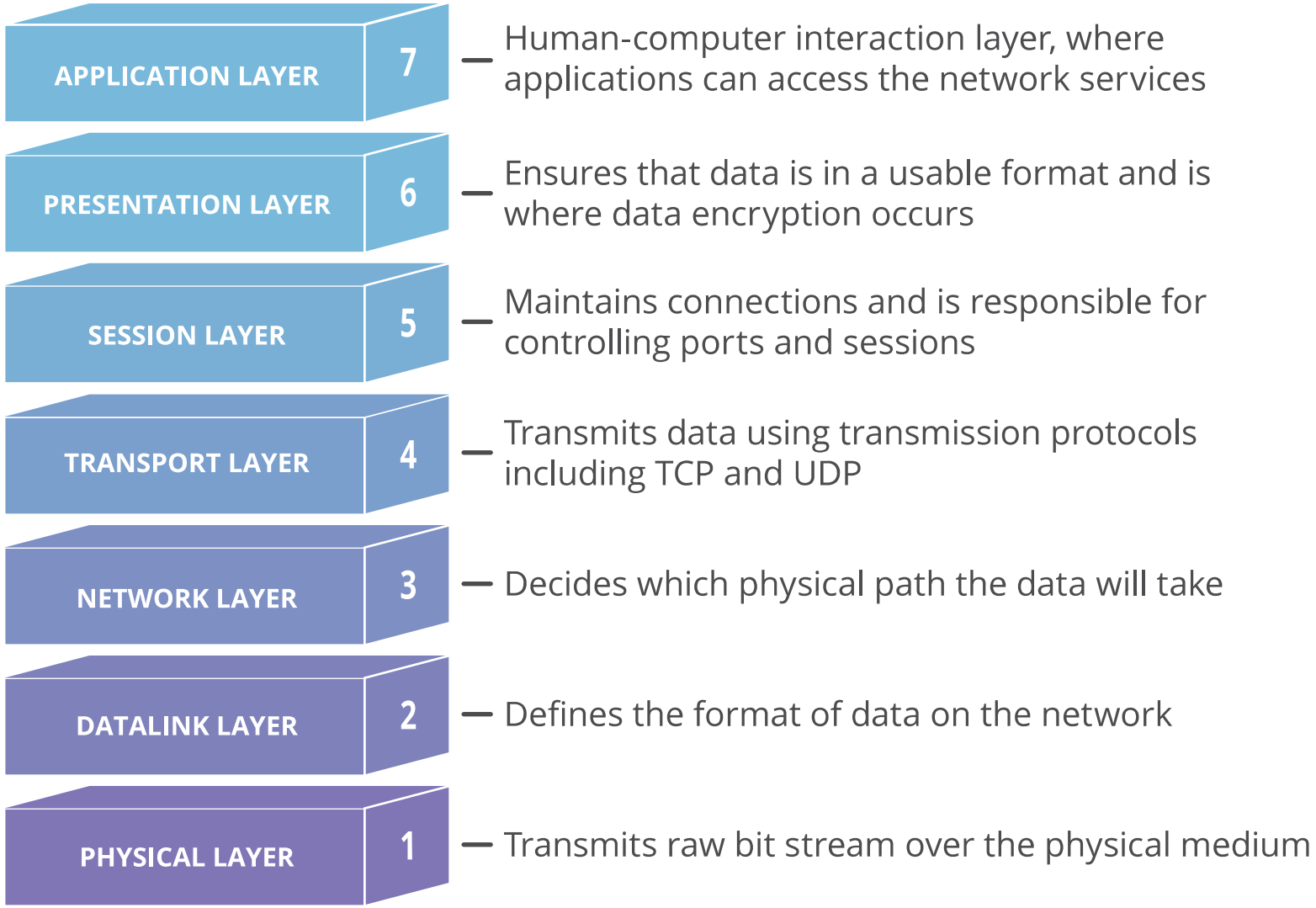
Network Basic

OSI model

- *Open Systems Interconnect*
- 7 layers which allow any computer to talk to any other computer through a network on the Internet.
- Uses standards and protocols to wrap data in packets as they head into the Internet 'wire' and to unwrap them as they come out.
- Not all layers are used.
  - e.g. Routers use layers 1-3.
  - Most Internet services don't use layer 5. The exceptions are web conferencing and internet TV.
  - Digital telephone systems skip many of the higher layers.
- OSI was retro-fitted to existing practices and technologies.

OSI



(img source: https://www.cloudflare.com/learning/ddos/glossary/open-systems-interconnection-model-osi/)

OSI

Various protocols/technologies handle the mapping from layer to layer:

- MAC to IP -> ARP
- public IP to public IP -> routing protocols
- public IP to private IP -> NAT
- IP to domain name -> DNS
- (search terms to domain name ->Google)

MAC address

MAC

- Media Access Control
- In practice, each NIC (network card) has a “unique” MAC address in the form of a 48-bit hexadecimal number 'burned' in to each NIC.
  - The **ARP protocol** manages the matching of MAC addresses to IP addresses.
  - ARP allows IP addresses (layer 3) to be mapped to MAC addresses (layer 2)

DNS

DNS

- Domain Name System
- A system of name servers distributed around the internet which translate URL domain names into IP addresses.
  - More reading: https://www.cloudflare.com/learning/dns/what-is-dns/
- An old system which is susceptible to attack.
  - Fallibility of the DNS system http://dns.measurement-factory.com/surveys/openresolvers.html
  - Kaminsky on the DNS cache poisoning attack (12 mins) http://www.securitytube.net/video/110
  - DNS cache poisoning https://www.cloudflare.com/learning/dns/dns-cache-poisoning/

Hub/Switch

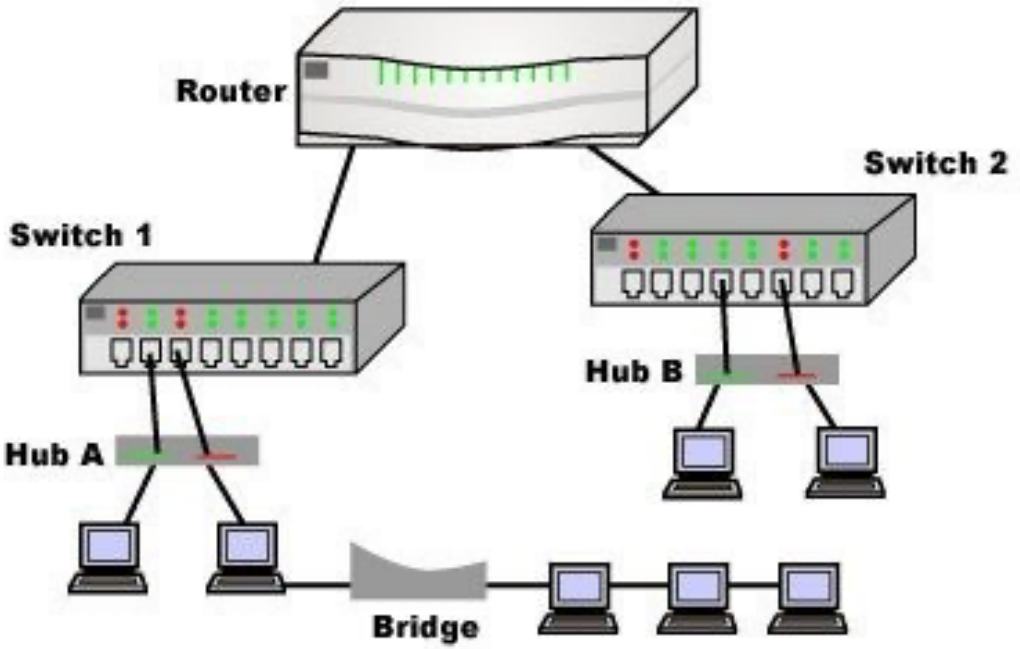
Link, Transport and Network layer devices (often purpose-built computers) which interconnect other devices and computer using network cables and wireless transmitters. These devices have multiple NICs.

- Hub (physical layer)
  - A Hub echoes all packets received to all connected devices.
- Switch (physical+link layer)
  - A Switch echoes all packets received to devices in their corresponding destinations, as defined by MAC addresses.
  - Switches use ARP to link the MAC addresses of their interfaces with IP addresses.
  - Many switches, when overloaded revert to hub-like behaviour.
  - http://www.slideshare.net/ishraqabd/packet-sniffing-in-switched-lans
  - http://www.linuxjournal.com/article/5869
  - http://articles.manugarg.com/arp_spoofing.pdf

Bridge/Router

- Bridge (physical + link layer)
  - A Bridge acts like a switch that can link two subnets or link two parts of a network which use different and incompatible physical layers or cables.
  - Bridges can break security by linking trusted LANs to the internet.

- Router (network + link layer + physical)
  - A Router can pass packets to a particular interface by checking the destination IP address and by using a routing algorithm to calculate the most successful path through a network of routers.



NAT

Network Address Translation

- A type of router which can open an IP packet and re-address it.
- Originally developed to allow many hosts (PCs) to share a common IP address.
- Incoming traffic is allocated to different internal IPs depending on the ports used for each incoming packet.
- Often used as a poor-man's proxy server because of the ability of NAT to hide the internal details of a private network.
- Often the principal feature of a firewall.
- Microsoft ICS is a common implementation of NAT: https://docs.microsoft.com/en-us/troubleshoot/windows-server/networking/set-up-internet-connection-sharing

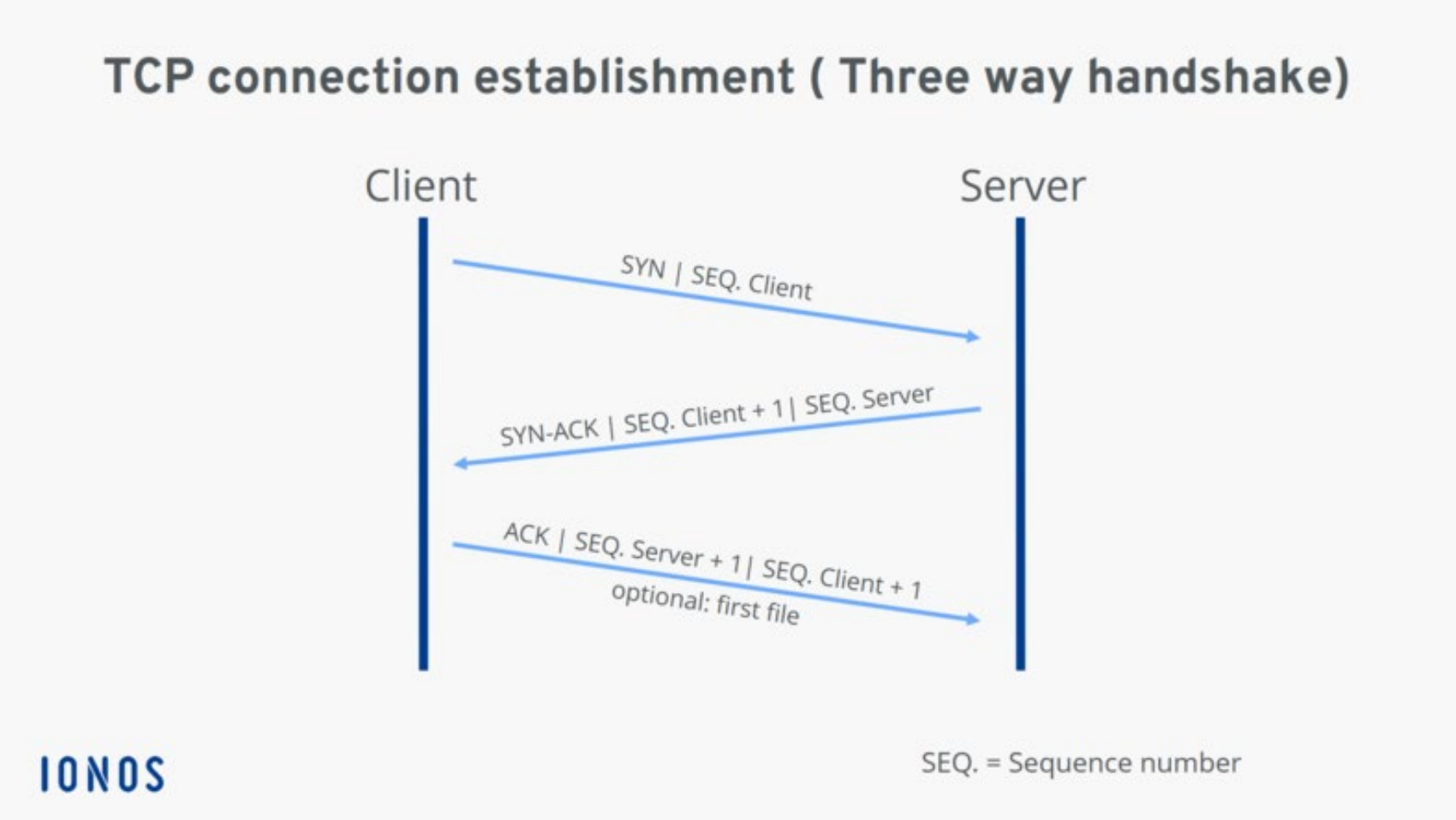
Common Protocols

- IP
  - Internet protocol (network layer)
  - An IP-addressable data container (packet) used to carry TCP and UDP packets through a network or internet.
- ICMP
  - Internet Control Message Protocol
  - Used by operating systems to exchange error messages and by network tools such as *Ping* and *TraceRoute*.
  - Does not use ports.

TCP

- Transmission Control Protocol
- A reliable but asynchronous (not real-time) data container carried by the IP protocol.
- Creates connections (sockets) over which packets can be exchanged reliably and in the correct sequence.
- Sometimes referred to as TCP/IP
- Used by many internet services such as FTP, HTTP, Telnet, POP as defined by their respective ports.
- Uses a 3-way handshake (syn, syn-ack, syn) to establish a connection which cannot be spoofed.

TCP handshake



(img source: https://www.ionos.com/digitalguide/server/know-how/introduction-to-tcp/)

UDP

- User Datagram Protocol
- An un-reliable but fast (near real-time) data container carried by the IP protocol.
- Packets are sent without prior connection (no set-up delay) but may be lost or arrive out of sequence.
- Used for multimedia streaming, telephony and DNS queries.
- Uses ports to define the service.
- source IP is easily spoofed because the source address is never checked.

Ports

- Well-known ports:
  - 0-1023
  - Services like telnet (23), FTP(20, 21), DNS(53), http(80), https (443), mail(110, 25), ssh(22)
- Registered ports
  - 1024 – 49,151
  - registered by companies for proprietary purposes.
    - many no-longer used

- Dynamic / private ports
  - 49,152 – 65,535
  - ports allocated at run-time by processes.
  - particular ports are known for the exploits that use them: http://www.grc.com/port_139.htm
- Port numbers are NOT bound to particular services.
- Any port can be used - a web server can operate on port 22 and a telnet server can operate on port 80.

IP Addresses

- Some IP address ranges are reserved for particular types of (private) networks.
- Private (non-routable) blocks of IP addresses – use behind a proxy server:
  - 10.0.0.0 through 10.255.255.255 Class A (16,387,064)
  - 172.16.0.0 through 172.31.255.255 (1 million)
  - 192.168.0.0 through 192.168.255.255 Class C (64,516)
- Default gateway (represents all possible IP addresses)
  - 0.0.0.0
    - 0 and 255 are reserved for ALL and Broadcast addresses

- Loopback address (localhost) of the local NIC
  - 127.0.0.1
- D Class Multicast addresses
  - 224.0.0.0 - 239.255.255.255
- E class reserved addresses
  - 240.0.0.0 - 254.255.255.255
- Broadcast address (for all local subnets)
  - 255.255.255.255