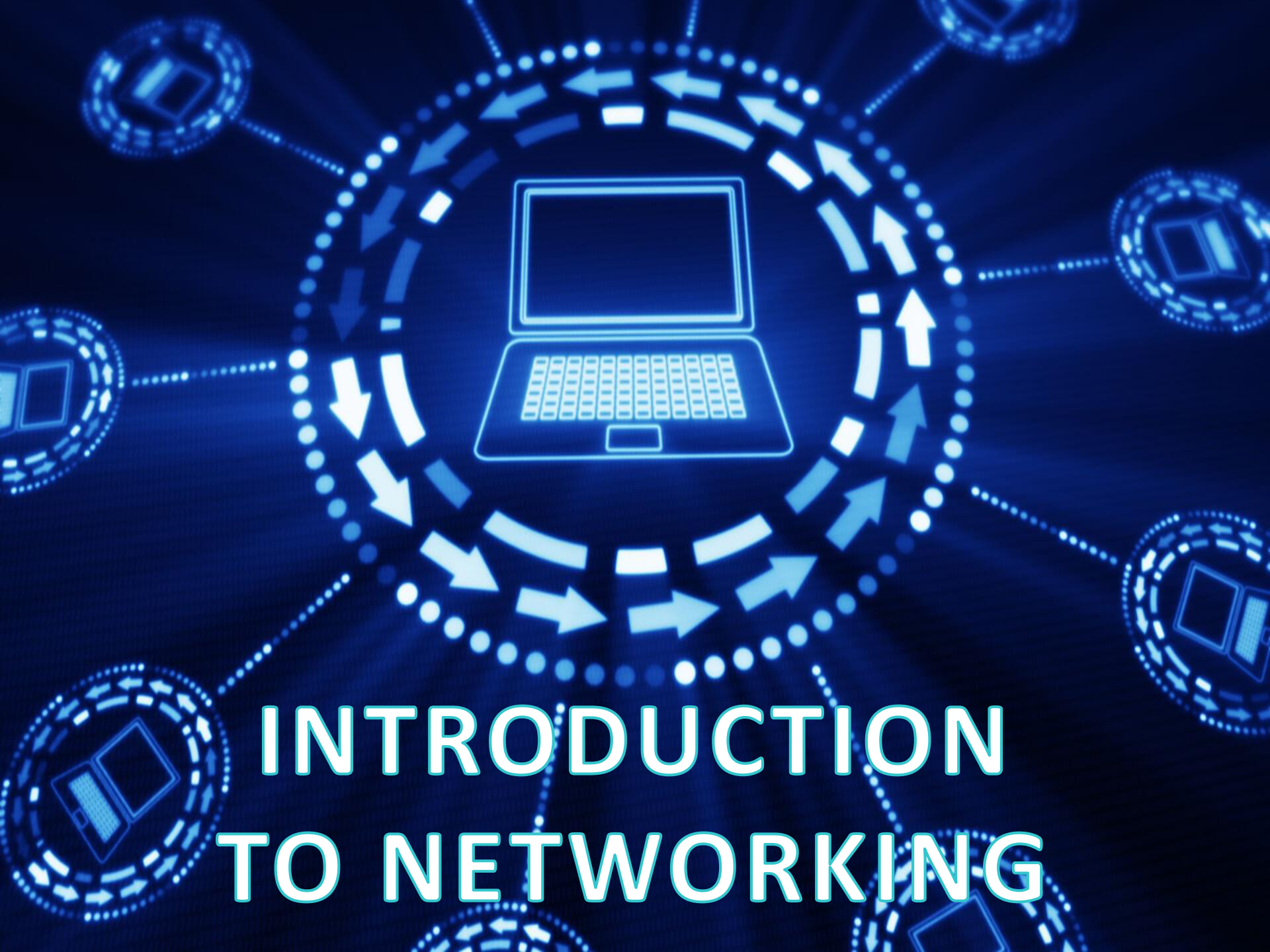

INTRODUCTION
TO NETWORKING

NETWORKING

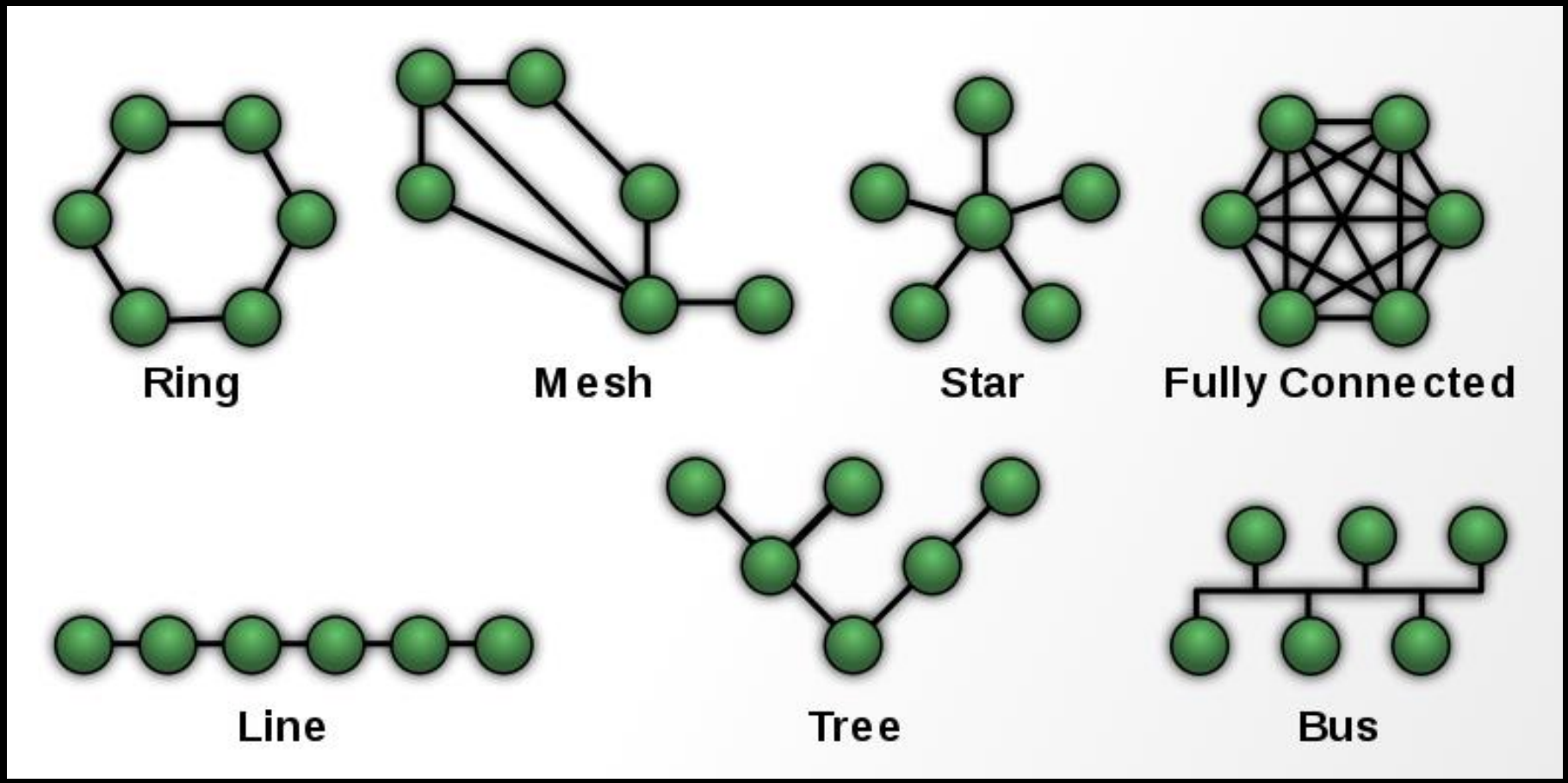
- Computers needs to communicate in order to share data
- Stand-alone computers can only communicate using transfer of removable media that tends to be cumbersome
- Thus computers started being connected together allowing on-the-fly transfer of data: networks
- Many techniques exist that allow transfer of data, from wired connection using electrical signals to wireless connections and optical communication
- Regardless of the type of computer being used, each computer needs a way to communicate: NIC
- A NIC allows data to be sent over a network

NETWORK DEVICES

- Each NIC has its own address called a MAC (Media Access Control) address
  - The form of this address depends on the networking technology being used (such as Ethernet and Token Ring)
- Any signal degrades the further it travels. Thus additional devices are required between the sender and receiver:
  - Repeaters
  - Bridges
- In addition, several different computers might want to communicate between each other:
  - Switches
  - Routers

NETWORKING TOPOLOGIES

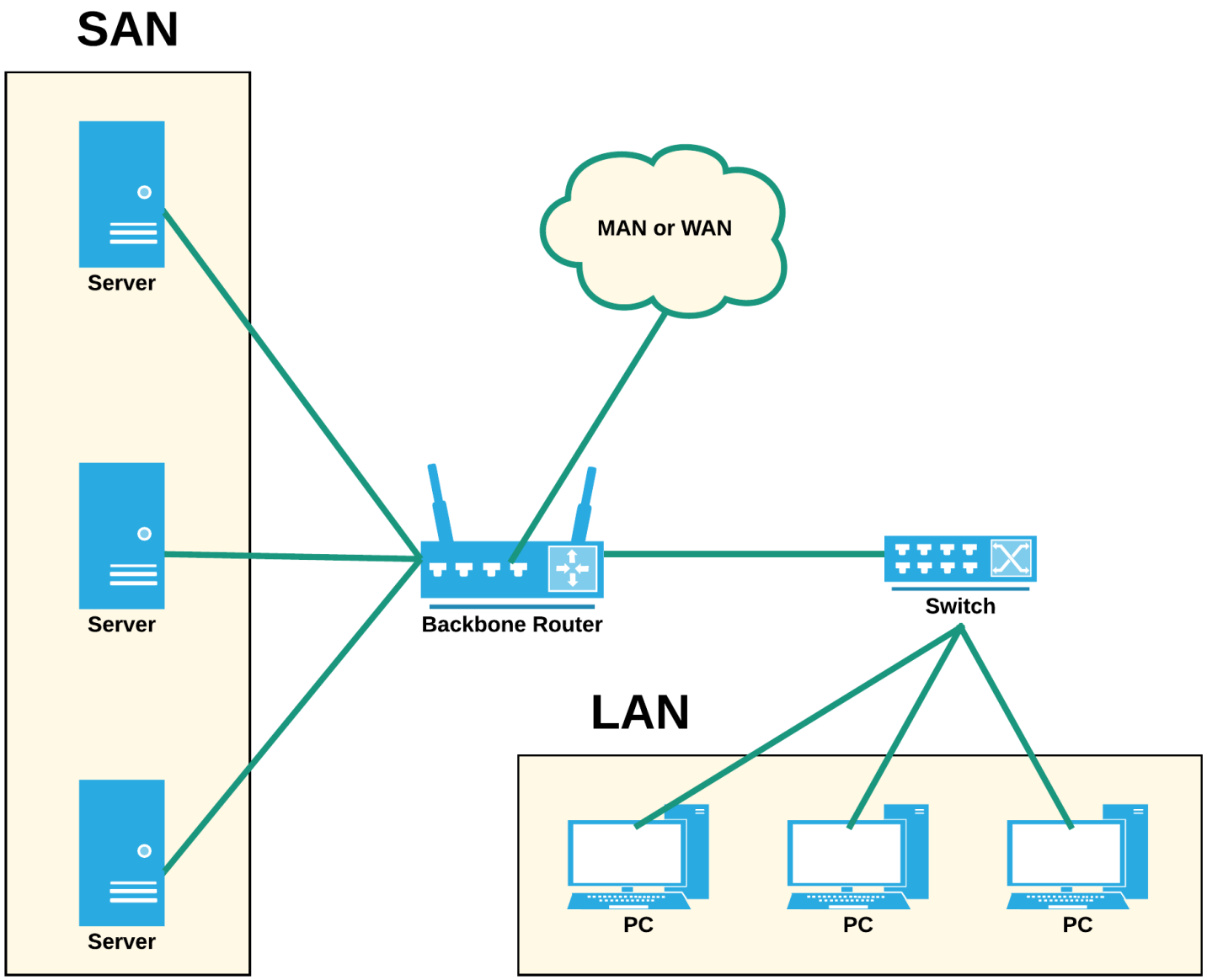
- Computers might be connected in a variety of ways



NETWORK TOPOLOGIES

- A network might span varying distances:
  - LAN: Limited geographically, high bandwidth, full time connectivity
  - WAN: large geographical area, lower bandwidth and full or part-time connectivity
  - MAN: two or more LAN's in a geographic area
  - SAN: Dedicated link to move data between servers and storage resources
- Another classification is by data access:
  - Intranet: only allowed users are given access
  - Extranet: provide services to the world

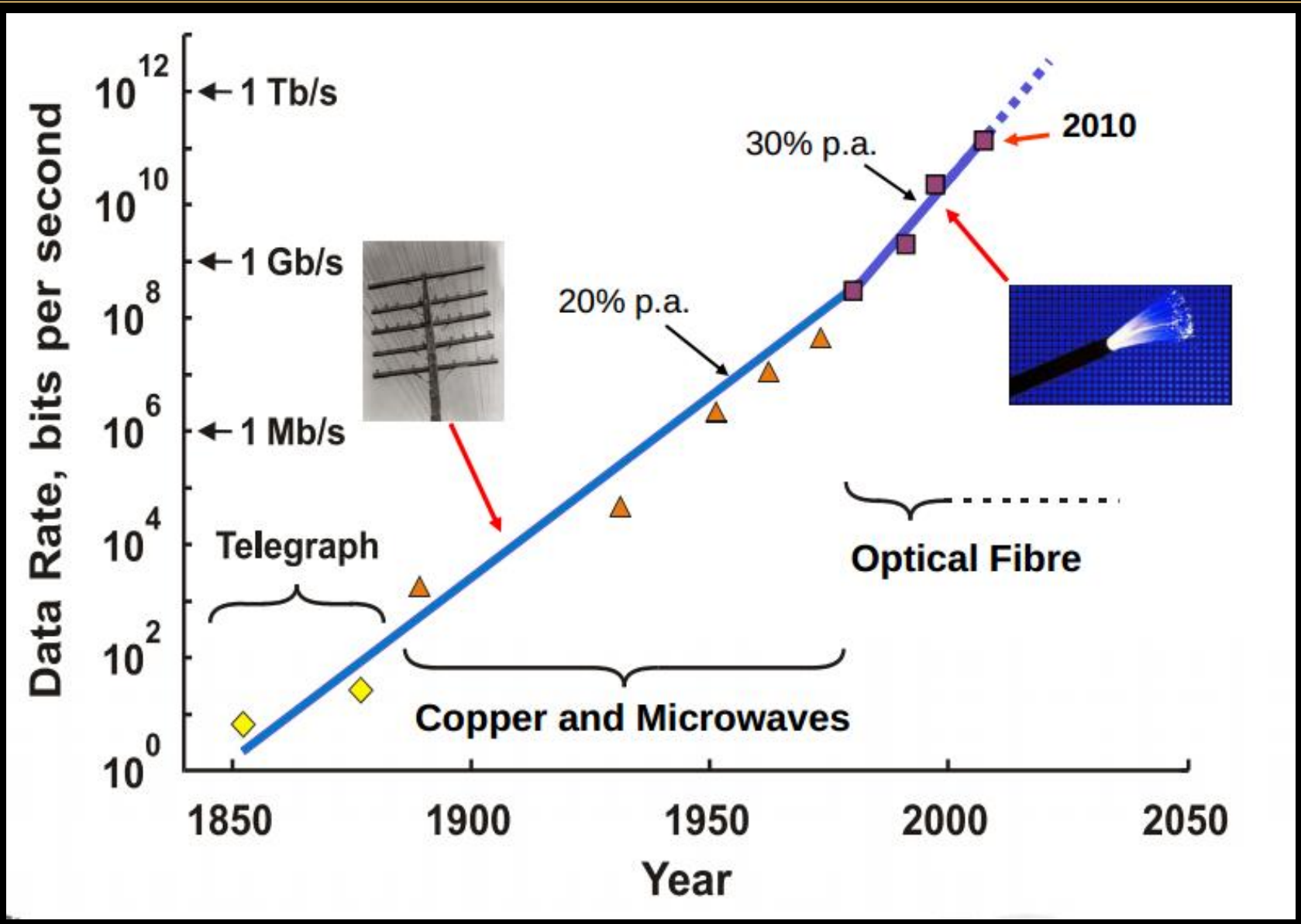
NETWORKING TOPOLOGIES



BANDWIDTH

- The most important factor in networking is bandwidth
  - Flow of data per unit time
- Bandwidth is
  - Finite
  - Not free
  - Affects network design
- Units: bps, Kbps, Mbps, Gbps, Tbps
- Most fundamental restriction of bandwidth are the type of media used and the LAN or WAN technology used
- Throughput is the actual bandwidth achieved

BACKHAUL NETWORK BANDWIDTH GROWTH



Note: p.a means per annum

NETWORK LAYERS

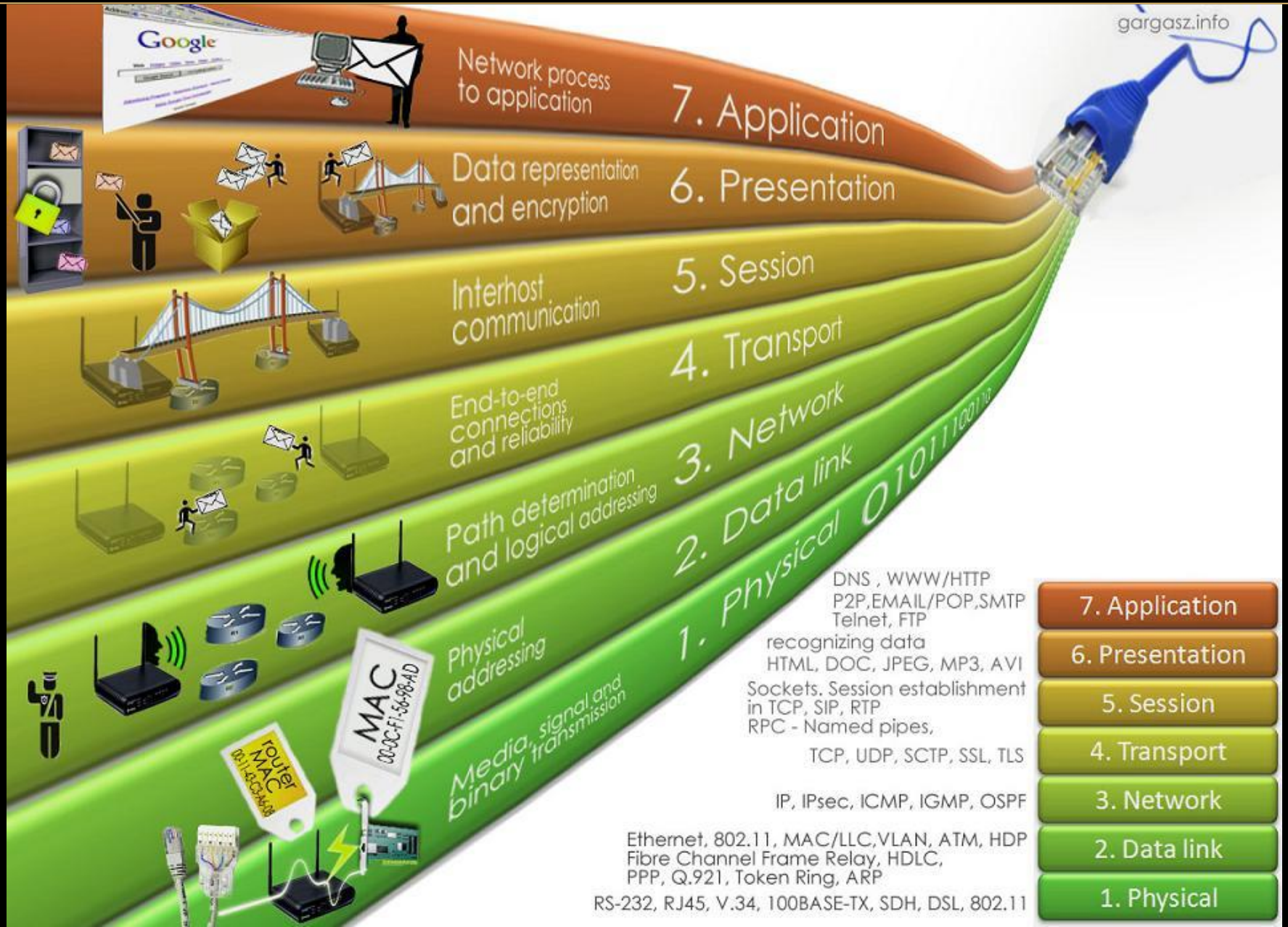
- For application to be able to communicate, they need to communicate using a single language
- Thus data communications is split into layers
- Layer X will speak to Layer X on the other computer
- One layer will pass data to the layer underneath
- The lowest layer will communicate directly with the lower layer on the other computer
- The OSI model is a framework showing how data travels to the network and back
- More accurate representation of networks
- Each layers normally introduces a header in the data packet

OSI MODEL

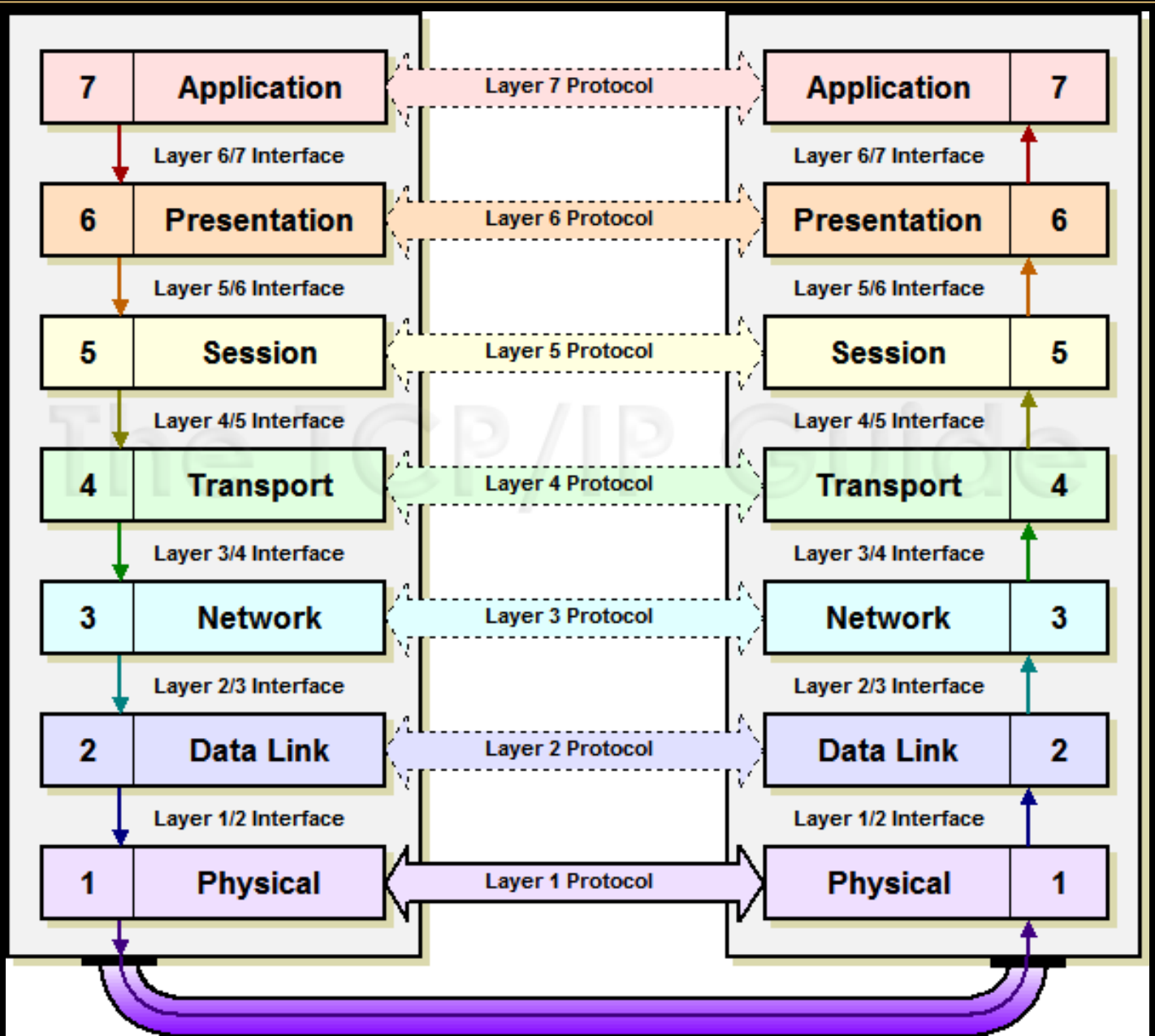
OSI (Open Source Interconnection) 7 Layer Model

Layer	Application/Example		Central Device/ Protocols		DOD4 Model
Application (7) Serves as the window for users and application processes to access the network services.	**End User layer** Program that opens what was sent or creates what is to be sent Resource sharing • Remote file access • Remote printer access • Directory services • Network management		**User Applications** SMTP	GATEWAY	Process
Presentation (6) Formats the data to be presented to the Application layer. It can be viewed as the "Translator" for the network.	**Syntax layer** encrypt & decrypt (if needed) Character code translation • Data conversion • Data compression • Data encryption • **Character Set Translation**		JPEG/ASCII EBDIC/TIFF/GIF PICT		
Session (5) Allows session establishment between processes running on different stations.	**Synch & send to ports** (logical ports) Session establishment, maintenance and termination • Session support - perform security, name recognition, logging, etc.		**Logical Ports** RPC/SQL/NFS NetBIOS names		
Transport (4) Ensures that messages are delivered error-free, in sequence, and with no losses or duplications.	**TCP** Host to Host, Flow Control Message segmentation • Message acknowledgement • Message traffic control • Session multiplexing	PACKET FILTERING	TCP/SPX/UDP		Host to Host
Network (3) Controls the operations of the subnet, deciding which physical path the data takes.	**Packets** ("letter", contains IP address) Routing • Subnet traffic control • Frame fragmentation • Logical-physical address mapping • Subnet usage accounting		**Routers** IP/IPX/ICMP	Can be used on all layers	Internet
Data Link (2) Provides error-free transfer of data frames from one node to another over the Physical layer.	**Frames** ("envelopes", contains MAC address) [NIC card — Switch — NIC card] (end to end) Establishes & terminates the logical link between nodes • Frame traffic control • Frame sequencing • Frame acknowledgment • Frame delimiting • Frame error checking • Media access control		**Switch Bridge WAP** PPP/SLIP	Land Based Layers	Network
Physical (1) Concerned with the transmission and reception of the unstructured raw bit stream over the physical medium.	**Physical structure** Cables, hubs, etc. Data Encoding • Physical medium attachment • Transmission technique - Baseband or Broadband • Physical medium transmission Bits & Volts		**Hub**		

OSI MODEL

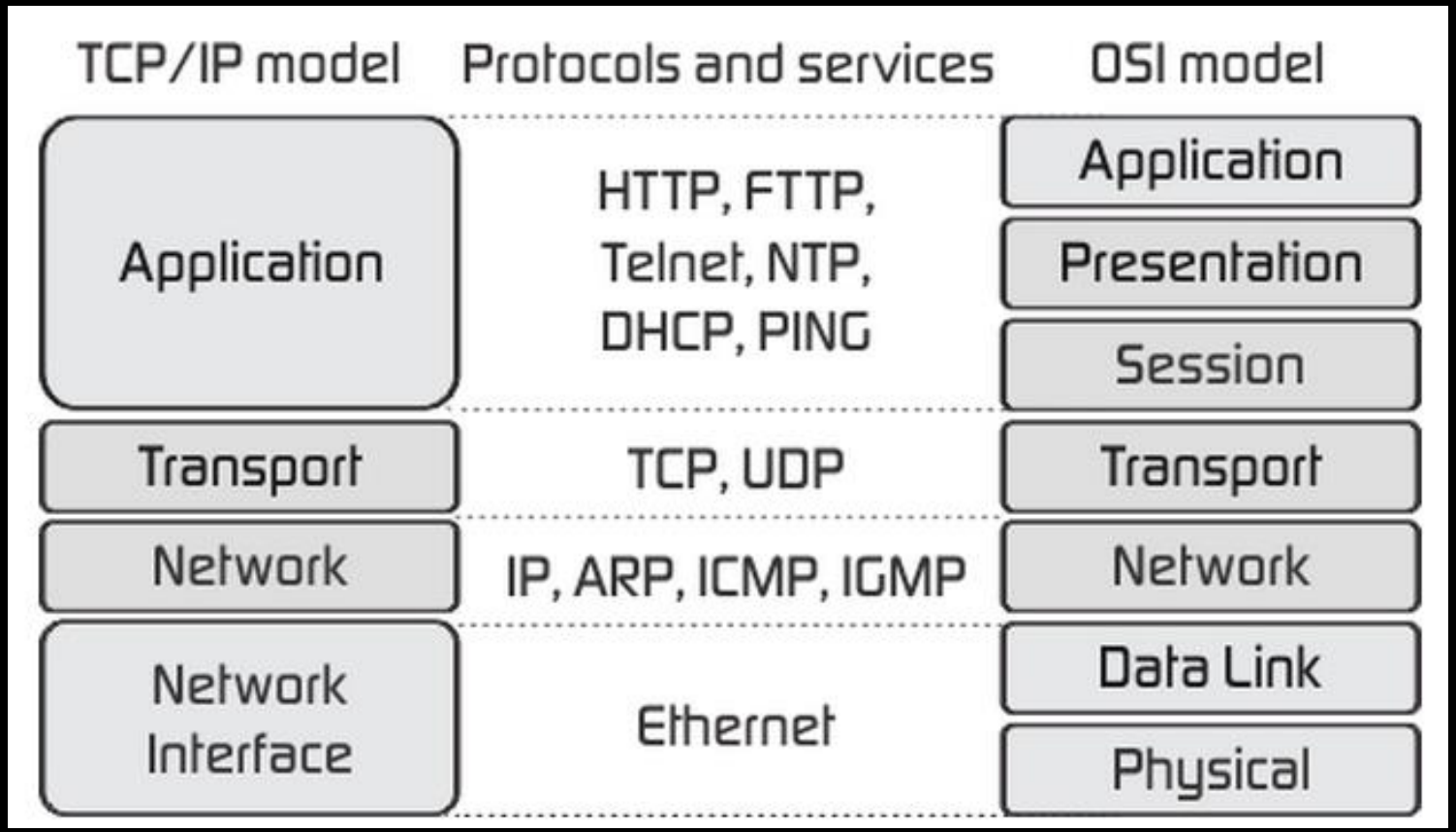

gargasz.info
Google
Network process to application
7. Application
Data representation and encryption
6. Presentation
Interhost communication
5. Session
End-to-end connections and reliability
4. Transport
Path determination and logical addressing
3. Network
Physical addressing
2. Data link
Media, signal and binary transmission
1. Physical
MAC
router MAC
DNS , WWW/HTTP
P2P,EMAIL/POP,SMTP
Telnet, FTP
recognizing data
HTML, DOC, JPEG, MP3, AVI
Sockets. Session establishment
in TCP, SIP, RTP
RPC - Named pipes,
TCP, UDP, SCTP, SSL, TLS
IP, IPsec, ICMP, IGMP, OSPF
Ethernet, 802.11, MAC/LLC,VLAN, ATM, HDP
Fibre Channel Frame Relay, HDLC,
PPP, Q.921, Token Ring, ARP
RS-232, RJ45, V.34, 100BASE-TX, SDH, DSL, 802.11
7. Application
6. Presentation
5. Session
4. Transport
3. Network
2. Data link
1. Physical

OSI MODEL


7
Application
Layer 7 Protocol
Application
7
Layer 6/7 Interface
Layer 6/7 Interface
6
Presentation
Layer 6 Protocol
Presentation
6
Layer 5/6 Interface
Layer 5/6 Interface
5
Session
Layer 5 Protocol
Session
5
Layer 4/5 Interface
Layer 4/5 Interface
4
Transport
Layer 4 Protocol
Transport
4
Layer 3/4 Interface
Layer 3/4 Interface
3
Network
Layer 3 Protocol
Network
3
Layer 2/3 Interface
Layer 2/3 Interface
2
Data Link
Layer 2 Protocol
Data Link
2
Layer 1/2 Interface
Layer 1/2 Interface
1
Physical
Layer 1 Protocol
Physical
1

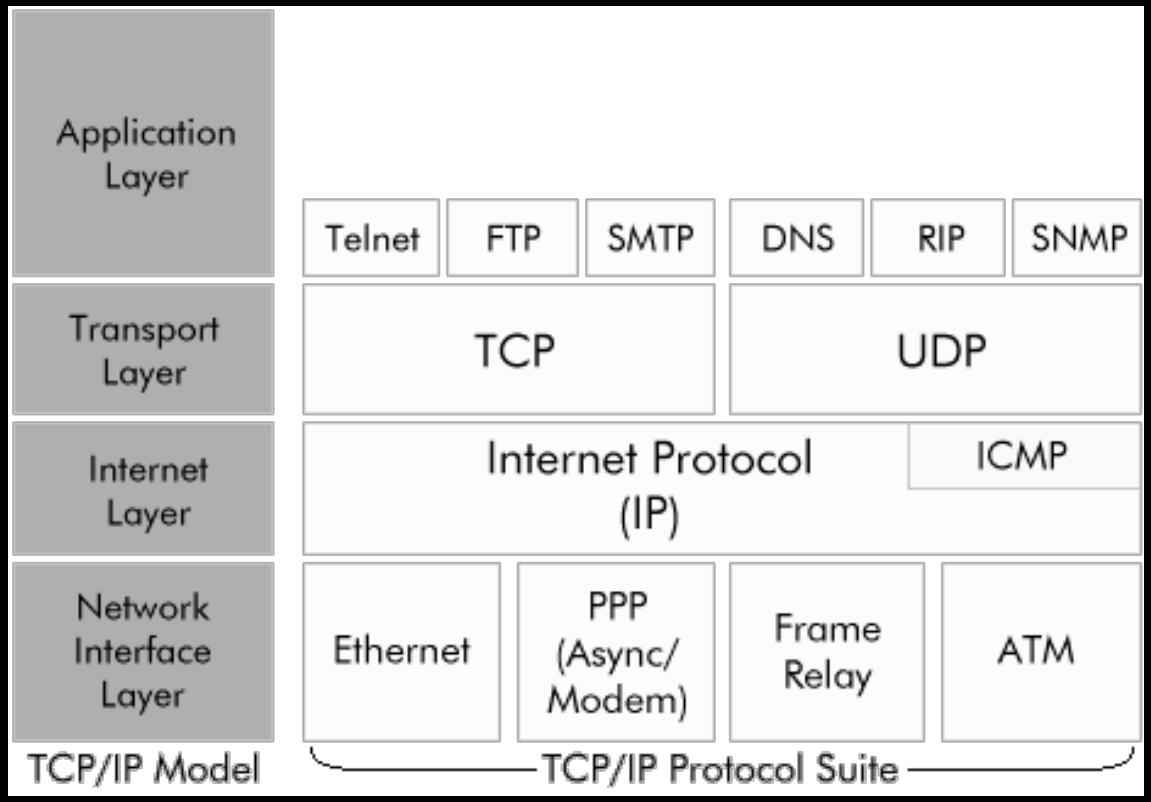
TCP/IP MODEL

- Mode used for internet connectivity
- Note correspondence with OSI layer



TCP/IP LAYER IMPLEMENTATION

- TCP/IP uses the Client/Server Model
  - The server is an application that offers services and receives requests from clients
  - The Client is an application that requests services from servers



THE INTERNET

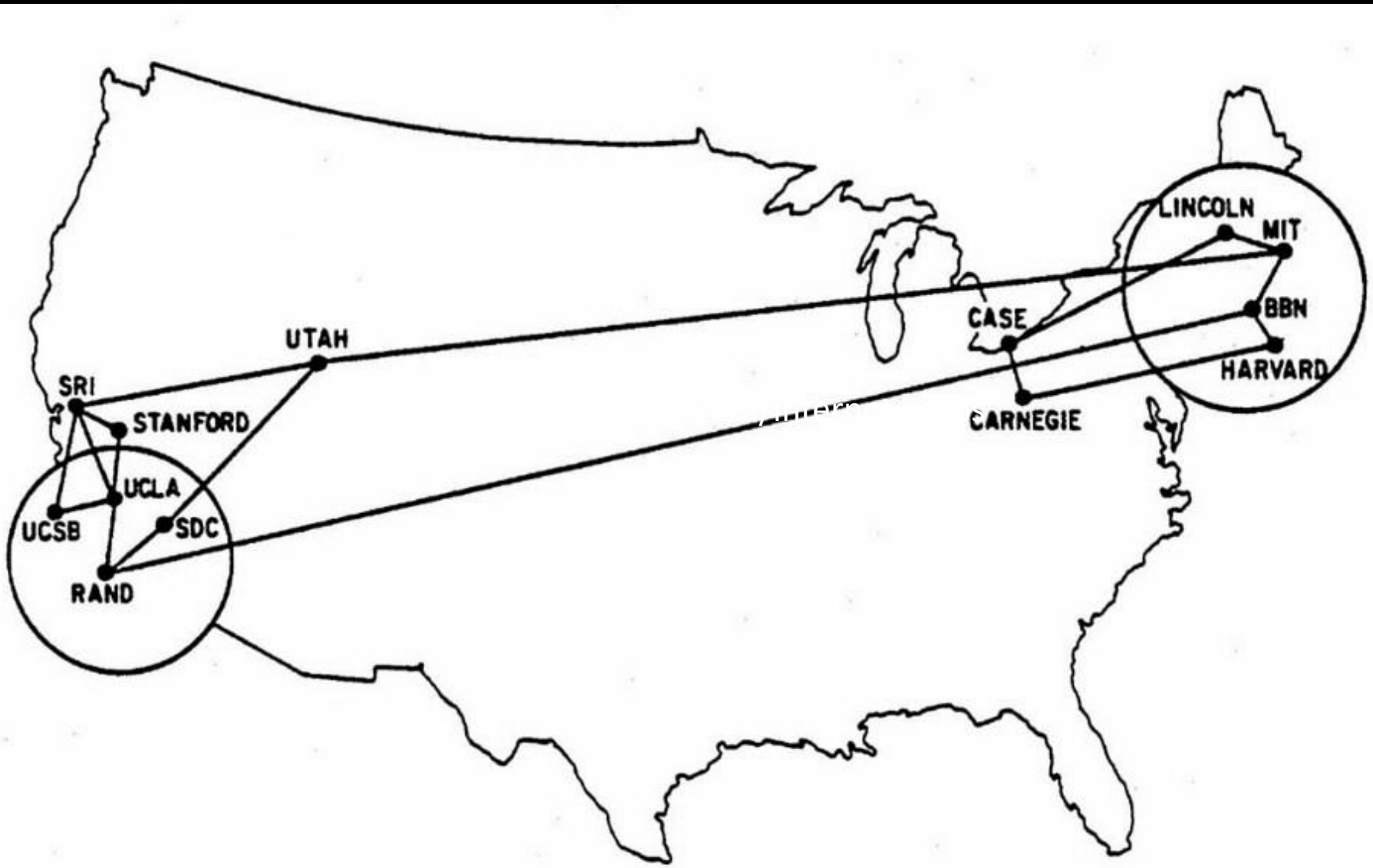
- A collection of computers communicating with each other through the use of TCP/IP protocol suite
- It was a result from research in the American defence agency for a network to withstand nuclear holocaust
- No one owns the internet, people pay for connectivity
- The protocol suite evolved (and still evolves) through the use of approved standards (www.ietf.org)
  - The Internet Engineering Steering Group (IESG) decides on new standards
  - It publishes RFCs (Request For Comments) containing new proposed standards

BEFORE THE INTERNET: ARPANET

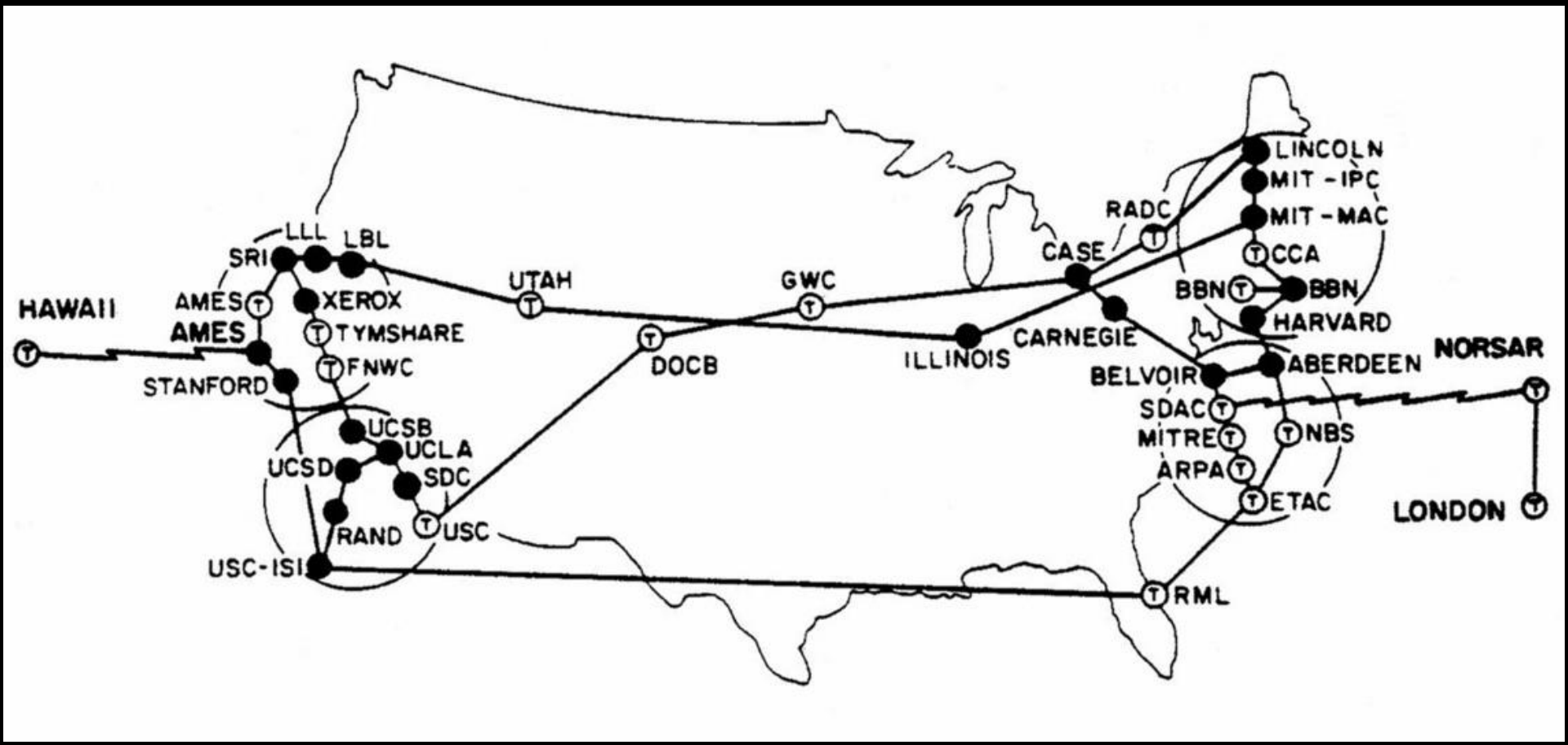
https://www.vox.com/a/internet-maps

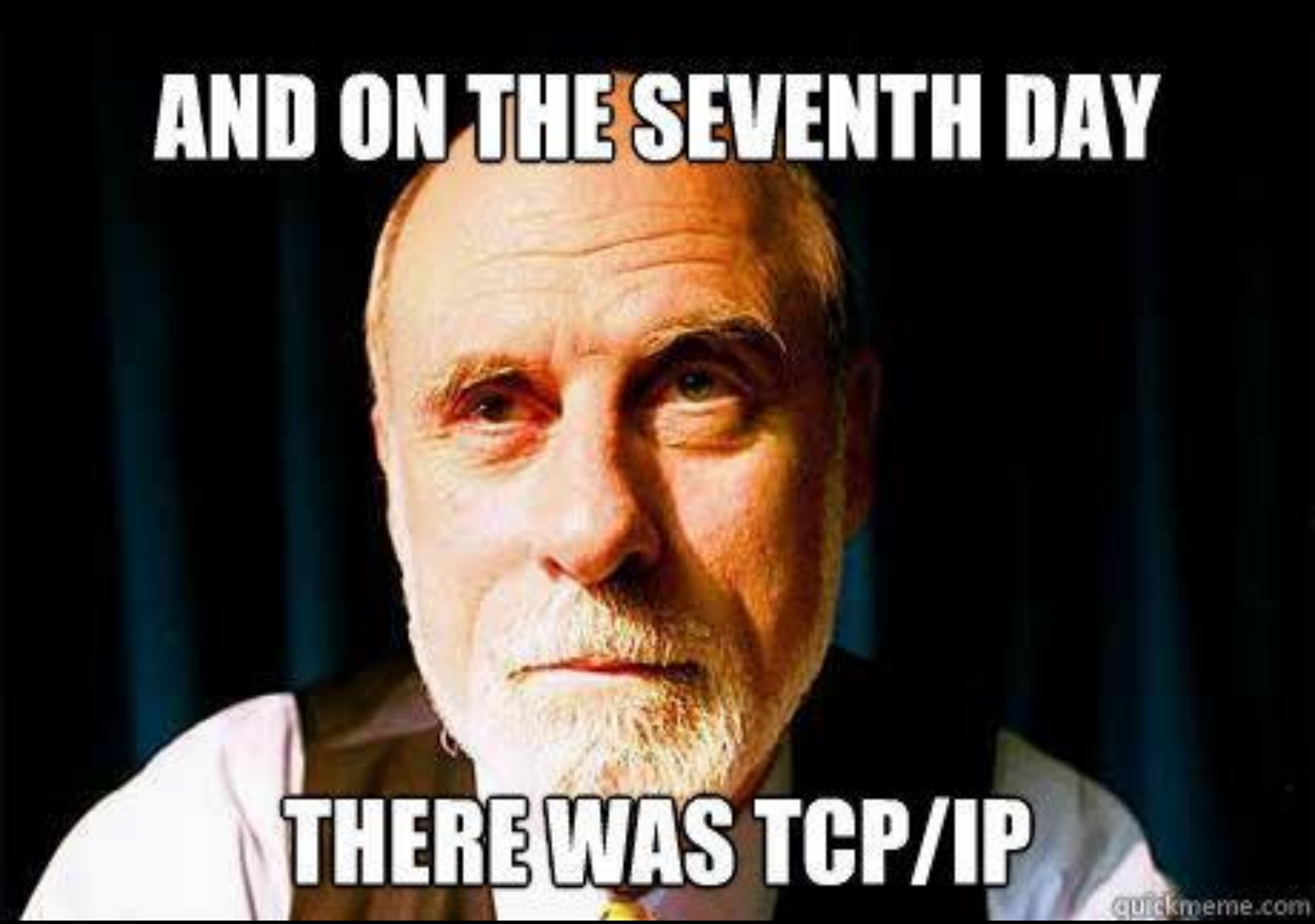
The ARPANET in December 1969

1970: ARPANET EXPANDS

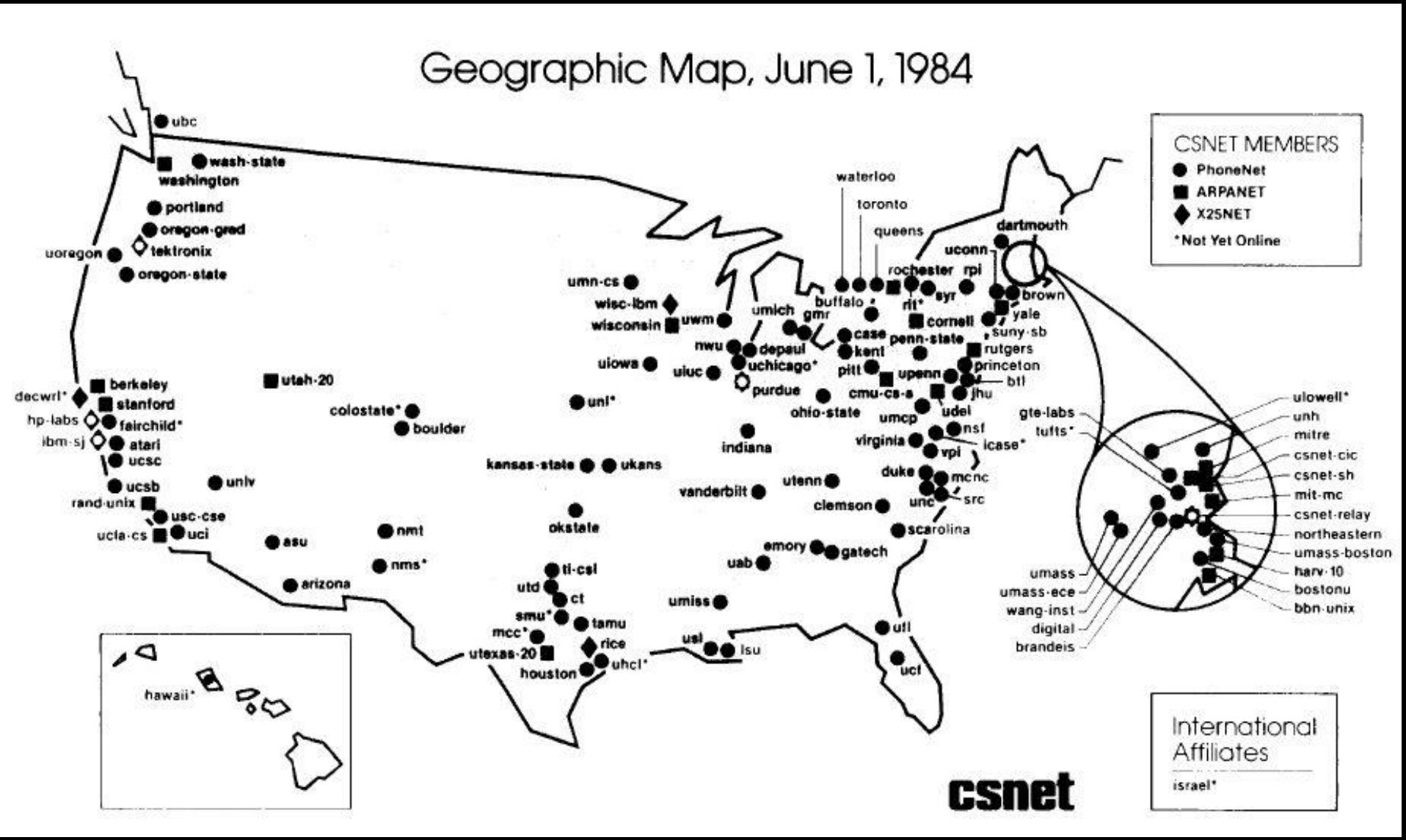


1973: ARPANET GOES INTERNATIONAL

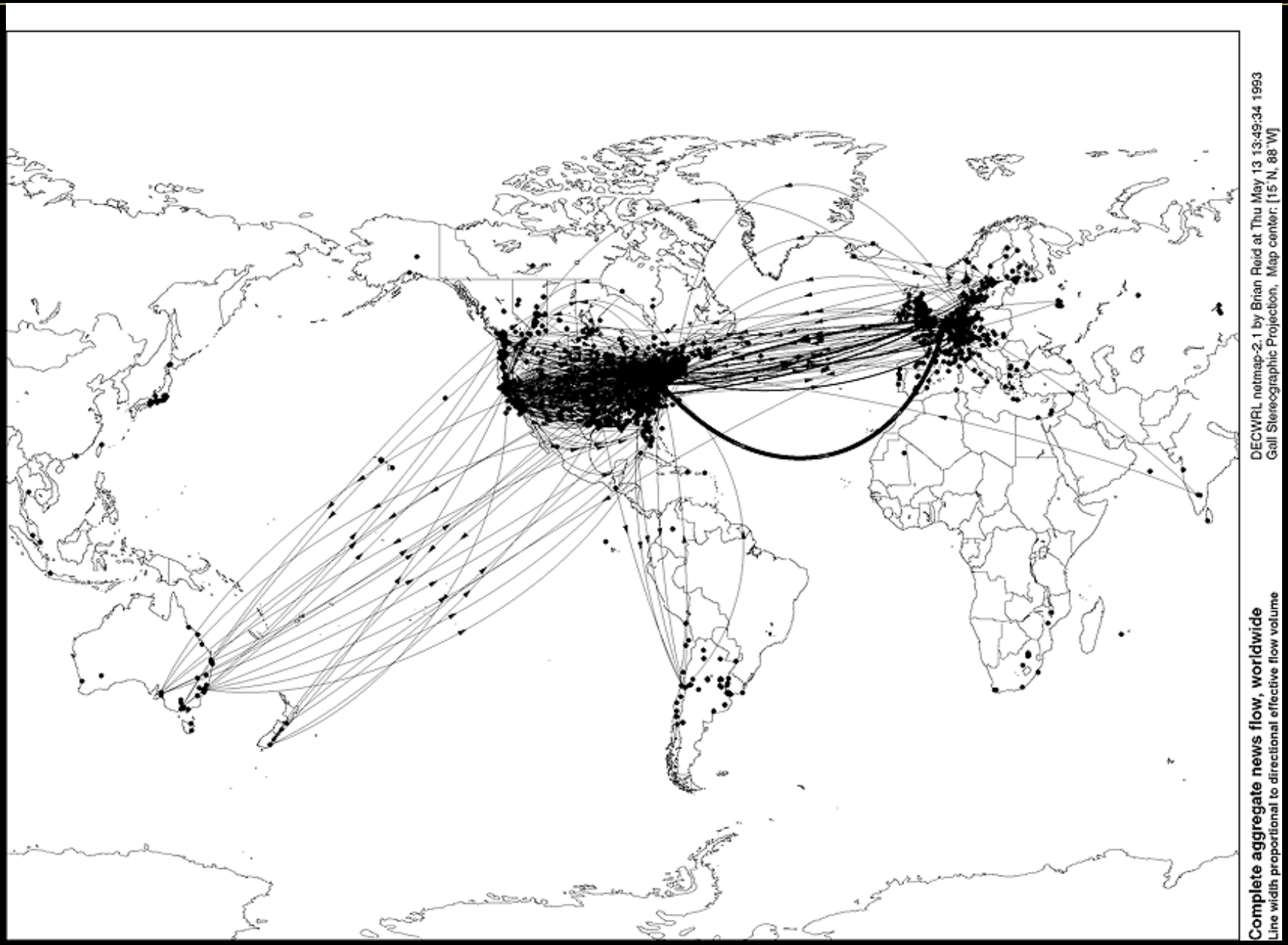



AND ON THE SEVENTH DAY
THERE WAS TCP/IP
quickmeme.com

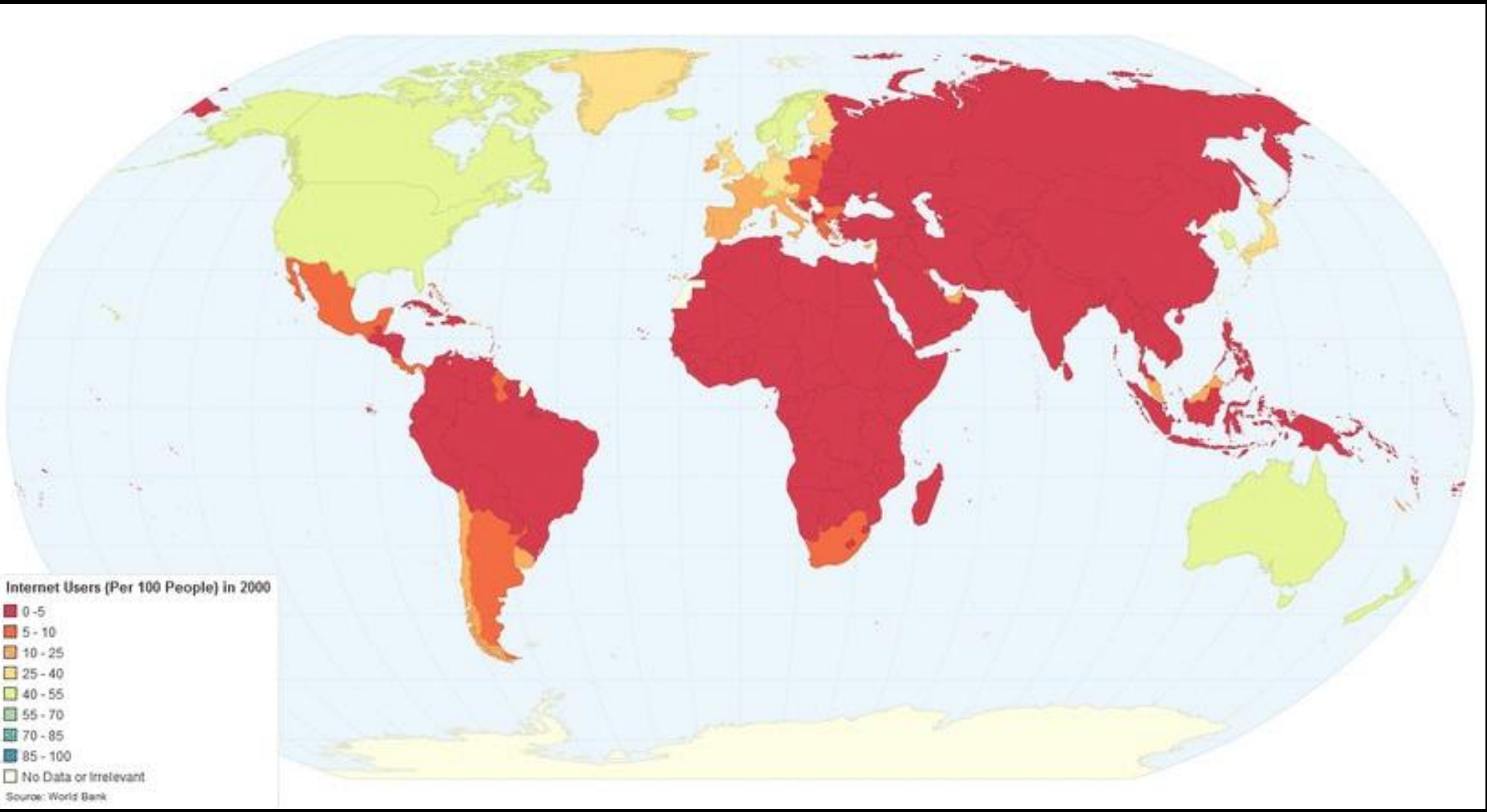
1984: ARPENET BECOMES THE INTERNET



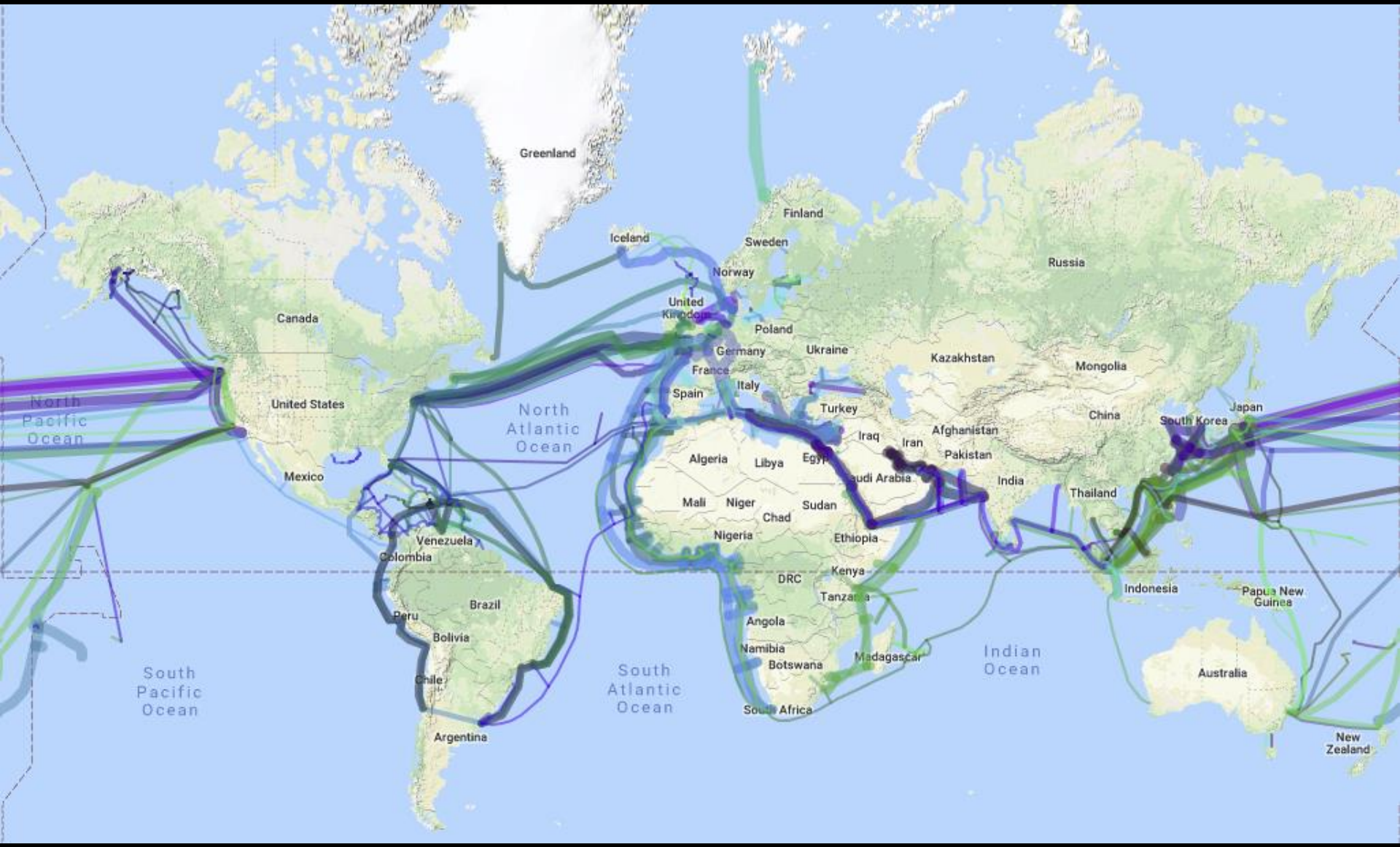
1993: THE INTERNET BECOMES A GLOBAL NETWORK



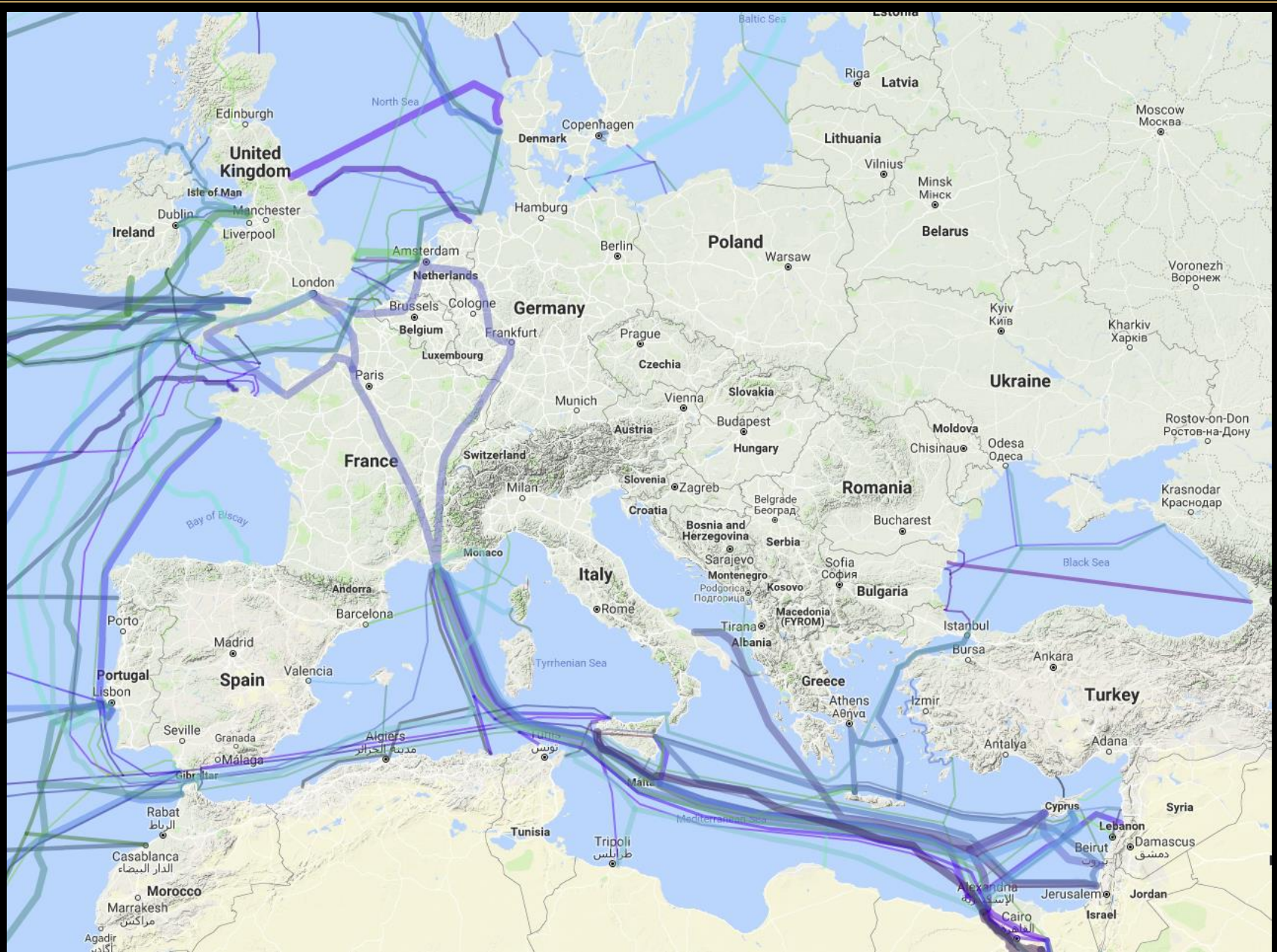
THE INTERNET CONQUERS THE WORLD



INTERNET BACKBONE LINKS



INTERNET BACKBONE LINKS



ETHERNET: A SIMPLE OVERVIEW

- Ethernet is a network protocol that controls how data is transmitted over a LAN
  - A protocol is a set or rules (the language) that govern the communication between computers on a network
- When a machine on a network wants to send data to another, it senses the carrier (“wire”)
- If it is free, it sends the data packet on the network, and all other devices check the packets to see whether they are the recipient. The recipient consumes the packet.
- If there is already a packet on the highway, the device that wants to send holds back for some thousandths of a second to try again until it can send

ETHERNET FRAMES

- A data packet on an Ethernet link is called an Ethernet packet, which transports an Ethernet frame as its payload
- Computers on the network are identified with a MAC address, an example of which is: 0F:A2:27:15:84:10
- Use `ifconfig` (Unix) or `ipconfig` (Windows) to find out the MAC addresses of your NIC devices

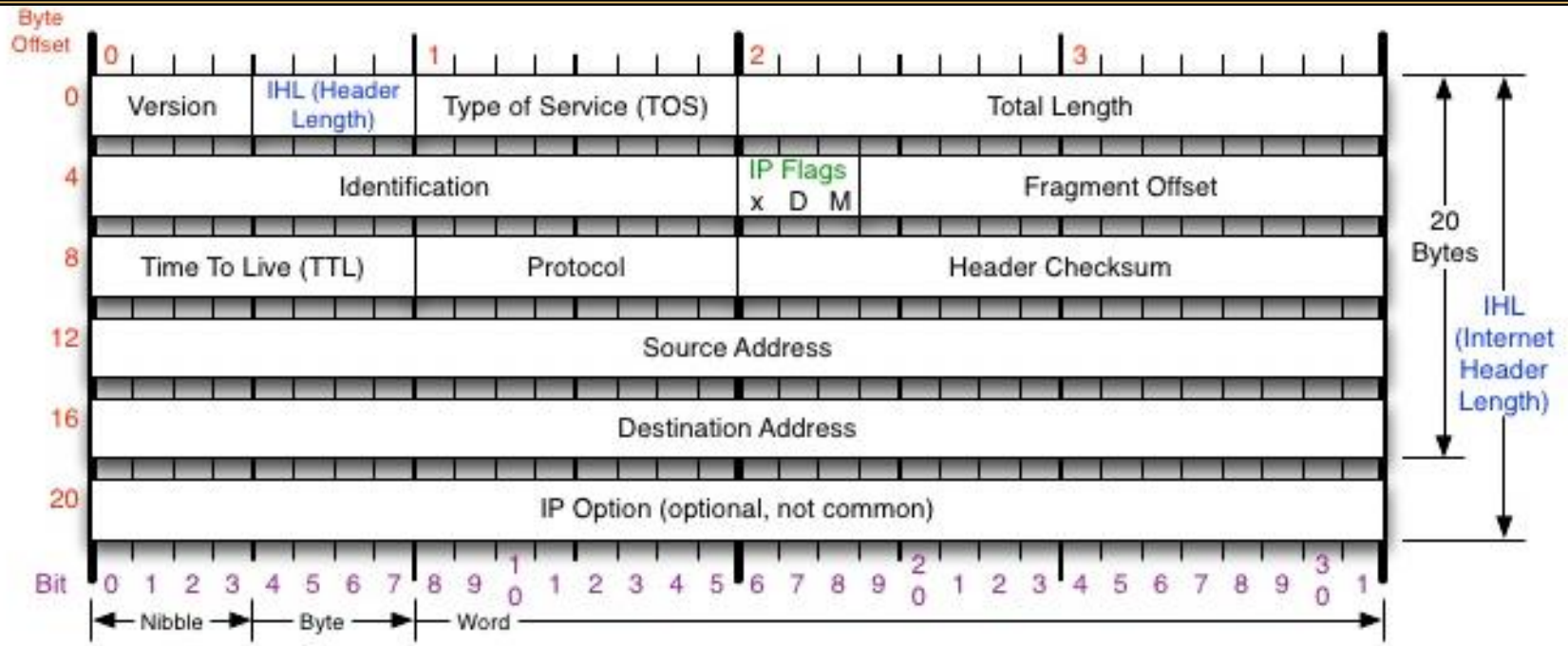
802.3 Ethernet packet and frame structure

Layer	Preamble	Start of frame delimiter	MAC destination	MAC source	802.1Q tag (optional)	Ethertype (Ethernet II) or length (IEEE 802.3)	Payload	Frame check sequence (32-bit CRC)	Interpacket gap
	7 octets	1 octet	6 octets	6 octets	(4 octets)	2 octets	46-1500 octets	4 octets	12 octets
Layer 2 Ethernet frame			← 64–1522 octets →						

INTERNET PROTOCOL

- IP is an addressing scheme for hosts on a network
- The address hides the underlying physical view by creating a virtual network view
- It also provides an unreliable, best-effort and connectionless packet delivery protocol
- Reliability and flow control are then provided by TCP
- The IP address consists of a 32-bit unsigned binary value
- It is usually expressed as a series of 4 byte integers separated by a decimal point: 192.168.17.23
- Each host needs to have a unique IP address throughout the whole network it wishes to communicate with
- Host textual names (such as um.edu.mt) are translated to an IP address using the DNS service (an application layer service)

IP HEADER



Version

Version of IP Protocol. 4 and 6 are valid. This diagram represents version 4 structure only.

Header Length

Number of 32-bit words in TCP header, minimum value of 5. Multiply by 4 to get byte count.

Protocol

IP Protocol ID. Including (but not limited to):

1 ICMP	17 UDP	57 SKIP
2 IGMP	47 GRE	88 EIGRP
6 TCP	50 ESP	89 OSPF
9 IGRP	51 AH	115 L2TP

Total Length

Total length of IP datagram, or IP fragment if fragmented. Measured in Bytes.

Fragment Offset

Fragment offset from start of IP datagram. Measured in 8 byte (2 words, 64 bits) increments. If IP datagram is fragmented, fragment size (Total Length) must be a multiple of 8 bytes.

Header Checksum

Checksum of entire IP header

IP Flags

x D M

x 0x80 reserved (evil bit)
D 0x40 Do Not Fragment
M 0x20 More Fragments follow

RFC 791

Please refer to RFC 791 for the complete Internet Protocol (IP) Specification.

IPV4 ADDRESSING

- The IP address is usually split up into two numbers: <network><host>
- This is done to allow finding the target host much faster
- The task of routing a packet to the appropriate network is done by a *router*
- Each IP datagram stores inside it the destination IP address in the header
- A network is defined as those hosts having the same network number and each host on the same network is connected with other using Layer 1 devices (i.e. devices that can only talk using Layer 1 language)
- Since all IP addresses need to be unique, then one needs to obtain and IP address (which are finite) to connect to the internet
- One usually buys a range of addresses within the same network
- Since networks tend to be of varying sizes, a classification of network number exits

CLASS-BASED IP ADDRESSES

- There are 5 classes of IP addresses
  - Class A: start with ‘0’, 7 bits network, 24 bits host
  - Class B: start with ‘10’, 14 bits network, 16 bits host
  - Class C: start with ‘110’, 21 bits network, 8 bits host
  - Class D: start with ‘1110’, used for multicasting
  - Class E: start with ‘11110’, reserved for future use
- The host based part of the IP address is then regulated by the systems administrator
- To calculate the number of networks or hosts allowed, one needs to subtract two from each number since the first and last are always reserved

RESERVED IP ADDRESSES

- Some IP addresses have special meaning and cannot be assigned
- A component of an IP address that has all its bits equal to 0 refers to ‘this’ network or host
  - In fact an IP address with all host bits set to zero is known as the *network address*
- A component of an IP address that has all its bits equal to 1 refers to all networks or hosts
  - An IP address with all host bits set to one is known as the *broadcast address*
- The address 127.0.0.0 is the loopback network

PUBLIC/PRIVATE IPS

- Public IP addresses are unique throughout all the networks
  - This will allow successful routing of datagrams from one to the other
- Private IP addresses are given to networks that do not need to crosstalk
  - Private IPs addresses are not unique
- A range of IP addresses are reserved, thus stopping routers from routing datagrams using such addresses:
  - 10.0.0.0 to 10.255.255.255 (Class A)
  - 172.16.0.0 to 172.16.255.255 (Class B)
  - 192.168.0.0 to 192.168.255.255 (Class C)


What's your address ?
173.168.15.10
No,your local address
127.0.0.1
I mean your physical address !
28:05:FF:58:31:05

IP SUBNETTING

- What happens when one has networks that do not correspond to the classes of IP address?
- One splits the host part into a subnet number and then a host number: <network><subnet><host>
- The subnet and host are transparent to external networks
  - A local host knowns about subnets
  - A foreign host does not know about the subnet and still sees subnet+host as one single host number
- The division into subnets is performed by the local administrator
- The routing is performed by a hierarchy of routers
- This division is identified through the use of a subnet mask

SUBNETTING METHODOLOGY

- Subnet addresses are also represented as /x, where x is number of bits borrowed for network+subnet:
  - Note that zeros represent the host part, ones represent the network part. So 255.255.255.0 is a Class C address
  - 255.255.255.255.0 can also be represented as /24
- Following table shows subnet borrowing Class C addresses (courtesy of Cisco)

Slash format	/25	/26	/27	/28	/29	/30	N/A	N/A
Mask	128	192	224	240	248	252	254	255
Bits borrowed	1	2	3	4	5	6	7	8
Value	128	64	32	16	8	4	2	1
Total Subnets		4	8	16	32	64		
Usable Subnets		2	6	14	30	62		
Total Hosts		64	32	16	8	4		
Usable Hosts		62	30	14	6	2		

SUBNETTING EXAMPLE

- Imagine acquiring the class C network address:
  - 193.188.34.0
- However, you need 4 networks each containing 20 PCs
- Thus, you can create the subnet borrowing 3 bits:
  - 255.255.255.224, or /27
- Now you have 6 usable networks, each able to hold 30 PCs
  - Network 1: 193.188.34.32, hosts 193.188.34.33-193.188.34.62
  - Network 2: 193.188.34.64, hosts 193.188.34.65-193.188.34.94
  - Network 3: 193.188.34.96, hosts 193.188.34.97-193.188.34.126
  - Network 4: 193.188.34.128, hosts 193.188.34.129-193.188.34.158
- and still have 2 unused networks and 10 unused host addresses for each of the first four networks
- Note how the first and last subnet address cannot be used and result in wastage of 30 hosts each

IP ROUTING

- IP needs to interconnect different networks and relay data between them, which is done through a router
- A router acts simultaneously as a normal host and a router
- A router has two or more physical network interfaces, thus is by default multi-homed. All hosts should be single-homed
- A router with *partial routing information* stores inside it information about the following destinations:
  - Hosts that are on the same network to which the router is physically connected
  - Hosts or networks about which explicit information has been provided
  - Hosts or networks about which the router has received explicit ICMP redirect plackets
  - Default route to any other destination
- All this information is stored inside the *routing table*

ROUTING TABLES

- Each host stores inside it the following mapping:
  - Destination IP network address
  - IP address of the router
- This information is called the IP routing table and is initialised at startup
- To view the routing table type `route` on Linux and `route print` on Windows
- There are three types of information in routing tables:
  - Direct routes reachable through one router's IP
  - Indirect routes reachable through one or more routers' IP
  - Default route when the above do not apply
- Thus all entries normally contain destination network and then an IP address or an interface to reach that network
- In addition, routing tables normally contain 127.0.0.1

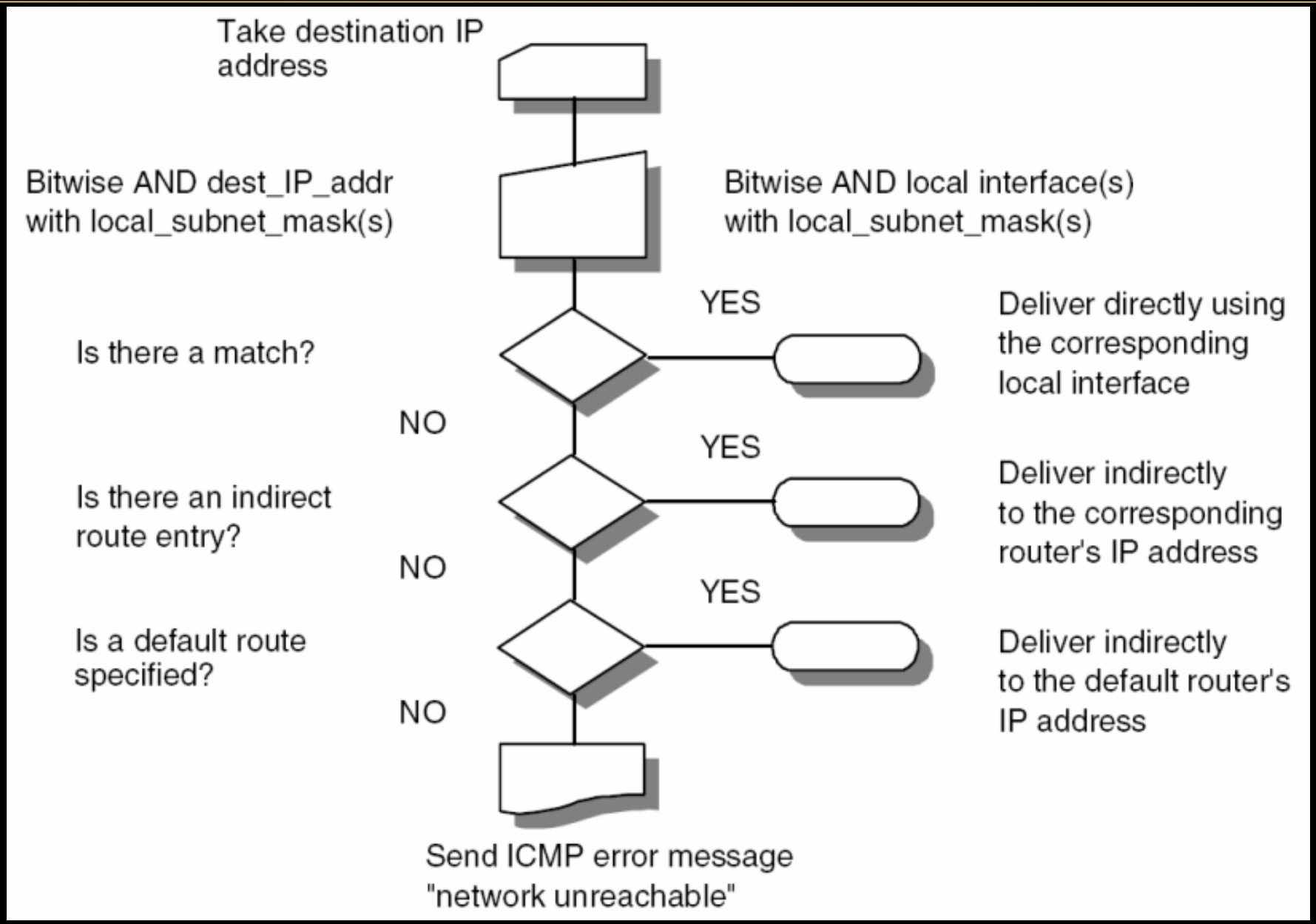
ROUTING ALGORITHM

- To allow a host to differentiate between destinations intended for the local network and those which are not the following is executed:
  - If destination IP network address is equal to host's network address
    - IP datagram is sent on local network
  - If not, IP datagram is sent to gateway corresponding to destination IP network address or the default gateway
- To allow subnets the following has to be done
  - If AND(destination IP address, subnet mask) equals AND(my IP address, subnet mask) then send to local network, otherwise send to corresponding gateway

ROUTING ALGORITHM

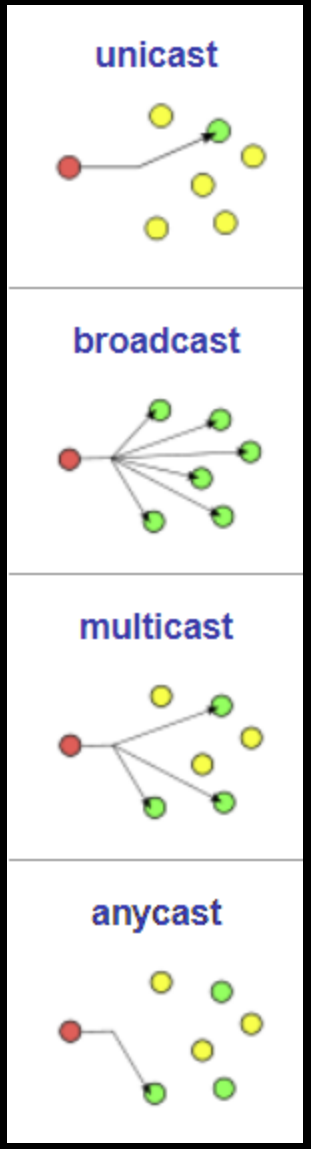
- This implies that each host needs to know about subnetting, otherwise that host will be unable to communicate with hosts on different subnets but on the same network
- When a destination is on the same network the destination IP is the same as the destination host's IP address and the physical address is that of the destination host
- When a destination is on another network, the destination IP is STILL the same as the destination host's IP address, yet the physical address is that of the router
- The algorithm in the next slide is the same for routers as for hosts, the only difference is that for routers, this algorithm is performed for each interface
- Routers are also able to update their routing table using Routing Protocols

ROUTING ALGORITHM



METHODS OF DELIVERY

- A datagram can be delivered in one of four ways (since it is connectionless)
- Unicast: directed to a single destination [one-to-one]
- Broadcast: directed to all hosts on a network or subnet/s [one-to-many]
- Multicasting: Hosts are grouped using the same class D IP address [one-to-many-of-many or many-to-many-of-many]
- Anycasting: Hosts are given same address and the first host to received it will for a connection [one-to-one-of-many]



OTHER IP-RELATED TOPICS

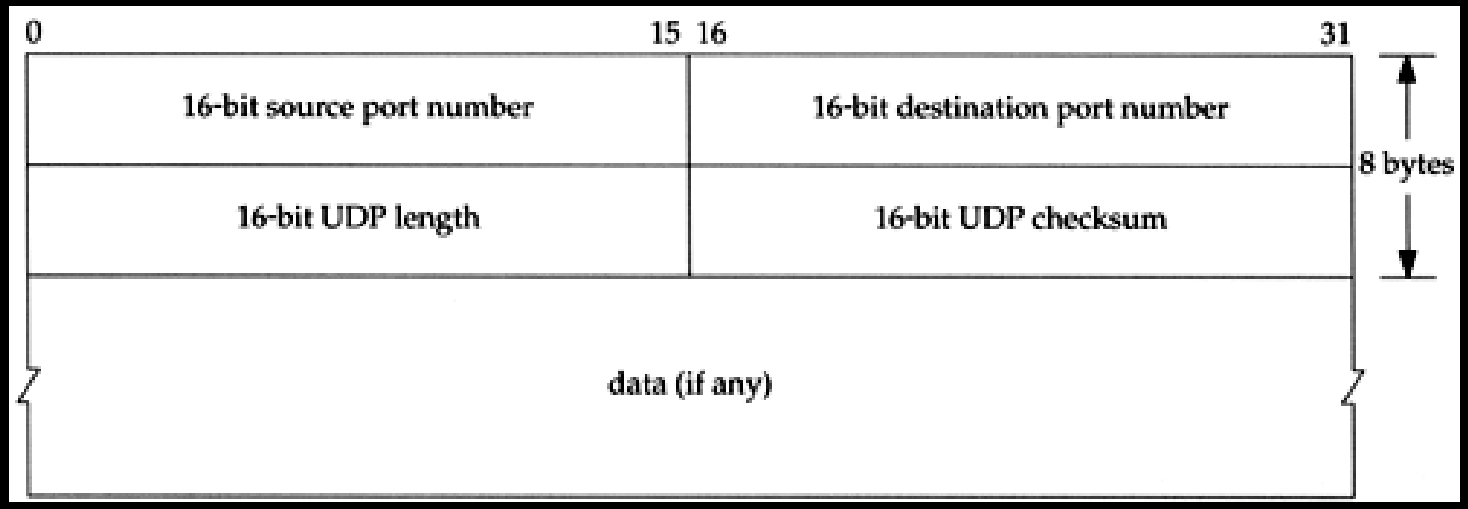
- The interested reader may want to have a look at:
  - The IP exhaustion problem
  - CIDR (Classless Inter-Doman Routing)
  - IPv6
  - ICMP, IGMP, ARP, RARP
  - IGP Routing protocols (example RIP, OSPF)
  - EGP Routing protocols (example BGP)

TRANSPORT LAYER

- For a connection on a host (single IP address), there exist many entry points through which there may be many-to-many connections. These are called *ports*
- A port is a 16-bit unsigned number used by the host-to-host protocol to identify to which higher level protocol or application process it must deliver the incoming messages
- Internet ports 1-1023 are considered *well-known* (for example, 80 for HTTP, 20/21 for FTP, 23 for telnet)
- When using TCP (a connection-based protocol), a client will make a connection to a server
  - A connection is established when a connection tuple is established on each side (called a *socket tuple)*
  - ***<protocol, local-addr, local-port, foreign-addr, foreign-port>***

USER DATAGRAM PROTOCOL

- Simply provides multiplexing/de-multiplexing capabilities on top of IP (introduces ports on top of IP)



- Length is length of the whole packet including header
- Checksum is over pseudo-IP header, UDP header and data
- UDP is used by TFTP, DNS, RPC, SNMP and LDAP

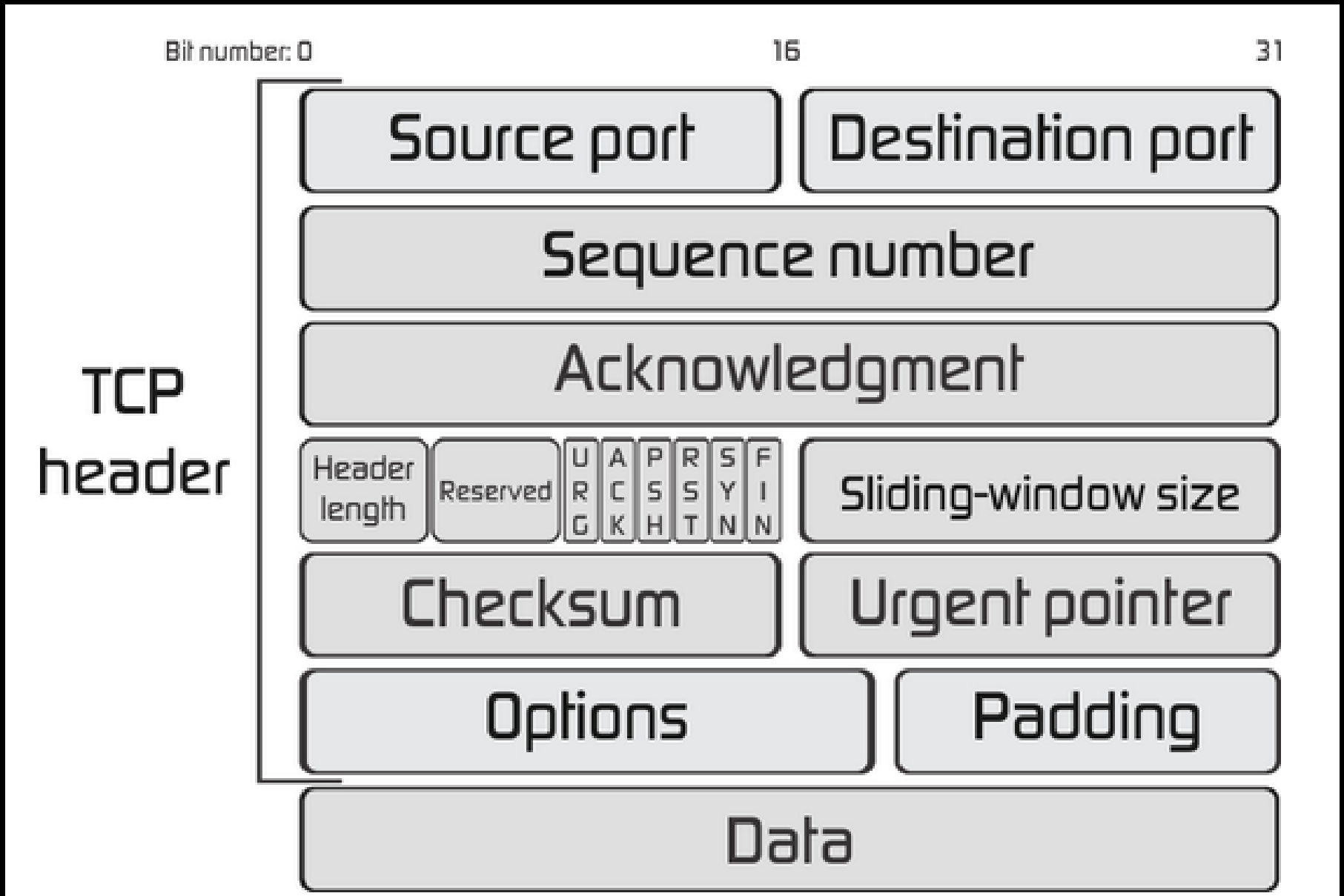
TRANSMISSION CONTROL PROTOCOL

- Stream Data Transfer
  - Application sees a stream of bytes
  - TCP groups the data into packets and vice-versa
- Reliability
  - A sequence number to each byte is transmitted to the receiver and sender expects ACK packet for it
    - Only sequence number of first byte is sent, since a segment will be received entirely
  - Receiver will use sequence number to re-order packets if needed

TRANSMISSION CONTROL PROTOCOL

- Flow control
  - When sending back ACK, receiver will also indicate remaining buffer size
- Multiplexing
- Logical connections
  - A socket tuple is established before data transfer
- Full duplex
  - Bi-directional concurrent data transfers

TCP SEGMENT


Bit number: 0
16
31
TCP header
Source port
Destination port
Sequence number
Acknowledgment
Header length
Reserved
URG
ACK
PSH
RST
SYN
FIN
Sliding-window size
Checksum
Urgent pointer
Options
Padding
Data

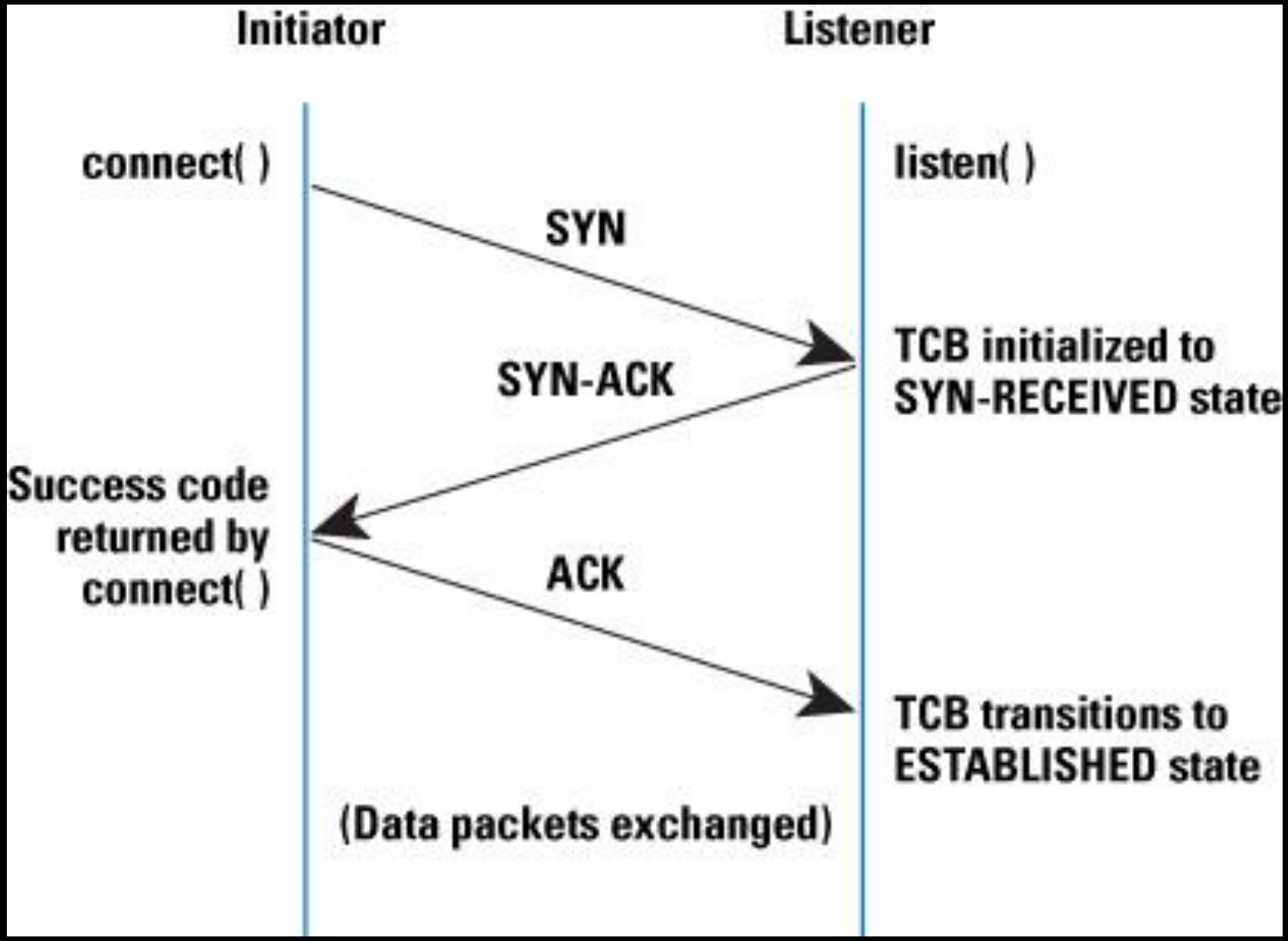
TCP SEGMENT

- Sequence number: of first data byte in this segment, unless SYN is set where first data byte is n+1
- ACK number: if ACK is set, number of next sequence number receiver is expecting (note: ACK piggy-back)
- Window: In ACL segments, number of bytes sender of packet is willing to accept beyond ACK number
- Checksum: Over pseudo IP header, TCP header and TCP data
- Urgent Pointer: Used for urgent data
- Options: Several that are rarely used apart from *window scale*

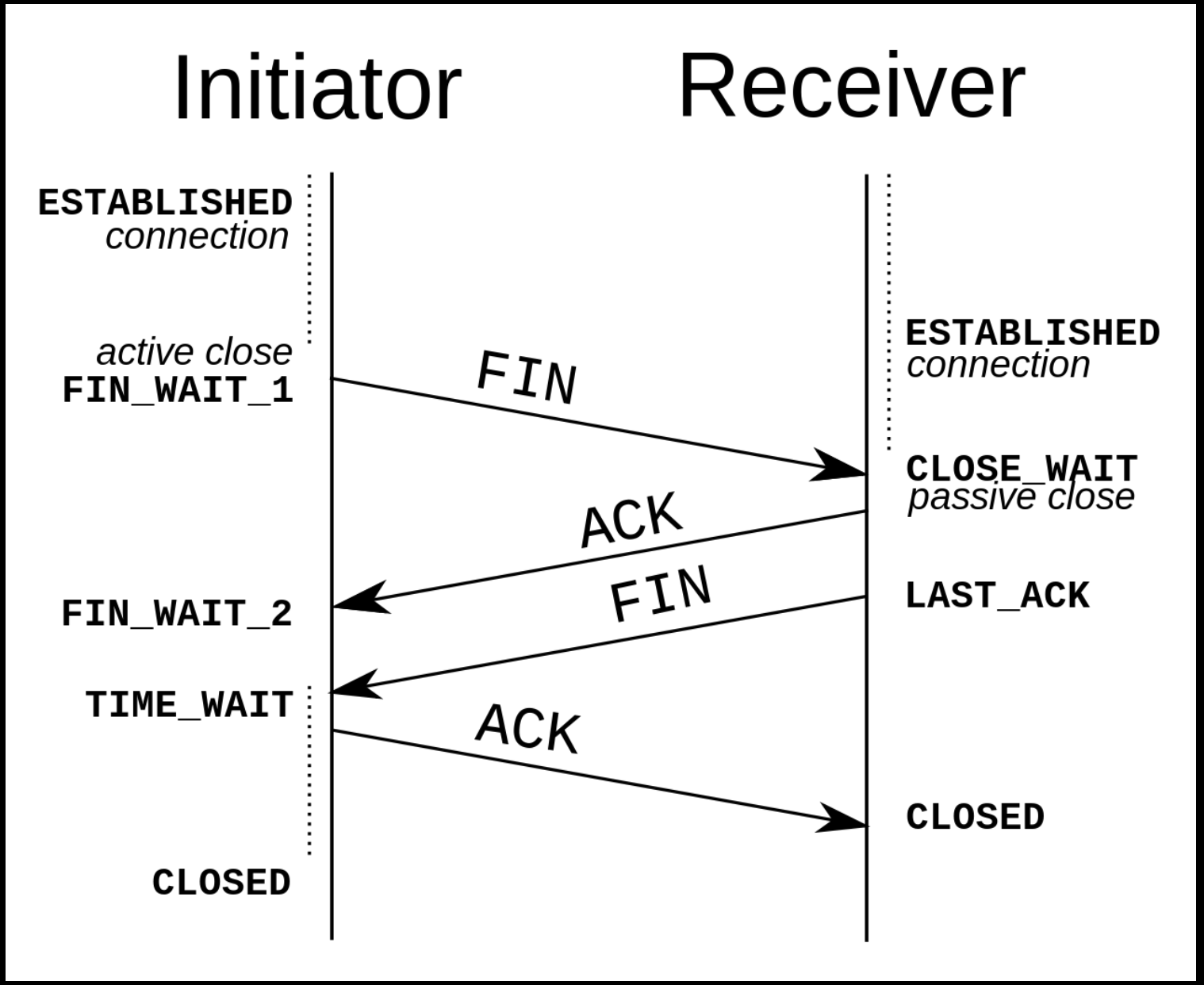
TCP SEGMENT

- Fields:
  - URG: urgent pointer is valid
  - ACK: ACK number is valid
  - PSH: Push function (used to transmit data before a whole segment is finished)
  - RST: Resets connection
  - SYN: Synchronize the sequence numbers
  - FIN: No more data from sender

THREE WAY HANDSHAKE (CONNECT)



FOUR WAY HANDSHAKE (CLOSE)



WINDOWING PRINCIPLE

- Basic Reliability Protocol:
  - Send data packet, expect ACK for packet, send next data packet
  - Expensive in terms of bandwidth
- Better reliability protocol
  - Send all packets within Window (settings timeout)
  - Slide windows for every ACK'd packet
  - Receiver will send sequence ACK of last well-received packet for each packet received

WINDOWING PRINCIPLE

- Provides:
  - Data reliability
  - Better throughput
  - Flow control (receiver can delay ACK)
- In TCP:
  - Sequence numbers are at the byte level and one sequence number per TCP segment
  - Window size is in term of bytes also
  - Windows size is transmitted at connection initiation
  - Each ACK will also contain the amount of data the receiver is ready to deal with

TCP WINDOWING