

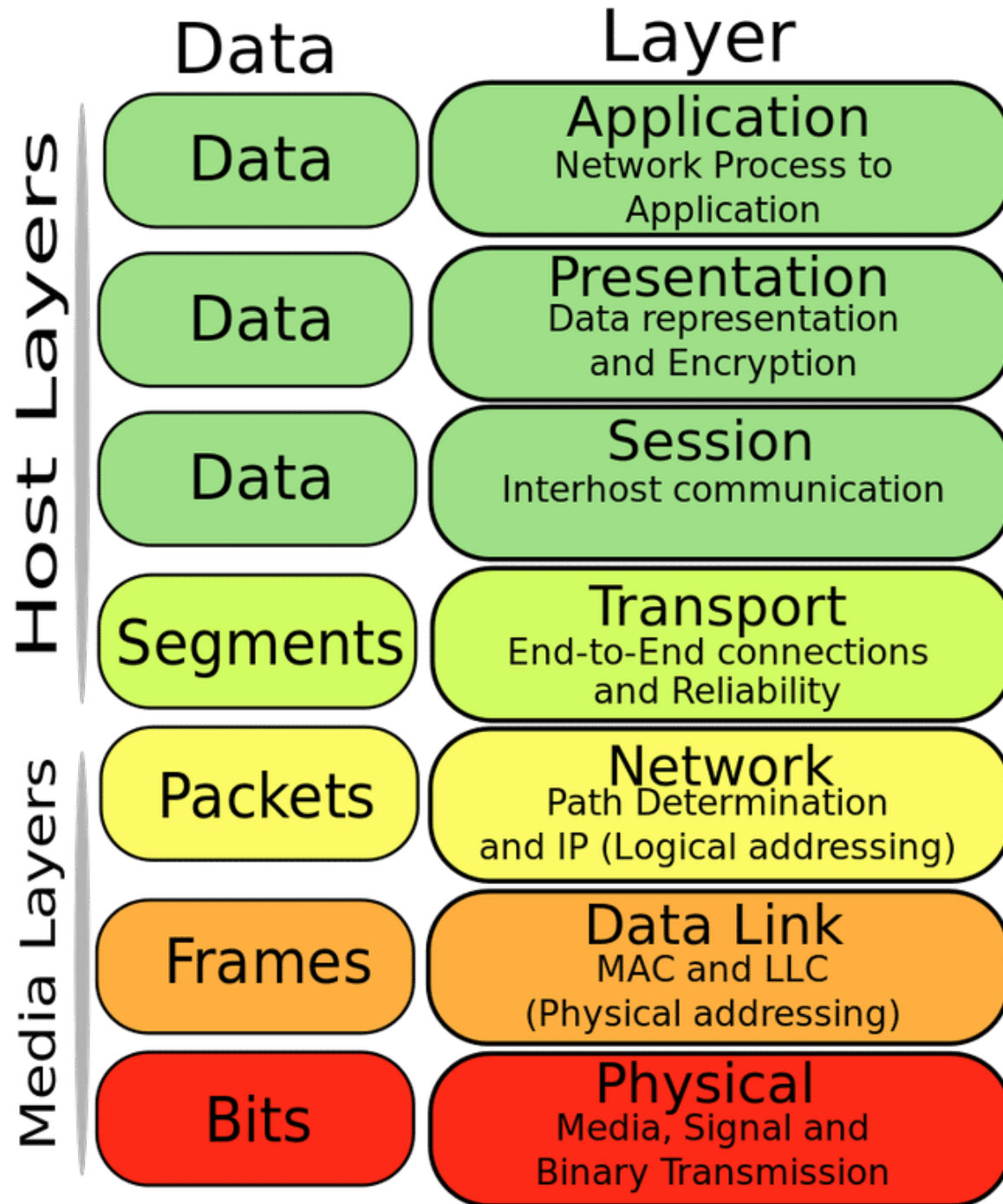
Unix/IP – Network Overview



Layers

- Complex problems can be solved using the common divide and conquer principle. In this case the internals of the Internet are divided into separate layers.
 - Makes it easier to understand
 - Developments in one layer need not require changes in another layer
 - Easy formation (and quick testing of conformation to) standards
- Two main models of layers are used:
 - OSI (Open Systems Interconnection)
 - TCP/IP

OSI Model



OSI

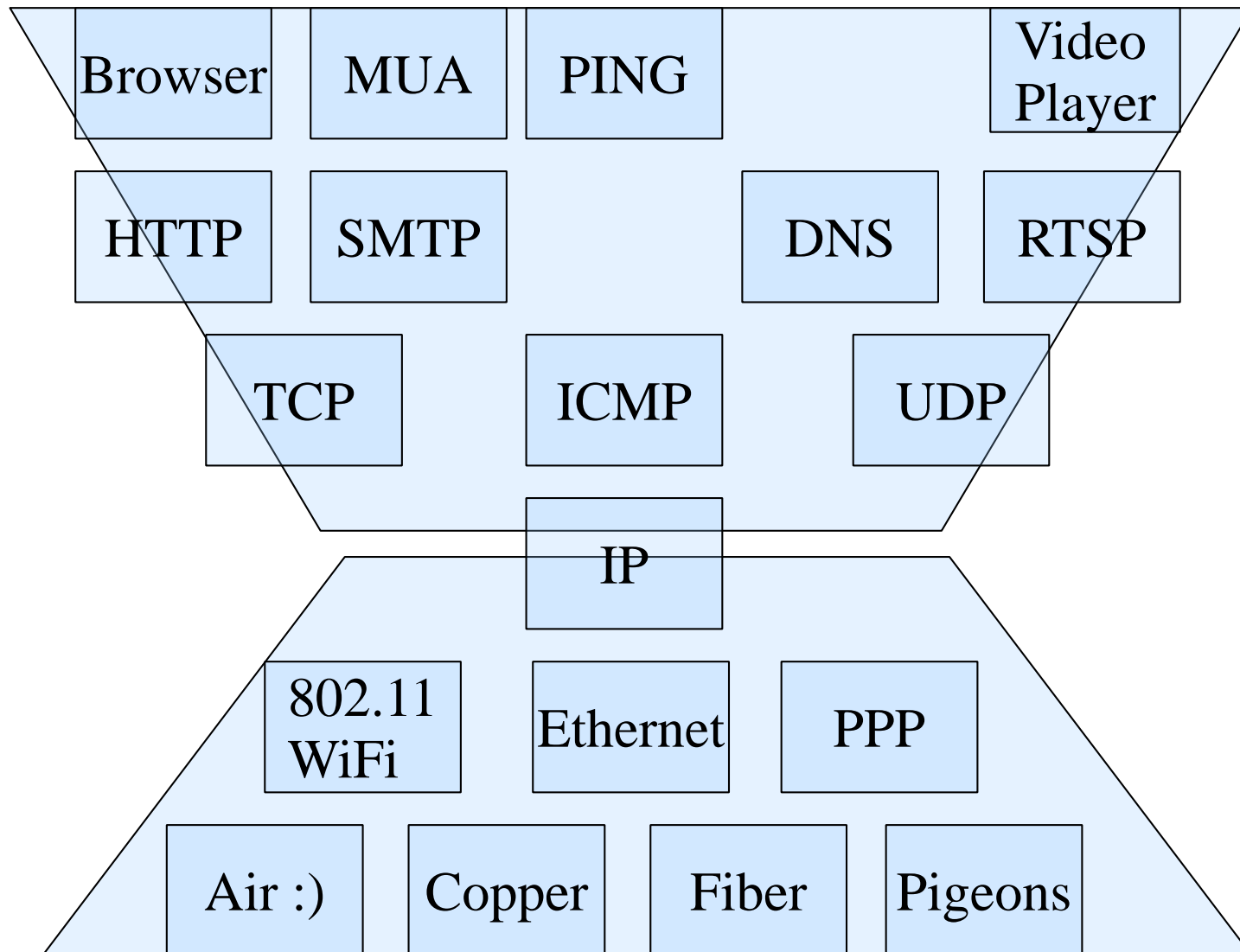
- Conceptual model composed of seven layers, developed by the International Organization for Standardization (ISO) in 1984.
- **Layer 7** – Application (servers and clients etc web browsers, httpd)
- **Layer 6** – Presentation (file formats e.g pdf, ASCII, jpeg etc)
- **Layer 5** – Session (conversation initialisation, termination,)
- **Layer 4** – Transport (inter host comm – error correction, QOS)
- **Layer 3** – Network (routing – path determination, IP[x] addresses etc)
- **Layer 2** – Data link (switching – media acces, MAC addresses etc)
- **Layer 1** – Physical (signalling – representation of binary digits)

Acronym: All People Seem To Need Data Processing

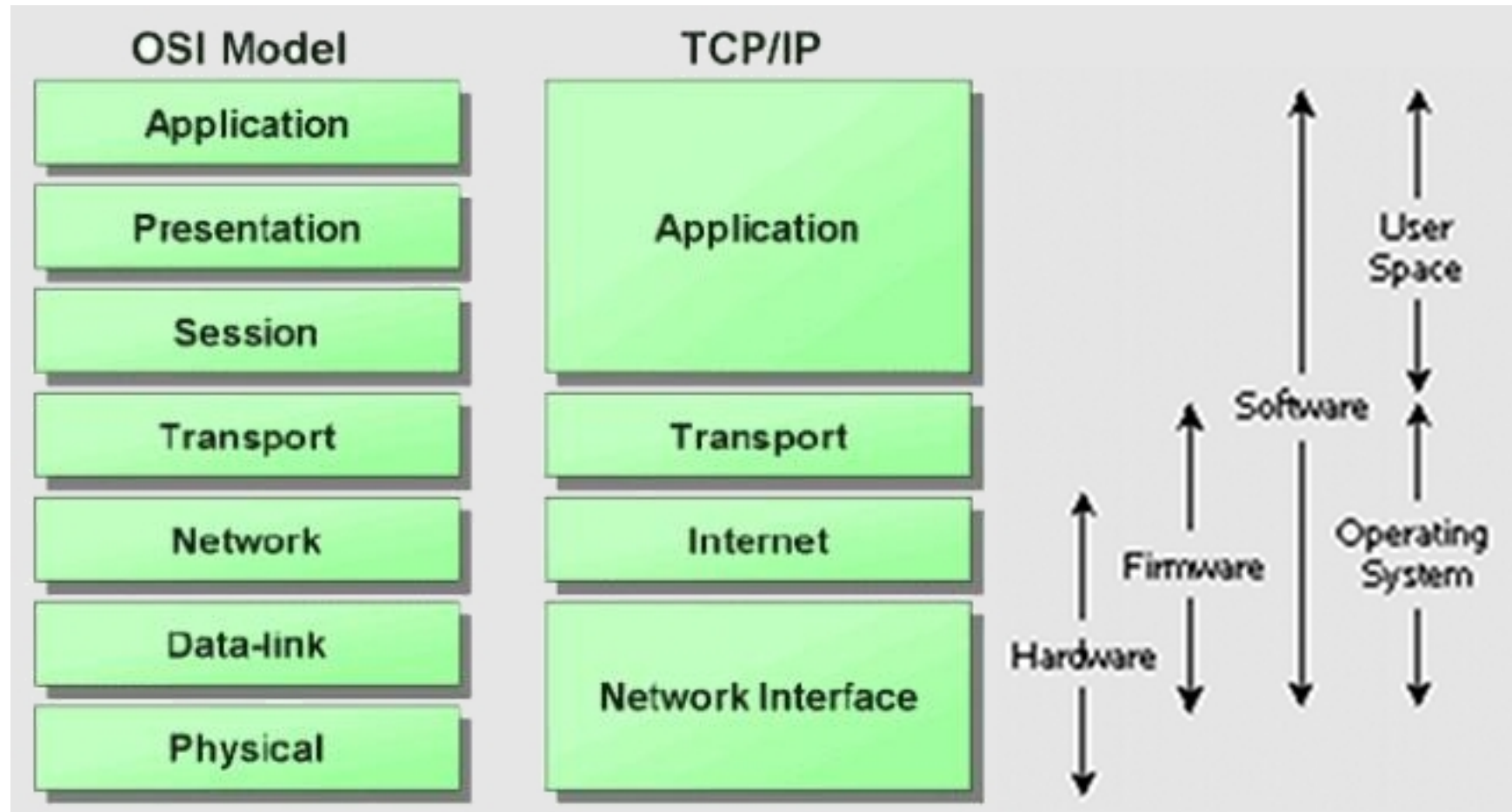
TCP/IP

- Generally, TCP/IP (Transmission Control Protocol/Internet Protocol) is described using three to five functional layers. We have chosen the common DoD reference model, which is also known as the Internet reference model.
 - Process/Application Layer consists of applications and processes that use the network.
 - Host-to-host transport layer provides end-to-end data delivery services.
 - Internetwork layer defines the datagram and handles the routing of data.
 - Network access layer consists of routines for accessing physical networks.

TCP/IP model – the “hourglass”



OSI and TCP/IP



Encapsulation & Decapsulation

- Lower layers add headers (and sometimes trailers) to upper layers packets

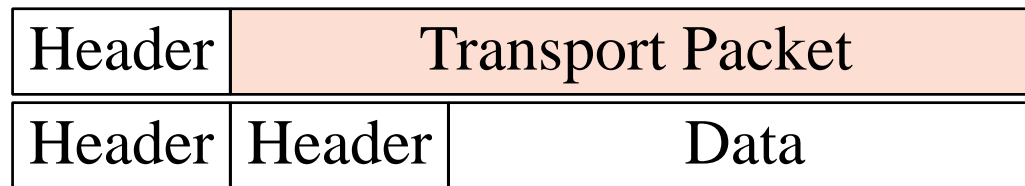
Application



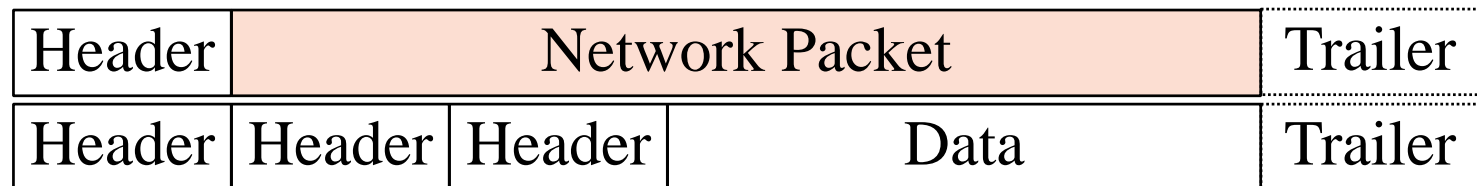
Transport



Network



Data Link



Frame, Datagram, Segment, Packet

- Different names for packets at different layers
 - Ethernet (link layer) frame
 - IP (network layer) datagram
 - TCP (transport layer) segment
- Terminology is not strictly followed
 - we often just use the term “packet” at any layer

Summary

- Networking is a problem approached in layers.
 - OSI Layers
 - TCP/IP Layers
- Each layer adds headers to the packet of the previous layer as the data leaves the machine (encapsulation) and the reverse occurs on the receiving host (decapsulation)

More to the structure

- Hierarchical Division in IP Address:
- Network Part (Prefix)
- describes which network
- Host Part (Host Address)
- describes which host on that network

205	.	154	.	8		1
11001101		10011010		00001000		00000001
Network					Mask	Host

- Boundary can be anywhere
- used to be a multiple of 8 (/8, /16/, /24), but not usual today

Network Masks

- **Network Masks** help define which bits are used to describe the **Network Part** and which for **hosts**
- Different Representations:
 - decimal dot notation: 255.255.224.0 (128+64+32 in byte 3)
 - binary: 11111111 11111111 111 00000 00000000
 - hexadecimal: 0xFFFFE000
 - number of network bits: /19 (8 + 8 + 3)
- Binary AND of 32 bit IP address with 32 bit **netmask** yields network part of address

Sample Netmasks

- 137.158.128.0/**17** (netmask **255.255.128.0**)

1111 1111	1111 1111	1	000 0000	0000 0000
1000 1001	1001 1110	1	000 0000	0000 0000

- 198.134.0.0/**16** (netmask **255.255.0.0**)

1111 1111	1111 1111		0000 0000	0000 0000
1100 0110	1000 0110		0000 0000	0000 0000

- 205.37.193.128/**26** (netmask **255.255.255.192**)

1111 1111	1111 1111	1111 1111	11	00 0000
1100 1101	0010 0101	1100 0001	10	00 0000

Allocating IP addresses

- The subnet mask is used to define size of a network
- E.g a subnet mask of 255.255.255.0 or /24 implies $32-24=8$ host bits
 - 2^8 minus 2 = 254 possible hosts
- Similarly a subnet mask of 255.255.255.224 or /27 implies $32-27=5$ host bits
 - 2^5 minus 2 = 30 possible hosts

Special IP Addresses

- All 0's in host part: Represents Network
- e.g. 193.0.0.0/24
- e.g. 138.37.128.0/17
- e.g. 192.168.2.128/25 (WHY ?)
- All 1's in host part: **Broadcast** (all hosts on net)
- e.g. 137.156.255.255 (137.156.0.0/16)
- e.g. 134.132.100.255 (134.132.100.0/24)
- e.g. 192.168.2.127/25 (192.168.2.0/25) (WHY ?)
- 127.0.0.0/8: **Loopback** address (127.0.0.1)
- 0.0.0.0: Various special purposes (DHCP, etc.)

Numbering Rules

- Private IP address ranges (RFC 1918)
 - 10/8 (10.0.0.0 – 10.255.255.255)
 - 192.168/16 (192.168.0.0 – 192.168.255.255)
 - 172.16/12 (172.16.0.0 – 172.31.255.255)
- Public Address space available from AfriNIC
- Choose a small block from whatever range you have, and subnet your networks (to avoid problems with broadcasts, and implement segmentation policies – DMZ, internal, etc...)

Network related settings

- Files

- `/etc/rc.conf`
- `/etc/netstart`
- `/etc/hosts`
- `/etc/resolv.conf`

-

- Commands

- `ifconfig eth0 196.200.218.x/24`
- `route add default 192.200.218.254`
- `hostname bcIP.ws.afnog.org`

Routing

- Every host on the internet needs a way to get packets to other hosts outside its local network.
- This requires special hosts called **routers** that can move packets between networks.
- Packets may pass through many routers before they reach their destinations.

Questions

?