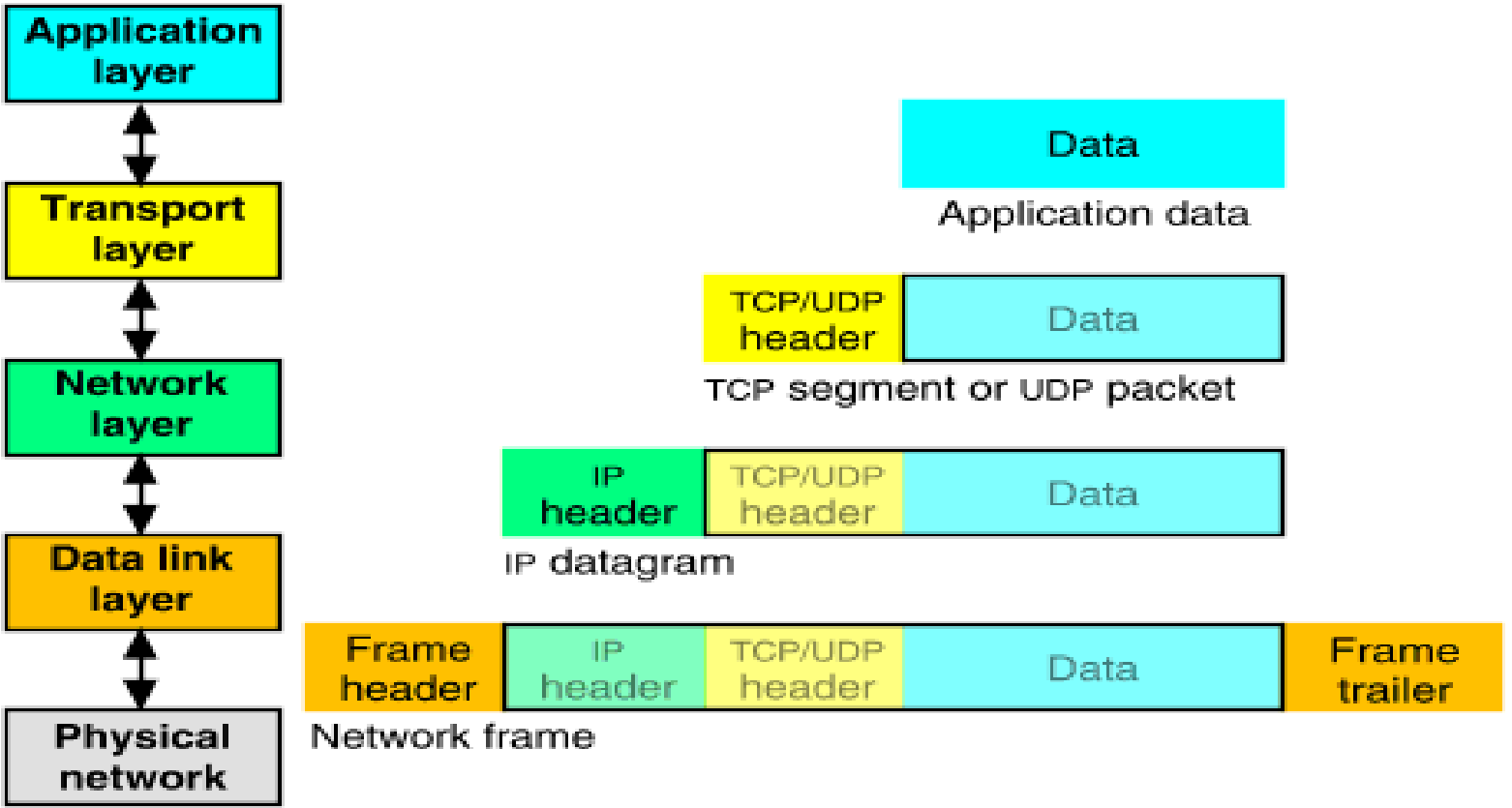
Raw Sockets

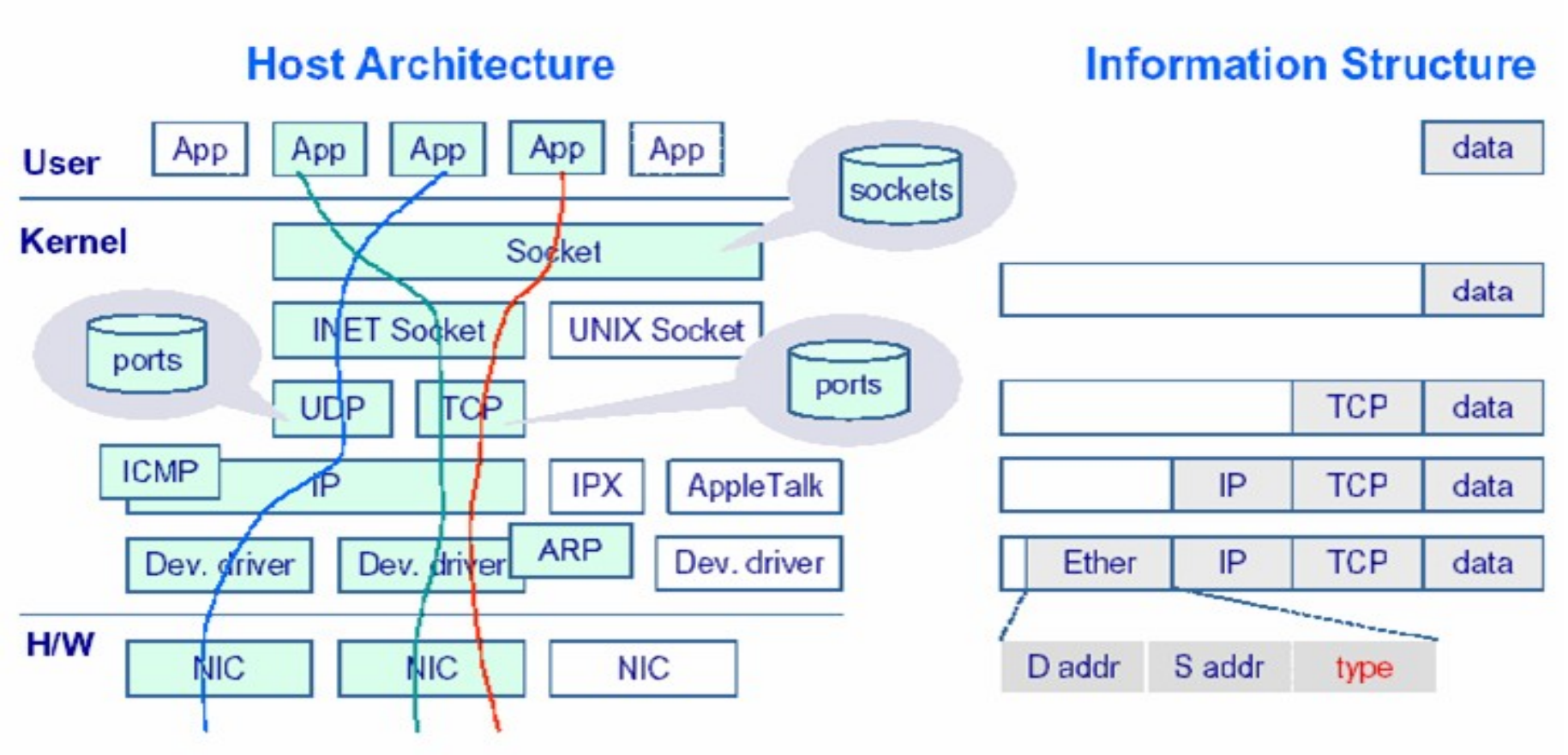
giorgio.richelli@uniroma1.it

Network Packet Encapsulation



giorgio.richelli@uniroma1.it

Path & Headers



Standard Sockets

- Can only receive frames sent to:
  - A specific address
  - Broadcast
  - Multicast

- Headers (Ethernet, IP, TCP, etc) are stripped by the network stack.
- Packet headers cannot be modified before send.

Advanced Functions

- Promiscuous mode
  - receive all frames in broadcast domain

- Raw Sockets:
  - Receive complete packets, including headers
  - Inject packets with custom headers and data into the network

Promiscuous Mode

- It is the “See All, Hear All” mode
- Tells the network driver to accept all packets irrespective of whom the packets are addressed to.
- Used for Network Monitoring (both legal and illegal)
- We can do this by:
  - programmatically setting the IFF_PROMISC flag
  - using the ifconfig utility (ifconfig <iface> promisc)

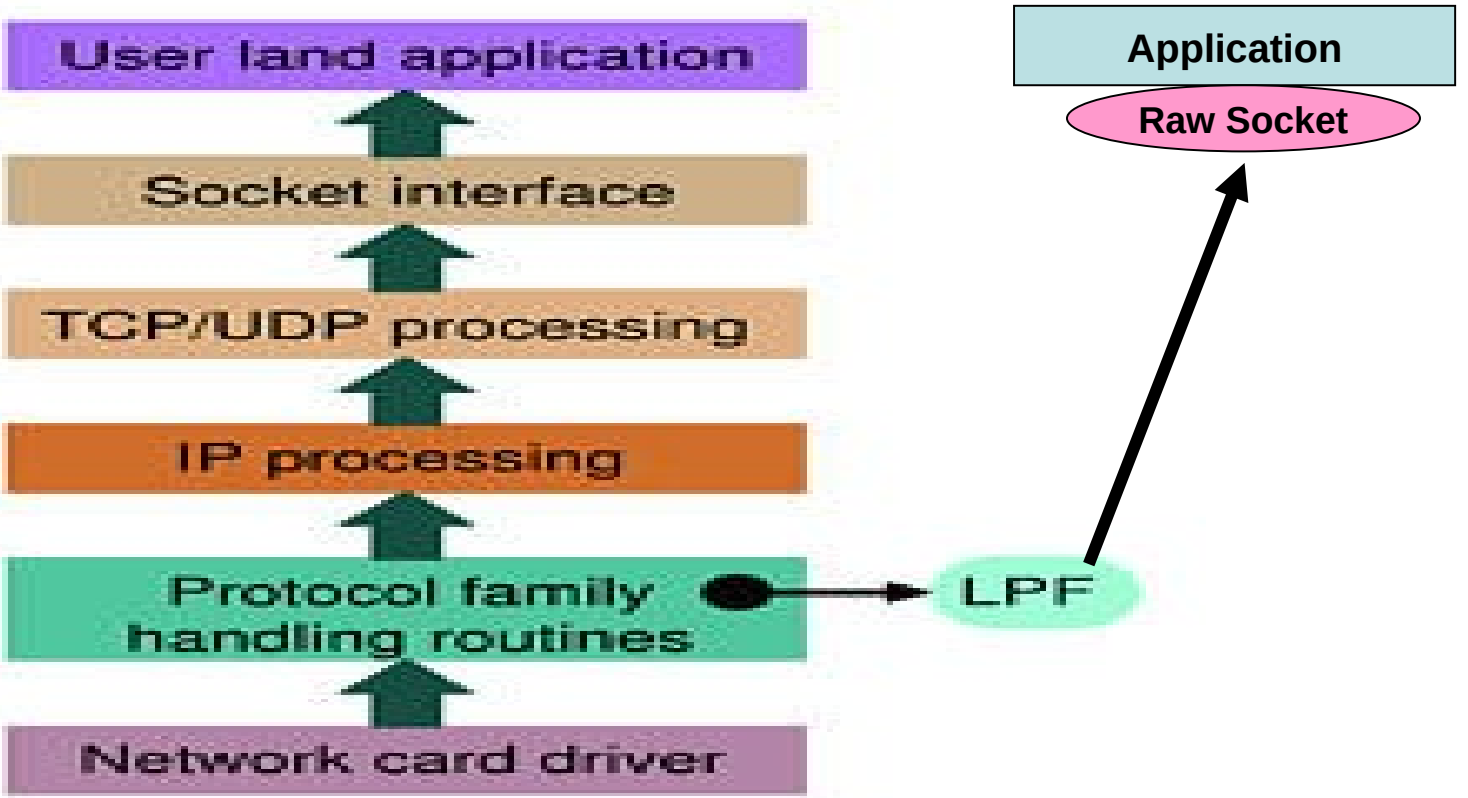
Getting all headers - Sniffing

- Once set the interface to promiscous mode, it gets “full packets” with all the headers.
- We can process these packets and extract data from it.
- Note we are receiving packets meant for other (all) hosts

Packet Injection

- We “manufacture” our own packets and send it out on the network.
- Total bypass of network stack
- Most active network monitoring tools and hacking tools use this
  - DOS attacks
  - Syn Floods
  - IP Spoofs

Raw Sockets



giorgio.richelli@uniroma1.it

PF_PACKET

- It is a software interface to send/receive packets at layer 2 of the OSI (i.e. device driver)
- All packets received will be complete with all headers and data.
- All packets sent will be transmitted without modification by the kernel to the medium.
- Supports filtering using Berkley Packet Filters.

giorgio.richelli@uniroma1.it

Creating a Raw Socket

- Call socket() with appropriate arguments.

  Socket(PF_PACKET, SOCK_RAW, int protocol)

  Protocol is:
  - ETH_P_IP to capture IP packets
  - ETH_P_ALL to get all information

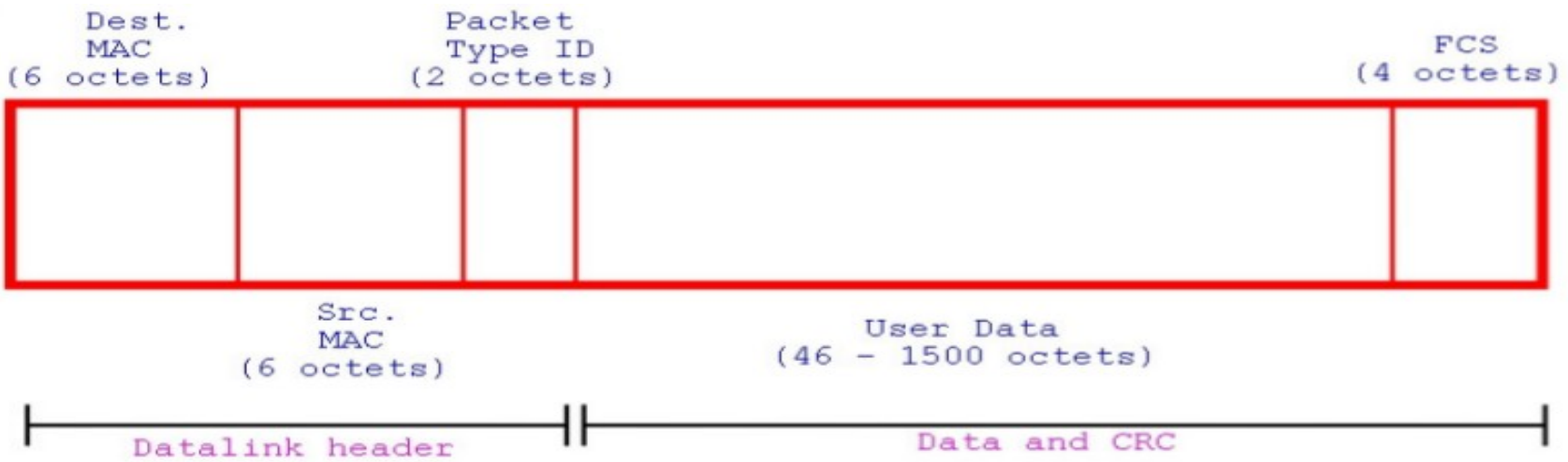
Sniffer HowTo

- Create raw socket – `socket()`
- Set interface you want to sniff on in promiscuous mode.
- Bind Raw socket to this interface – `bind()`
- Receive packets on the socket – `recvfrom()`
- Process received packets
- `close()` the raw socket.

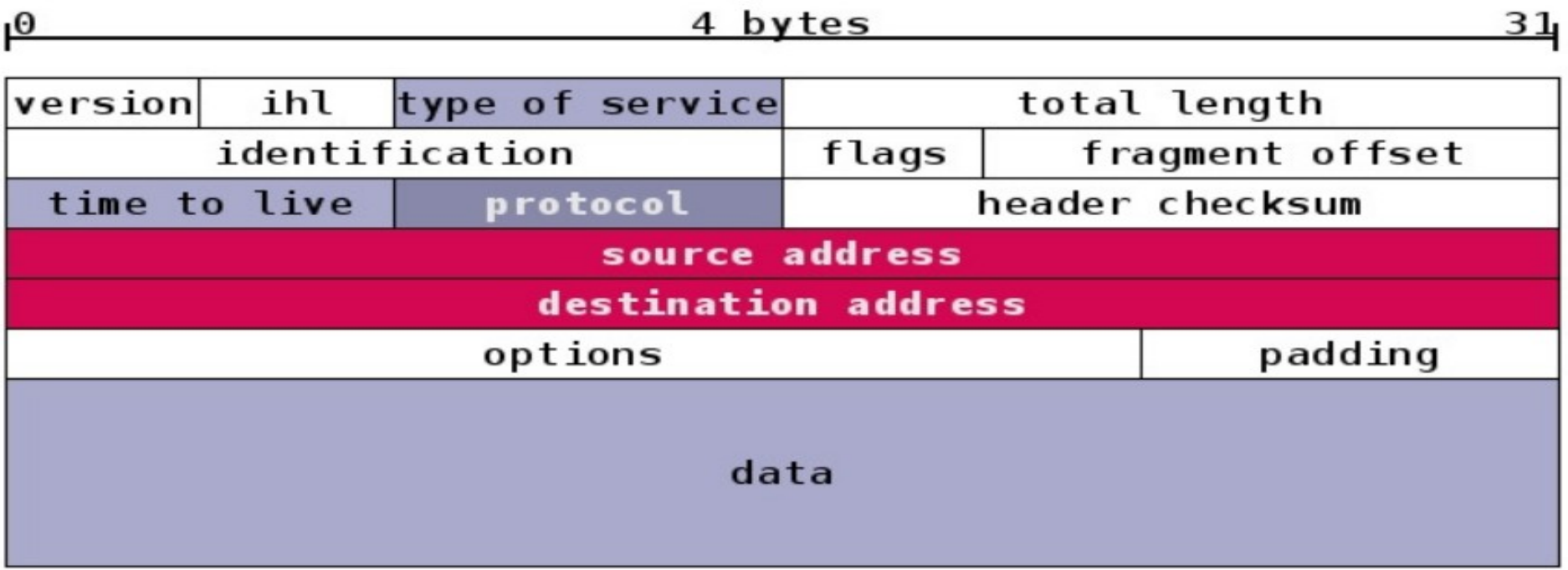
Packet Inject HowTo

- Create a raw socket – `socket()`
- Bind socket to the interface you want to send packets onto – `bind()`
- Create a packet
- Send the packet – `sendto()`
- Close the raw socket – `close()`

Ethernet Frame



IP Frame


0
4 bytes
31
version
ihl
type of service
total length
identification
flags
fragment offset
time to live
protocol
header checksum
source address
destination address
options
padding
data

IP Protocols

Maintained by IANA:

Internet Assigned Number Authority

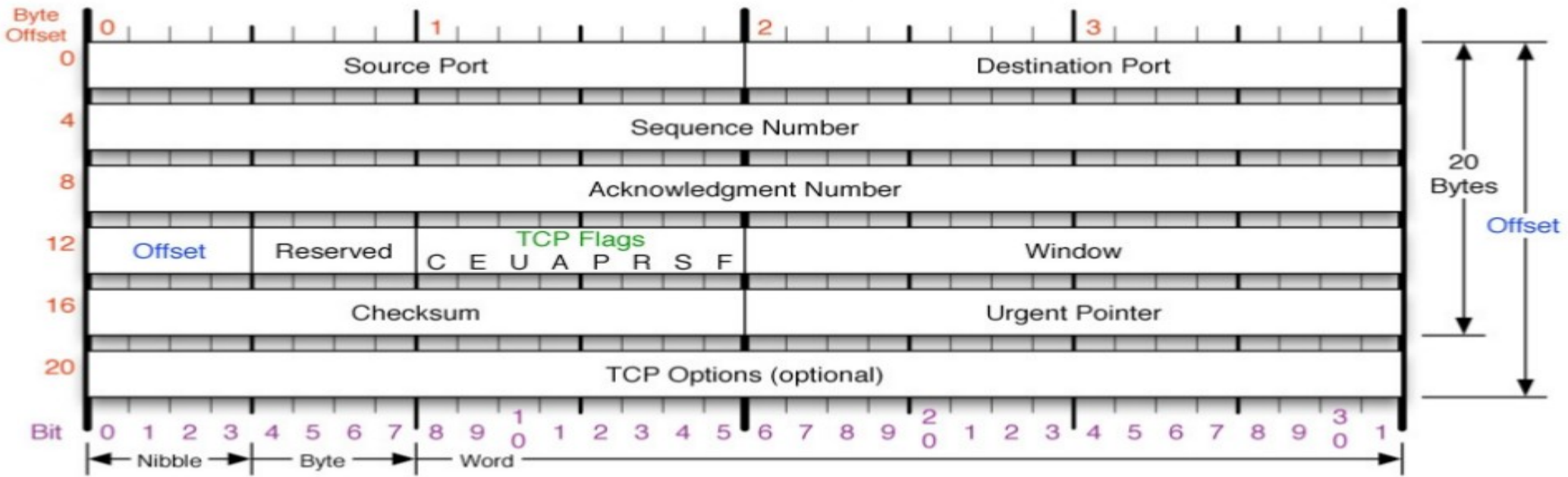
Responsible for coordinating some of the key elements that keep the Internet running:

- Domain names
- Number Resources (IP and AS pools)
- Protocol Assignement

See `/etc/protocols`

UDP Frame

TCP Frame



giorgio.richelli@uniroma1.it