# TCP/IP MODEL

| | | | | |
|---|---|---|---|---|
| 5 | Application | HTTP, SMTP etc... | Messages | — |
| 4 | Transport | TCP/UDP | Segment | Ports |
| 3 | Network | IP | Datagram | IP address |
| 2 | Datalink | Ethernet, Wifi | Frames | MAC address |
| 1 | Physical | 10baseT, 802.11 | Bits | — |

INTERNET ACCES LAYER / INTERFACE LAYER

## PHYSICAL LAYER

Represent the physical devices that interconnect computers
Cabling, connectors, adapters, devices...

## DATALINK LAYER

Responsible for defining a common way of interpreting these signals so network devices can communicate

## NETWORK LAYER

Allows different networks to communicate with each other through devices known as routers

## TRANSPORT LAYER

Sorts of which client and server programs are supposed to get data

## APPLICATION LAYER

Location Layer. Contents of the package itself

# OSI MODEL

| | | |
|---|---|---|
| 7 | Application | Provides different services to the application |
| 6 | Presentation | Converts the information |
| 5 | Session | Handles problems which are not communication issues |
| 4 | Transport | Provides end to end communication control |
| 3 | Network | Routes the information in the network |
| 2 | Datalink | Provides Error Control |
| 1 | Physical | Connects to entity to the trasmission media |

## Application

⊕ File transfer, access and management (FTAM) — FTAM
⊕ Virtual Terminal (VT) — VT
⊕ Electronic Mail and Messaging Handling (MHS) — MHS
⊕ Directory Services (DS) — DS
⊕ Common management information protocol (CMIP) — CMIP

## Presentation

⊕ Responsible for the format of the data transferred during the communications. SYNTAX and SEMANTICS

**Syntax** AND **Semantics**

Rules of grammar in sentence structure

That words are ordered to form sentence

grammar rules

refers to the meaning of a sentences

gramatically correct ordering of words

meaning rules

## Session

Permits to parties to hold ongoing communications called a session across a network

Provide one-or-two way communication (Dialge control)

## Transport

⊕ Accept data from session layer
⊕ Split the data up into smaller units
⊕ Pass the the network layer
⊕ Ensure that the bits delivered or not
⊕ Controls without modification, loss or duplication packets

## Network

Controls the operation of a subnet, routing, congestion control accounting.

HOW PACKETS ARE ROUTED FROM SOURCE TO DESTINATION

## DataLink

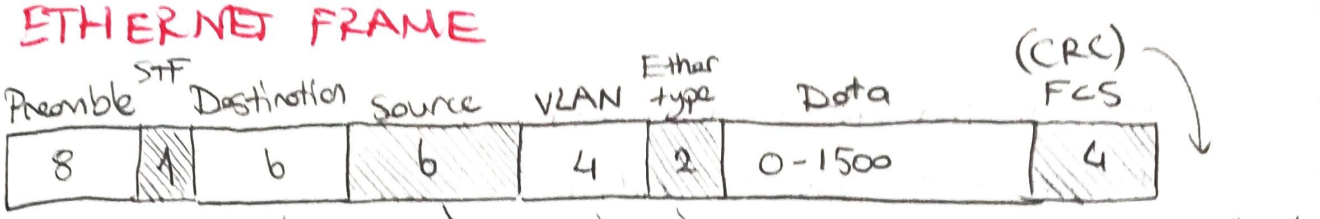
Take a raw transmission
Transforms it into a line
Ethernet, Token Ring and ARCNet (LAN datalink)
Point to Point (PPP) Serial Line Internet Protocol (SLIP)
Encrypts — Deencrypts

## Physical

Transmitting raw bits over a communication channel "1" and "0"

Mechanical, Electrical, Functional and procedural interface

# ETHERNET FRAME



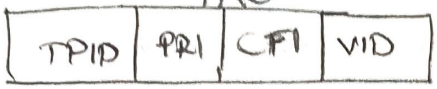

Mathematic calculation

Preamble
10101010....

STF (Start Frame Delimeter)
1111....

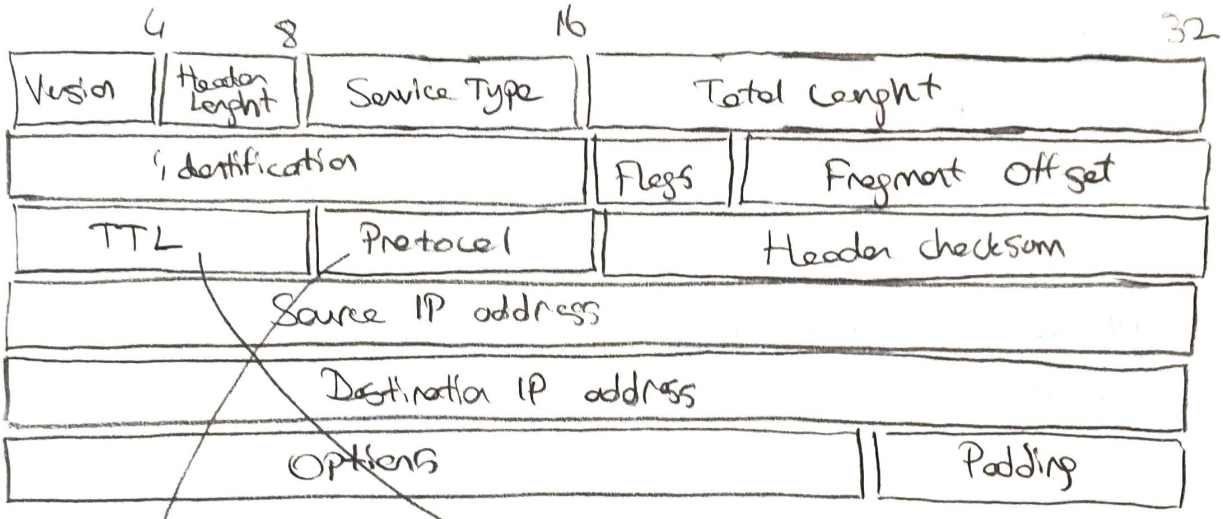
Destination and Source MAC address

Describe VLAN TAG



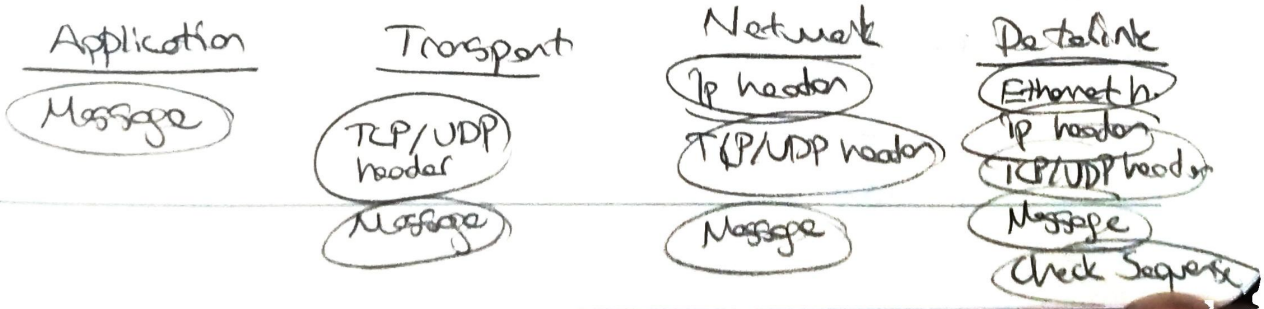

Describes the protocol of the frame
Upper protocol
0x0800 - ipV4
0x0806 - ARP
0x86DD - ipV6

# IP DATAGRAM HEADER




Protocol shows upper layer protocols
TCP 6
UDP 17
KMP 1

Shows how much router passed and how many will pass



# ROUTING

Interior

## Routing Information Protocol (RIP)

Distance Vector routing protocols which employs hop count as a routing metric

## Enhanced Interior Gateway Routing Protocol (EIGRP)

Advanced distance vector routing protocols

Determines the value of the path with: bandwidht, load, delay, reliability and MTU.

## Open Shortest Path First (OSPF)

Link-state routing algorithm.

It computes the shortest-path tree with Dijkstra algorithm and detects the changes in the topology.

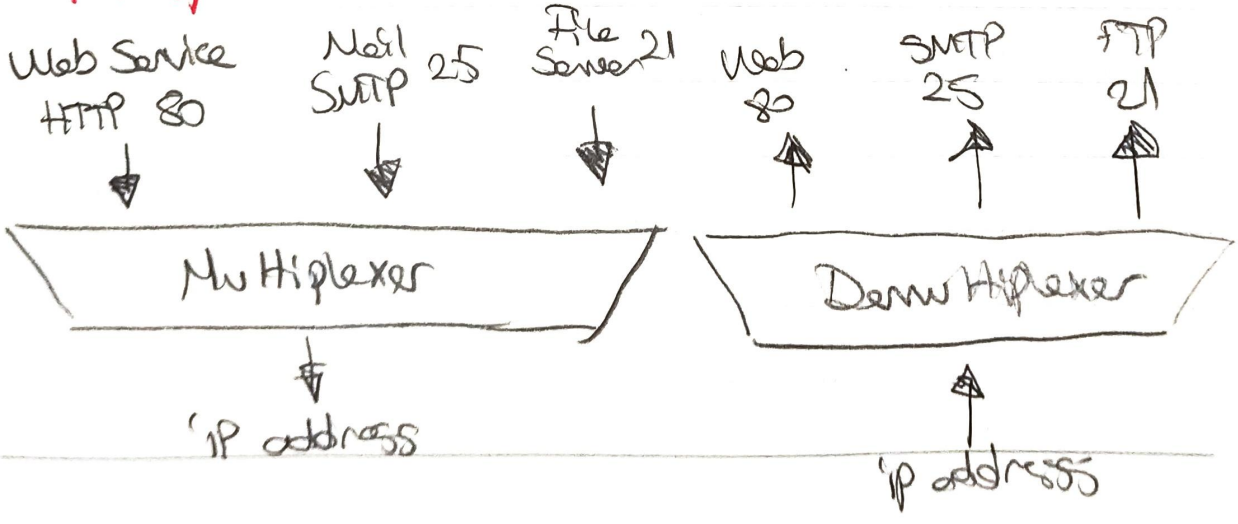
Exterior

## Border Gateway Protocol (BGP)

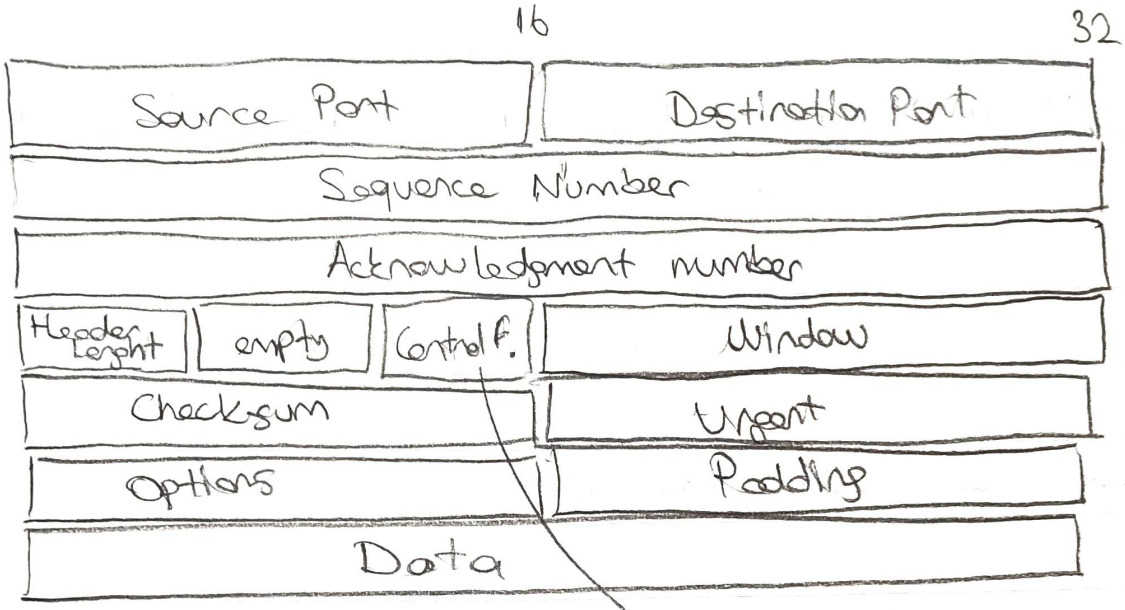
Exterior gateway protocol designed to exchange routing and reachability information. Path-vector routing protocol. It makes decision based on paths, network policies or rule sets configured by network administrator.

# TRANSPORT LAYER

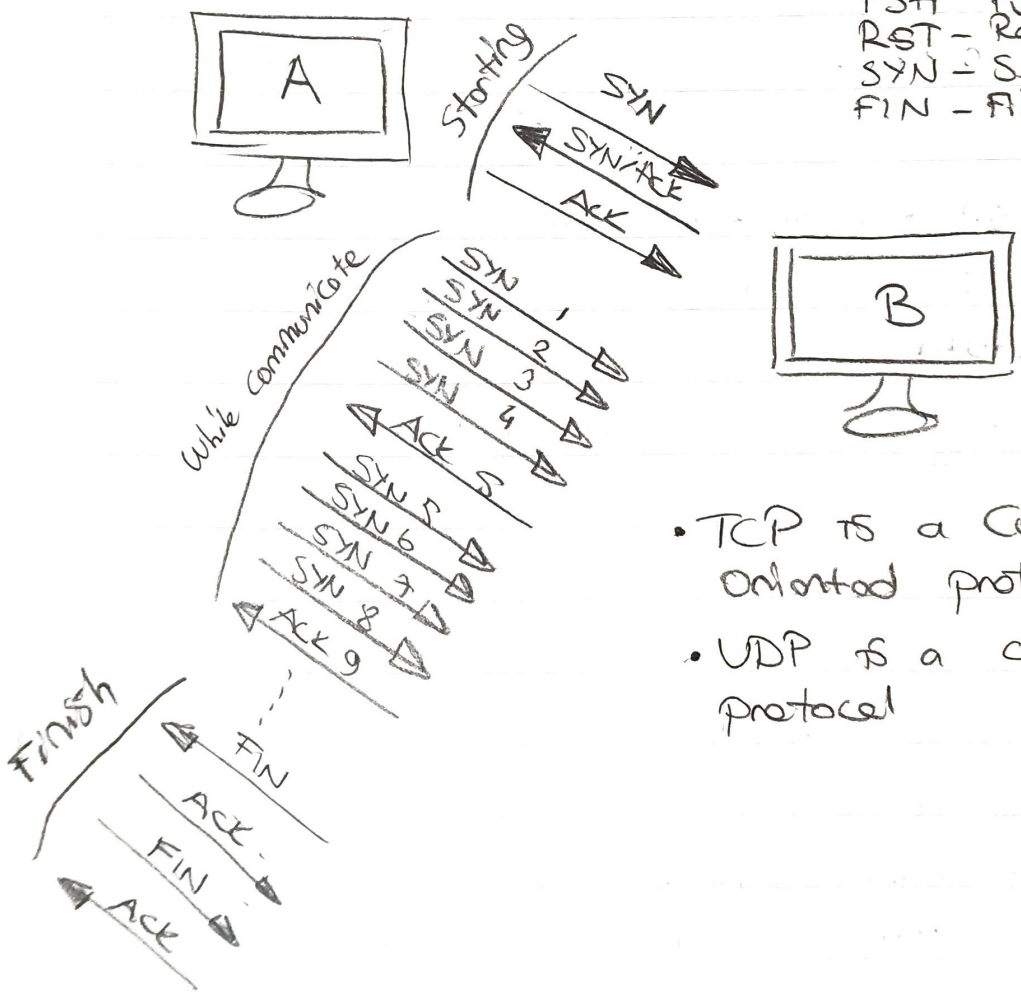
## Multiplexer



# TCP HEADER

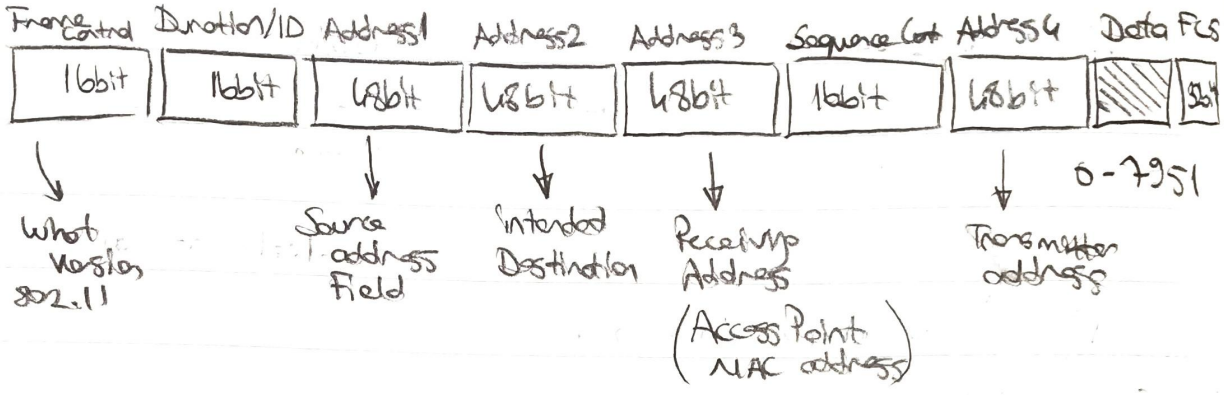


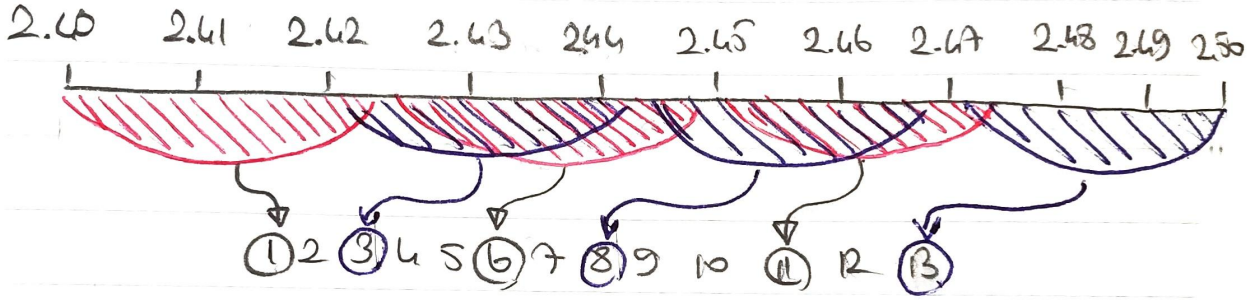

URG - Urgent
ACK - Acknowledgment
PSH - Push
RST - Reset
SYN - Synchronize
FIN - Finish




- TCP is a Connection Oriented protocol
- UDP is a connectionless protocol

## 802.11 HEADER



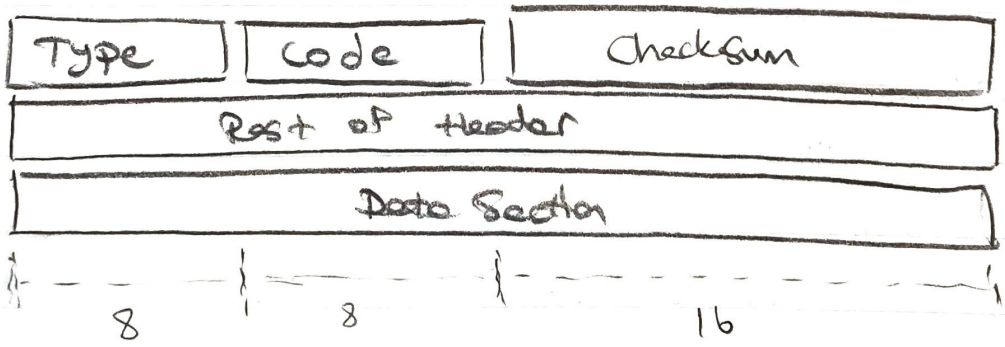




- 1 channel 2.44 GHz

Wifi Security

WEP → WPA → WPA2 → WPA3

## ICMP HEADER




- Ping ⇒ Echo Request → Echo Reply (if device is here)
- if TTL = 0 ICMP sends TimeExceed message

Traceroute — Windows Tracert
Traceroute — UNIX MAC OS Traceroute (UDP)

• Testing Port connectivity

| Linux / MACOS | Windows |
| --- | --- |
| nc (network connectivity) command (Netcat) | Test-NetConnection command |
| nc google.com 80 | Test-NetConnection -ComputerName google.com -Port 80 |
| nc -z -v google.com 80 | |

• Digging DNS

nslookup command (shows DNS records)

Public DNS Servers → 4.2.2.1
4.2.2.2
4.2.2.3
4.2.2.4
4.2.2.5
4.2.2.6

IPV6 HEADER