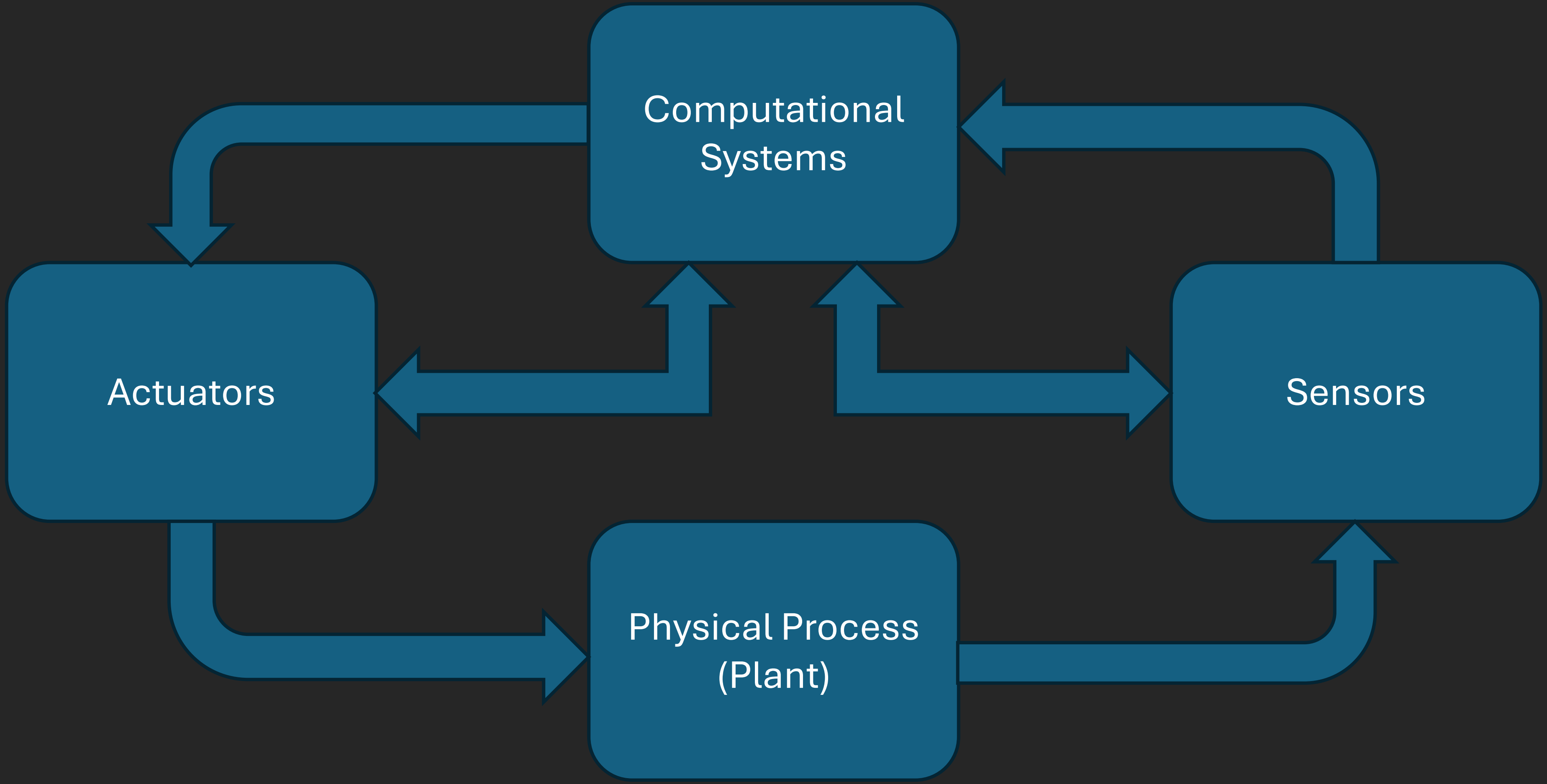
Cyber-Physical Systems

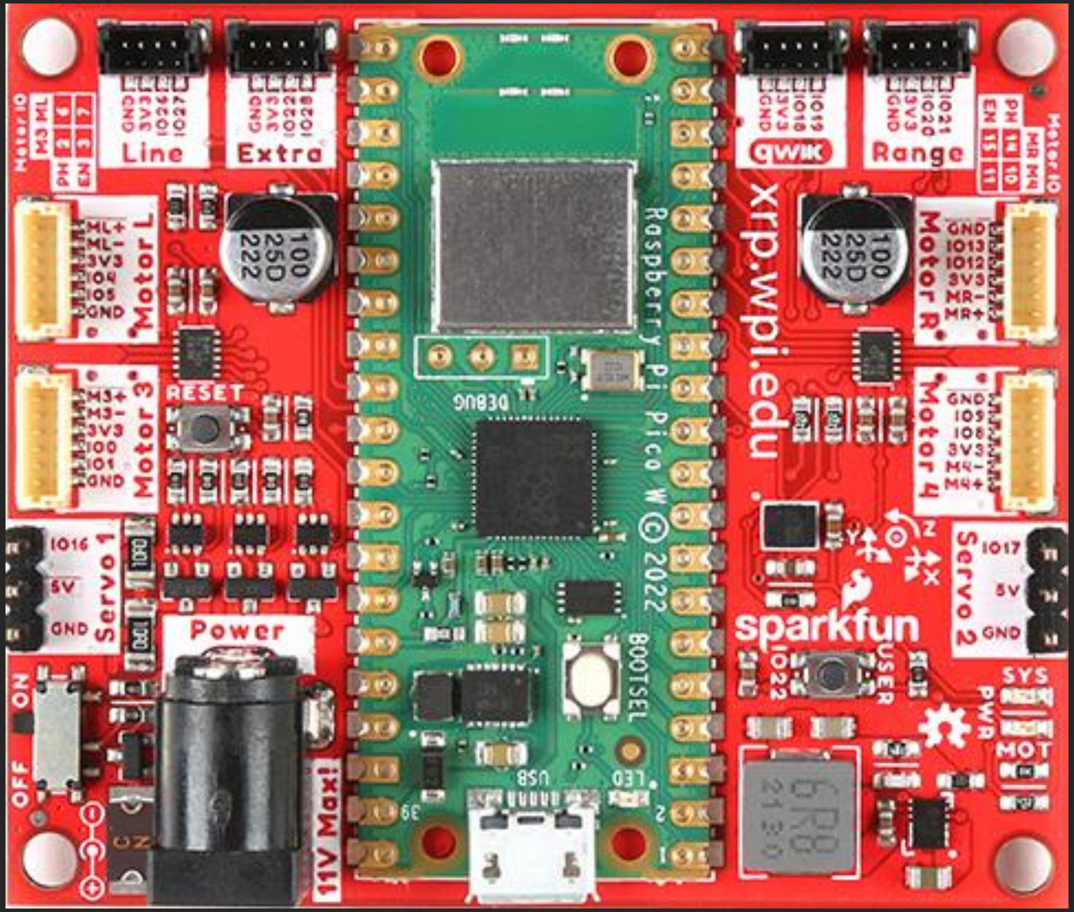
Dr. Jonathan Jaramillo

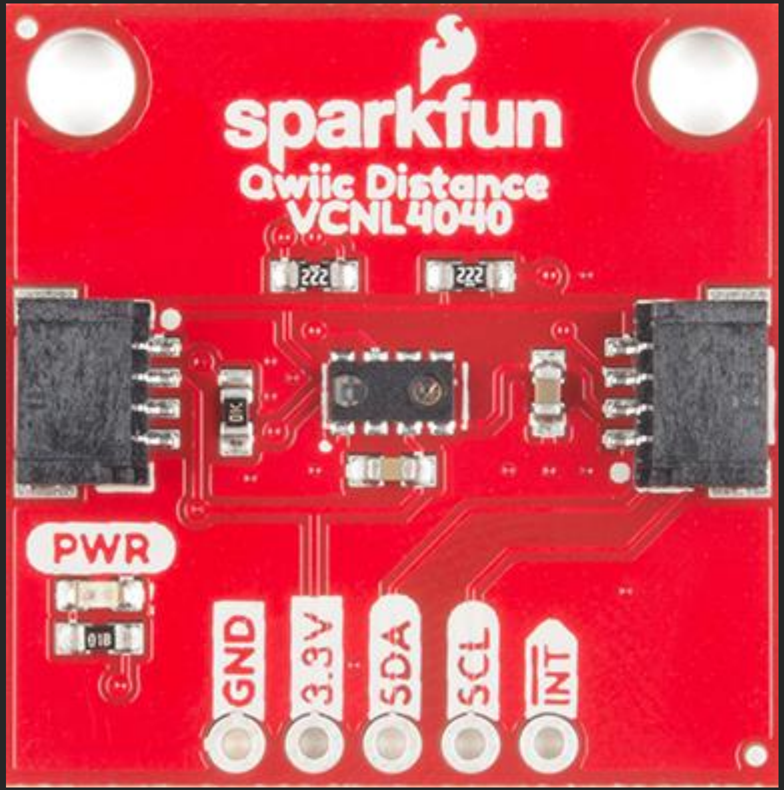
Communication Systems

What are Cyber-Physical Systems?



Wired Communication


Line
Extra
qwiic
Range
Motor L
Motor 3
Motor R
Motor 4
RESET
Raspberry Pi Pico W © 2022
xrp.wpi.edu
Servo 1
Servo 2
Power
sparkfun
BOOTSEL
USER
11V Max!
ON
OFF
SYS
PWR
MOT


sparkfun
Qwiic Distance
VCNL4040
PWR
GND
3.3V
SDA
SCL
INT

Fundamentals of Wired Communication

- Signal Transmission – Analog vs Digital and Modulation
- Synchronous vs Asynchronous
- Duplexing – Half-duplex vs Full-duplex
- Topology – Bus, single master vs multi-master
- Addressing – Static vs Dynamic addressing
- Electrical Characteristics – Pullup and pulldown resistors
- Framing and Data Packets
- Protocol layering and abstraction

Analog Vs Digital

- Analog Signals - Continuous signals that represent information using a **continuous range of values**. They vary smoothly over time and can take on any value within a given range.
  - Examples: audio signals, temperature readings.
- Digital Signals - Discrete signals that represent information using **binary values (0 and 1)**. They change in distinct steps or levels and are commonly used in computers and digital devices.
  - Examples: computer data, digital audio.

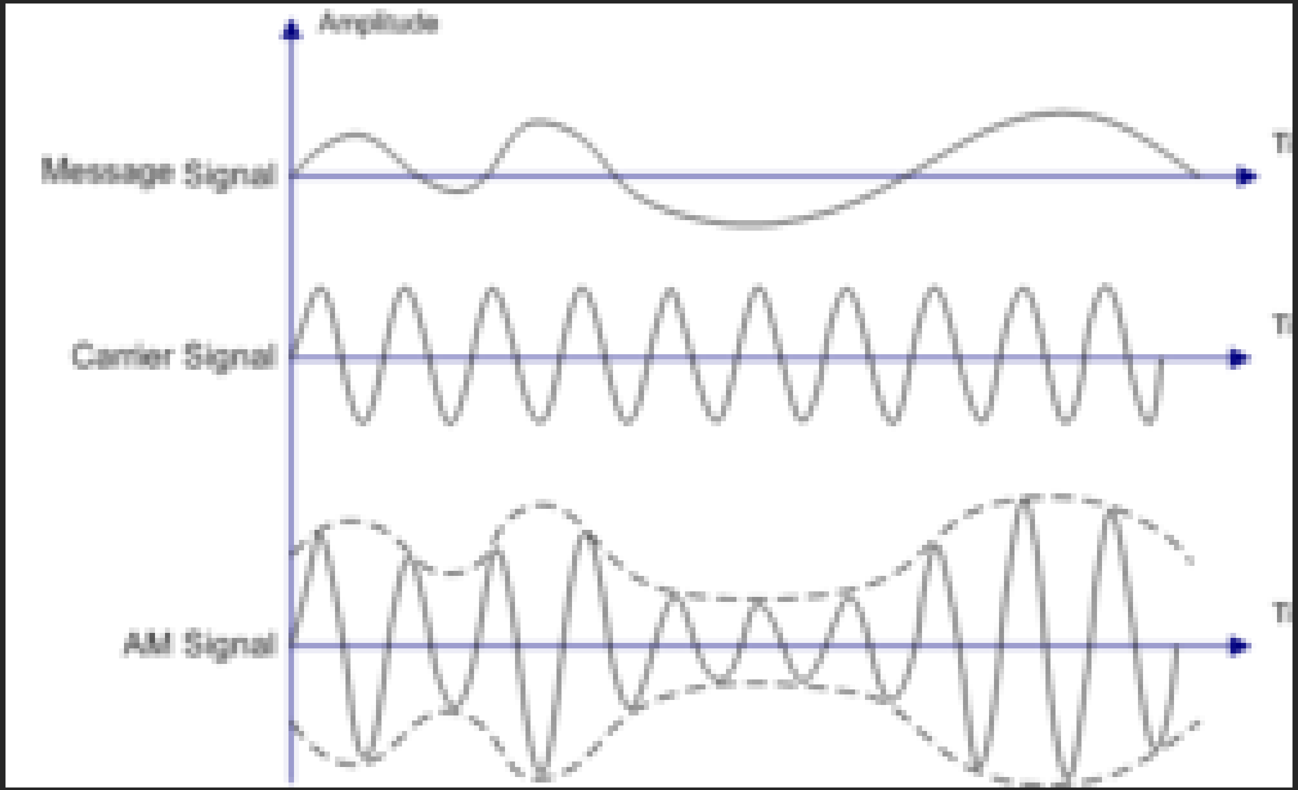
Analog Vs Digital

- When to use analog:
  - High Bandwidth
  - High Frequency
  - Real-time response
  - Example: FM radio
- When to use digital:
  - High noise environments
  - Encryption, compression, error correction
  - Storage
  - Example: video camera

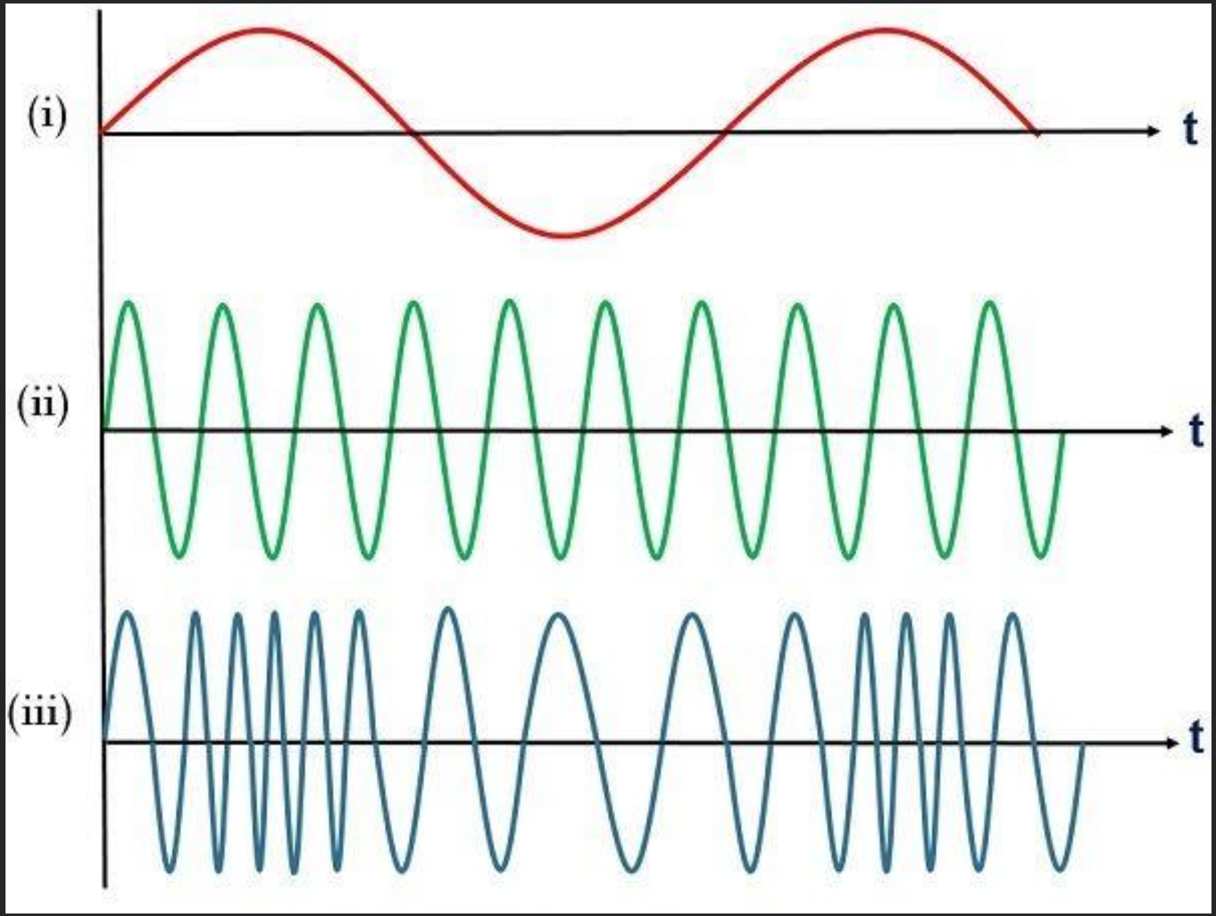
Modulation

- A **modulated signal** is a signal in which one or more characteristics of a **carrier wave** are varied in accordance with the information signal being transmitted.
- The purpose of modulation is to efficiently transmit information over long distances or through specific communication channels.
- **Carrier wave**: A high-frequency signal used as the base signal.
- **Information signal**: The data or message to be transmitted.

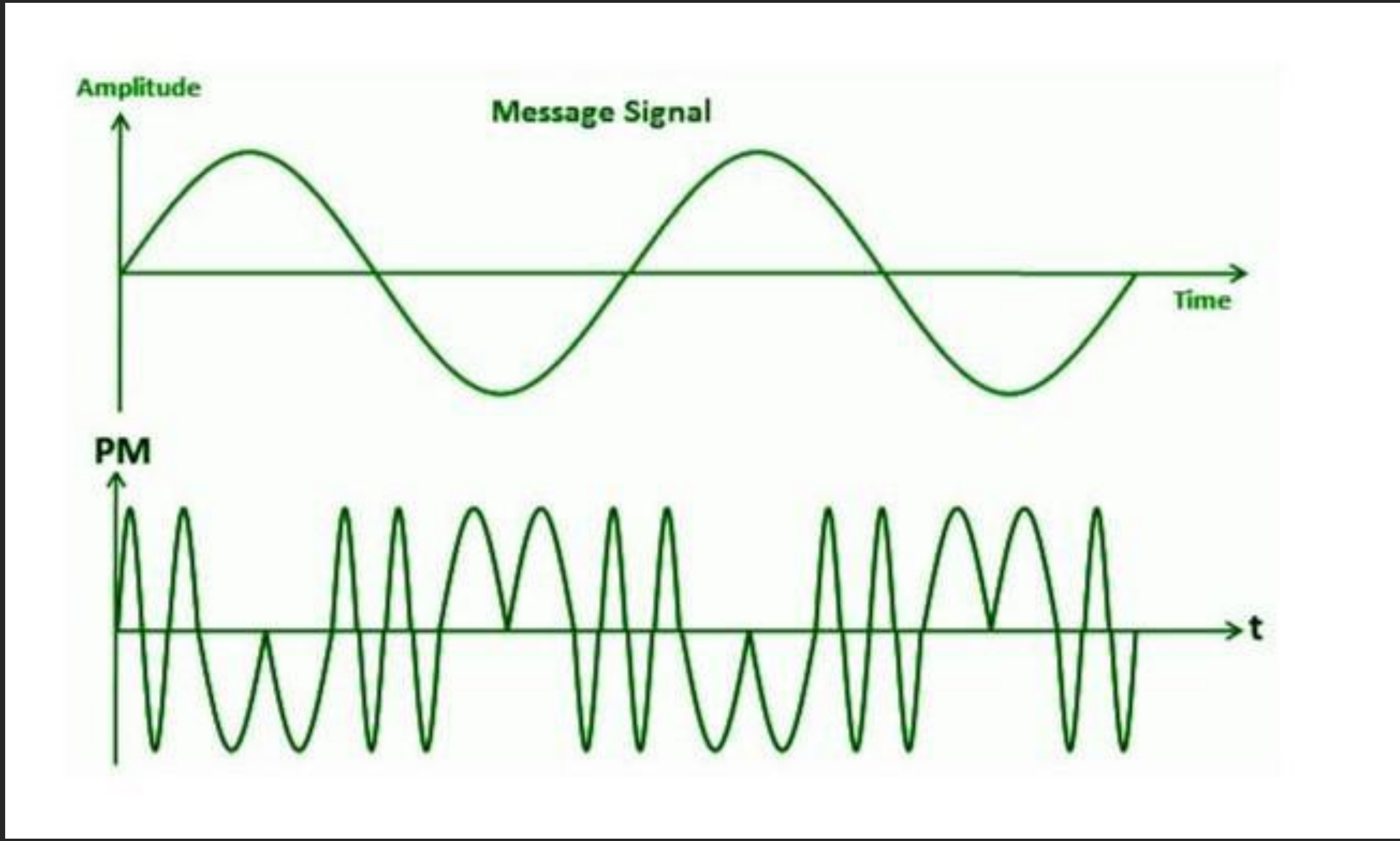
Amplitude Modulation



Frequency Modulation



Phase Modulation



Modulation

- Information signal can be analog or digital.
- Carrier signal frequency must be higher than the information signal.
  - Nyquist-Shannon Sampling Theorem – Carrier frequency must be at least twice the information frequency.
  - Often is significantly higher.

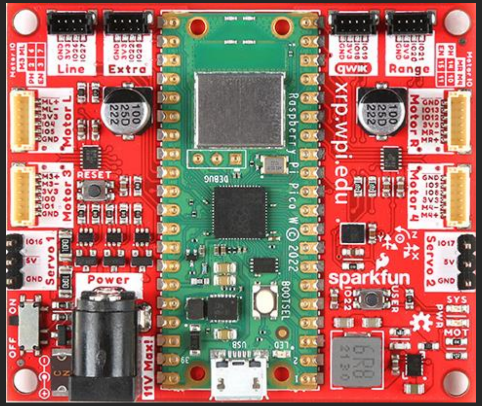

RADIO STATION
VIDEO GAMES

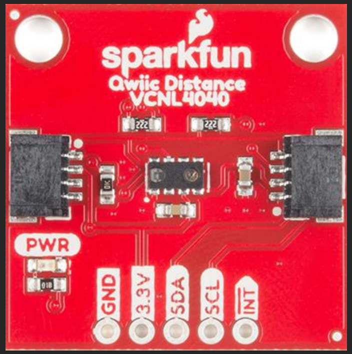
Synchronous vs Asynchronous

- Synchronous communication protocols – transmit data using a **shared clock signal** between the sender and receiver to ensure that data is sent and received at precisely coordinated intervals.
- Asynchronous communication protocols – do **not rely on a shared clock**. Instead, the sender and receiver synchronize data at the beginning of each transmission using **start and stop bits**.

Synchronous vs Asynchronous

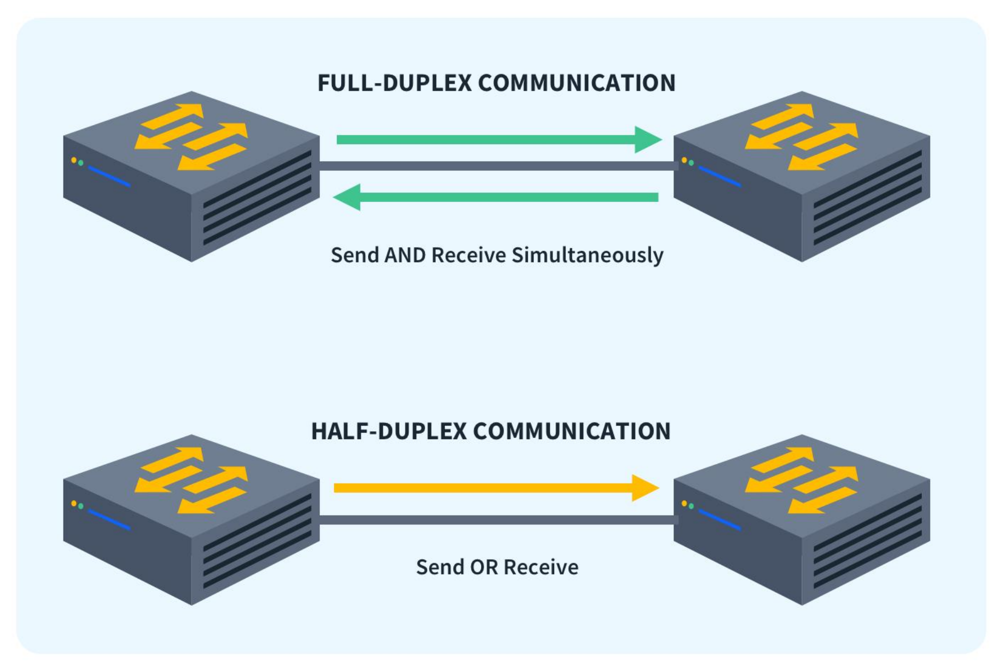
- When to use synchronous:
  - Faster communication speeds
  - Extra wires
  - Example: I2C – up to 3.4Mbps – half-duplex
- When to use asynchronous:
  - Slower communication speeds
  - Limited wires
  - Example: UART – up to 115.2kbps, full-duplex



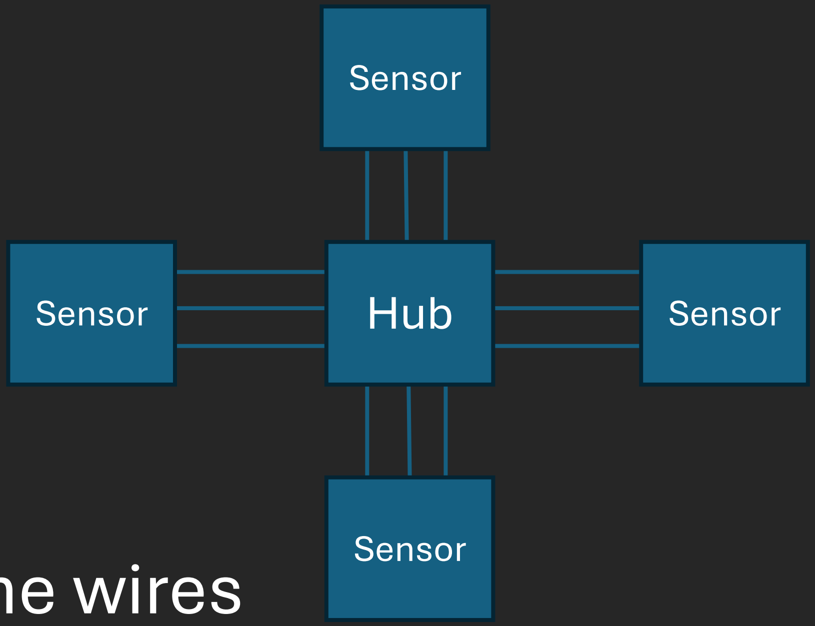


Duplexing

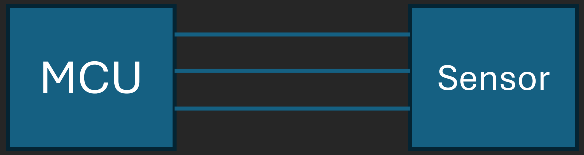
- Half duplex – Can only communicate one direction at a time
- Full duplex – simultaneous bidirectional communication

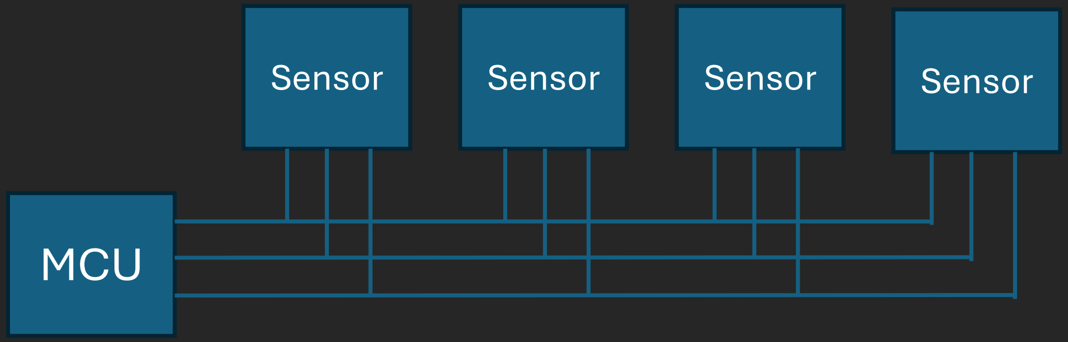


Topology



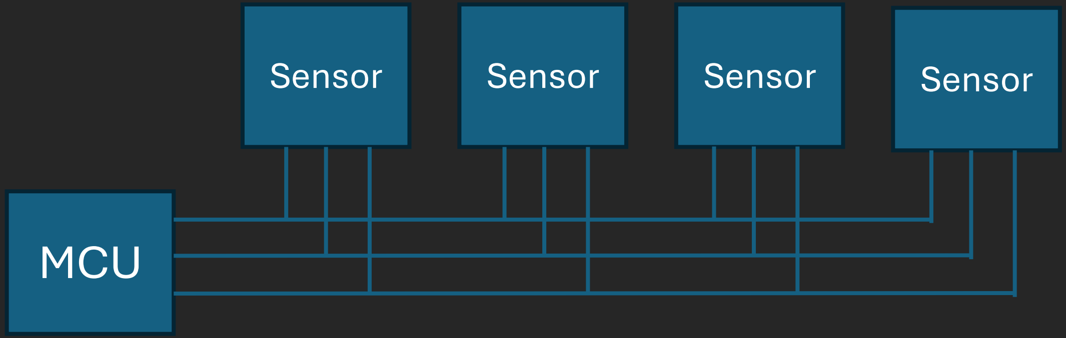
- Point-to-point
  - Example: UART, RS-232
- Bus – multiple devices connected to the same wires
  - Example: I2C, CAN bus
- Star – Multiple devices connected to the same central point
  - Examples: Ethernet, USB

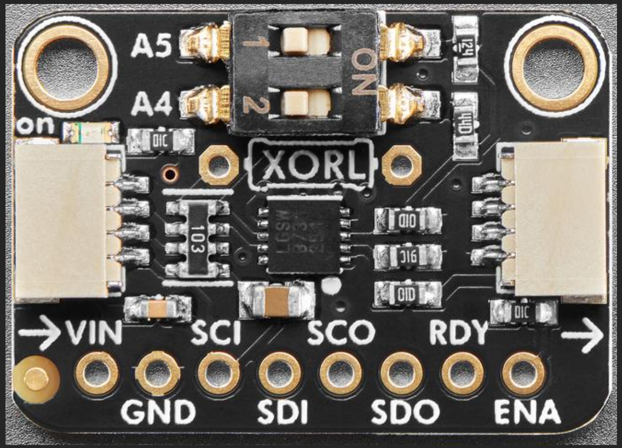


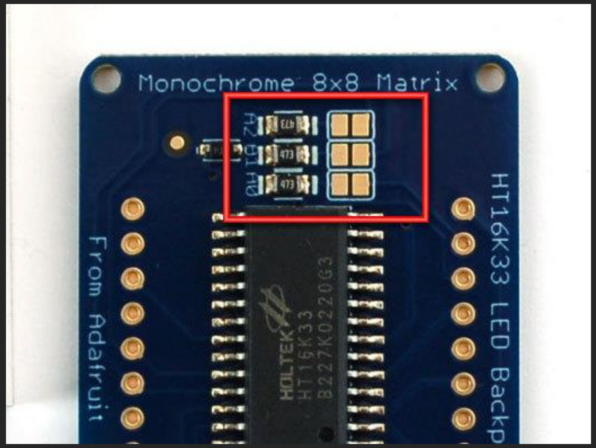


Addressing

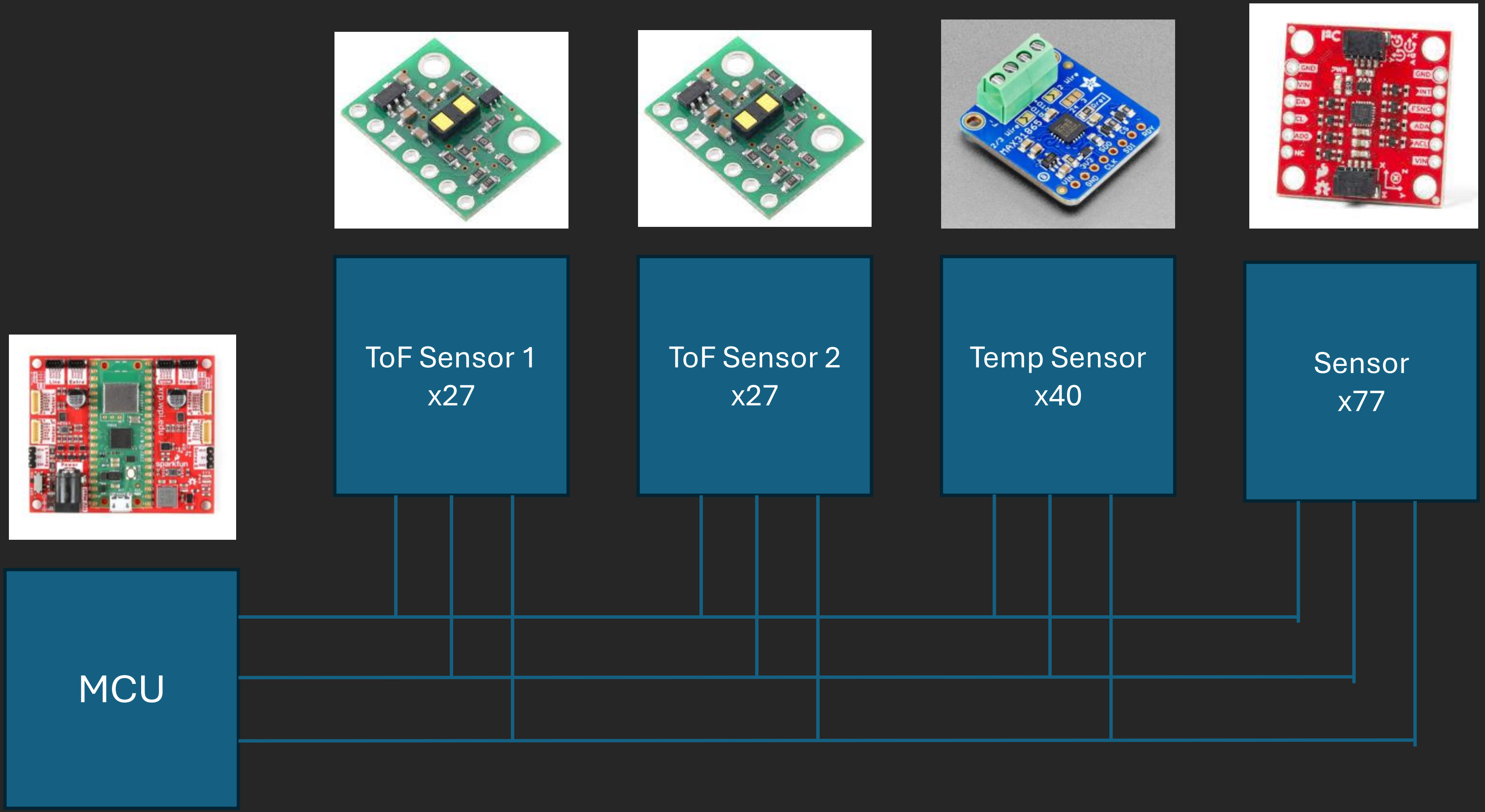
- Static Addressing
- Dynamic Addressing







Addressing


ToF Sensor 1
x27
ToF Sensor 2
x27
Temp Sensor
x40
Sensor
x77
MCU

Electrical Characteristics

- Pull-up & Pull-down resistors for open-drain/open-collector
- Wire capacitance – delay in state transition
- Time constant: $\tau = RC$
- Power vs Speed

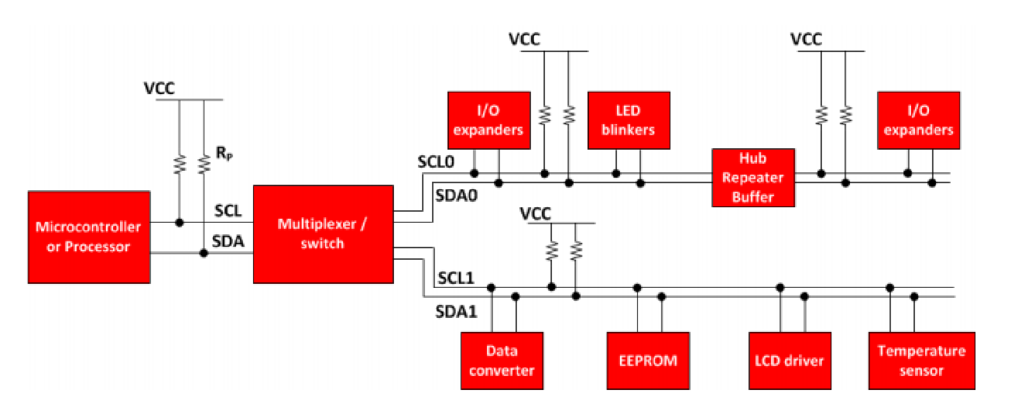
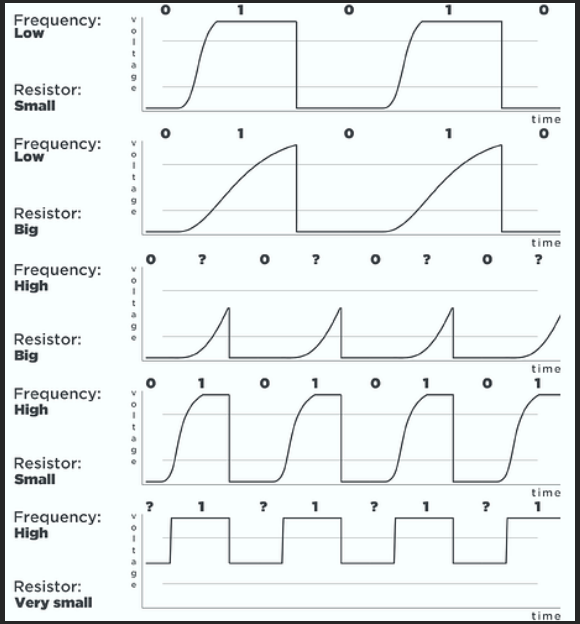
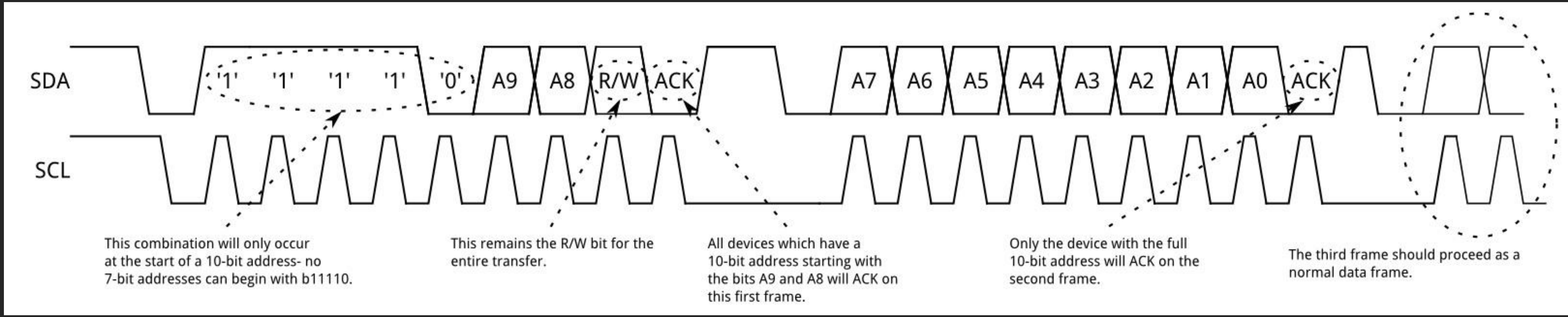


Figure 1. Application Example Showing I2C Communication Between the Different IC's on a System and With Pullup Resistors on I2C Bus



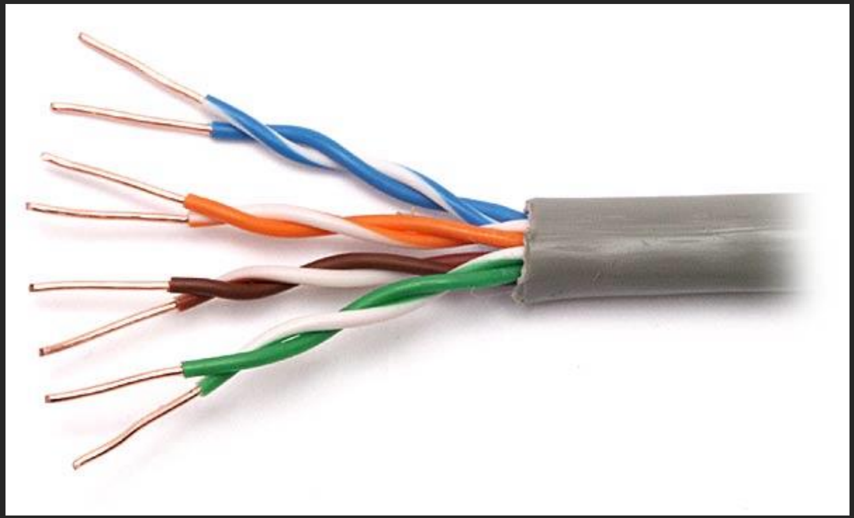
Frames & Packets

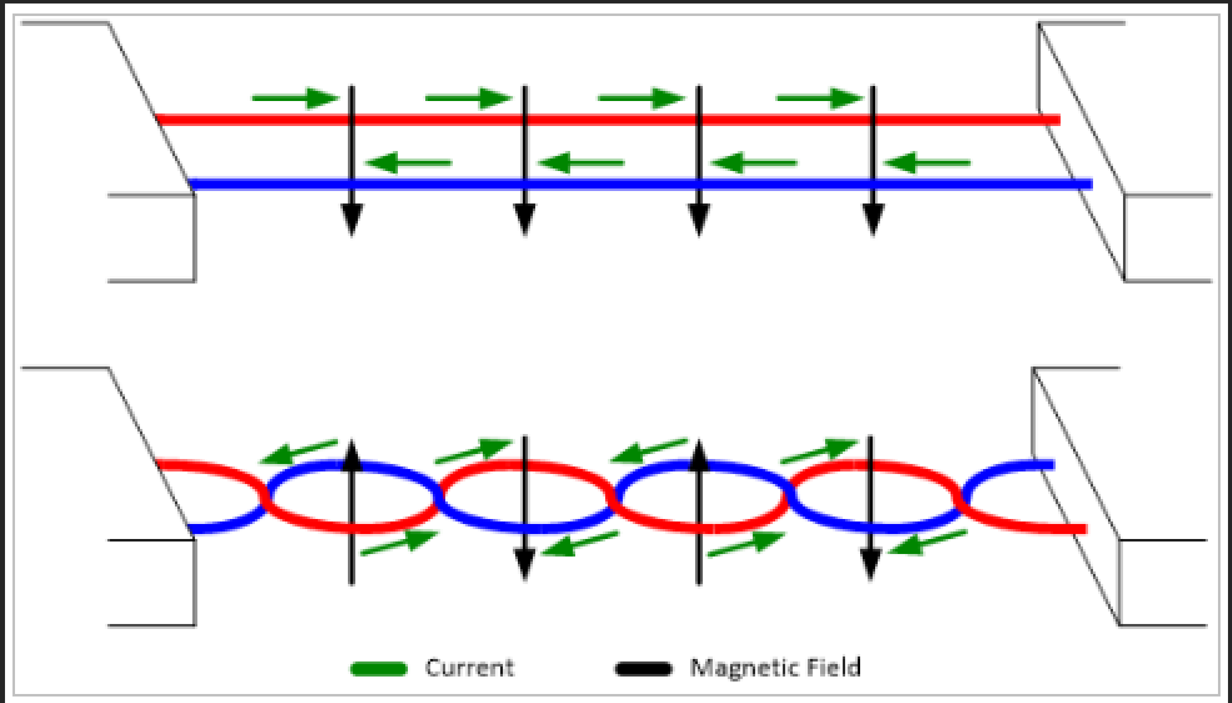
- “Unit of Data” or “Message”
- Contains meta data and data



Considerations

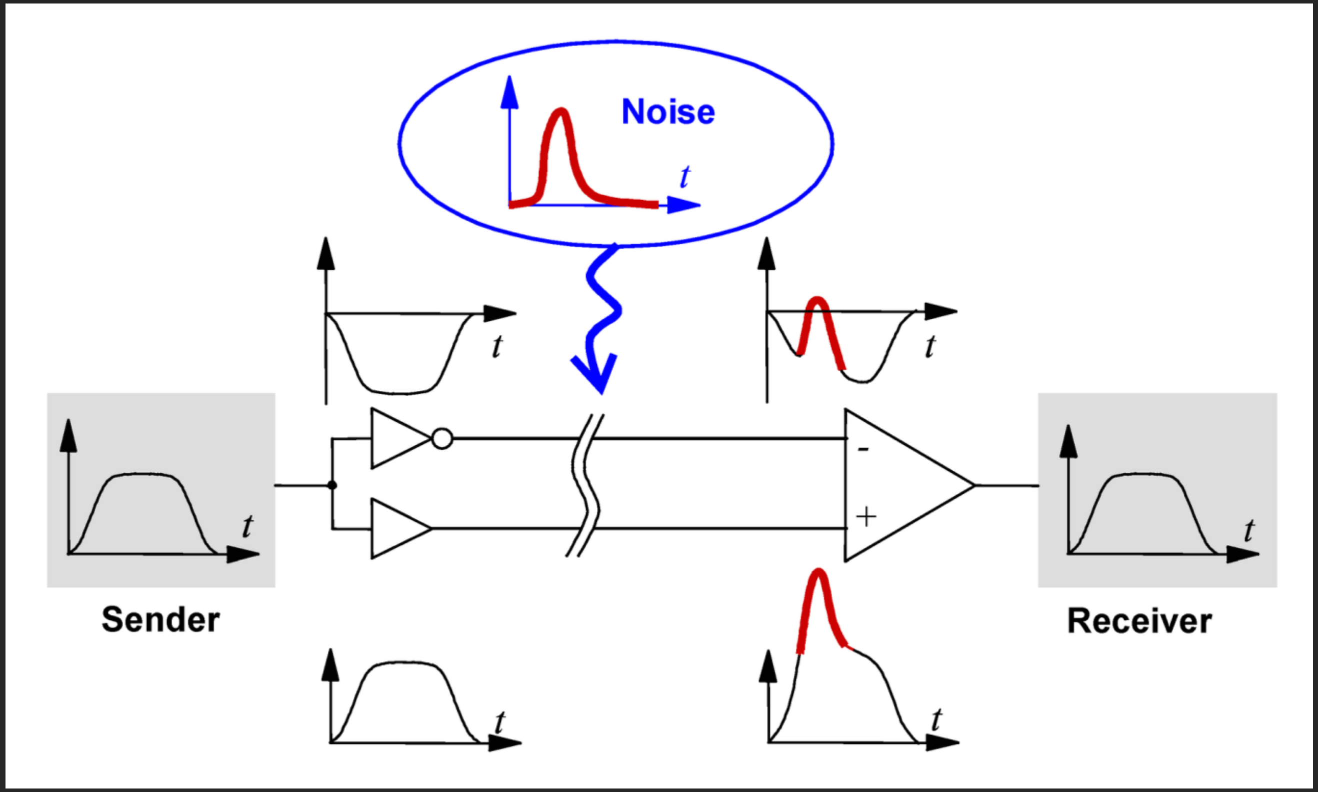
- Twisted Pair Cabling





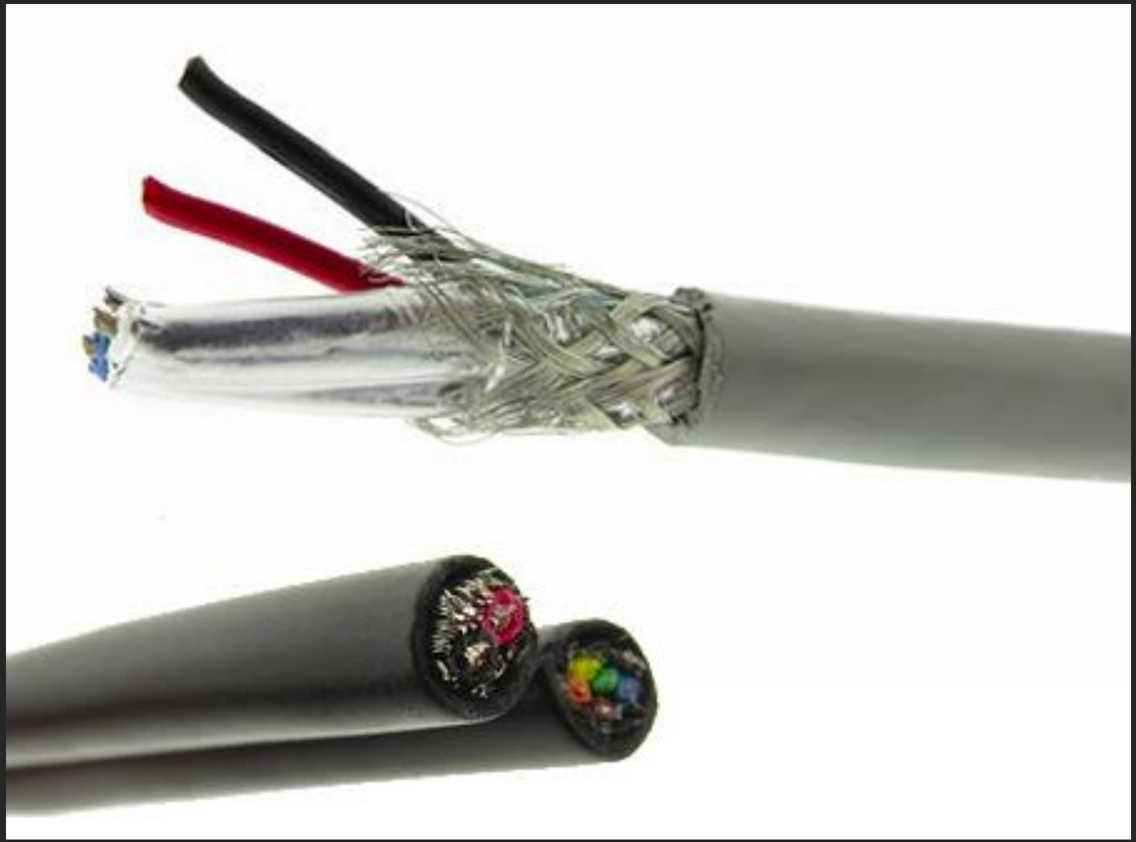
Considerations

- Twisted Pair Cabling
- Differential signals



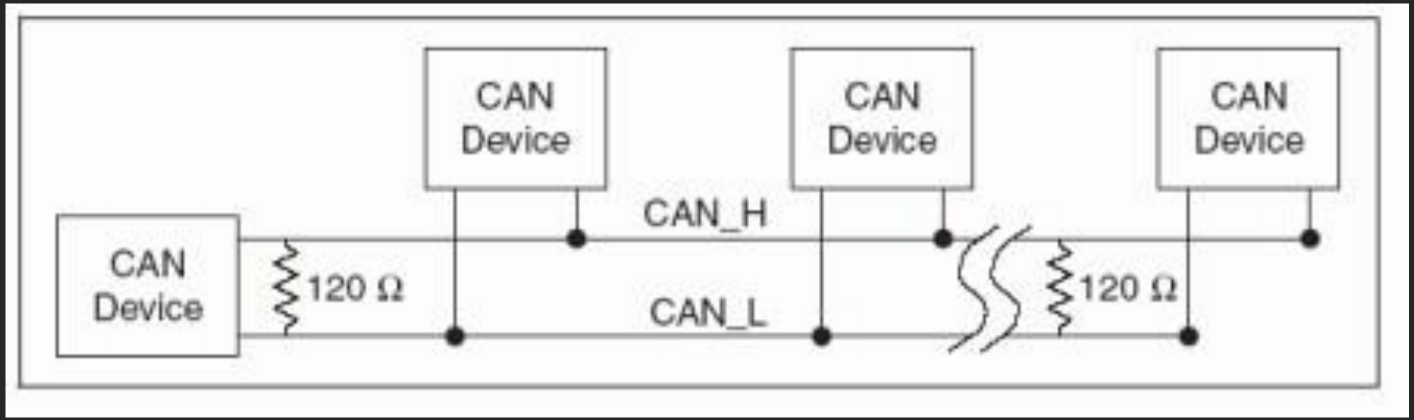
Considerations

- Twisted Pair Cabling
- Differential signals
- Shielded Cables
- Cable Routing



Considerations

- Twisted Pair Cabling
- Differential signals
- Shielded Cables
- Cable Routing
- Termination Resistors

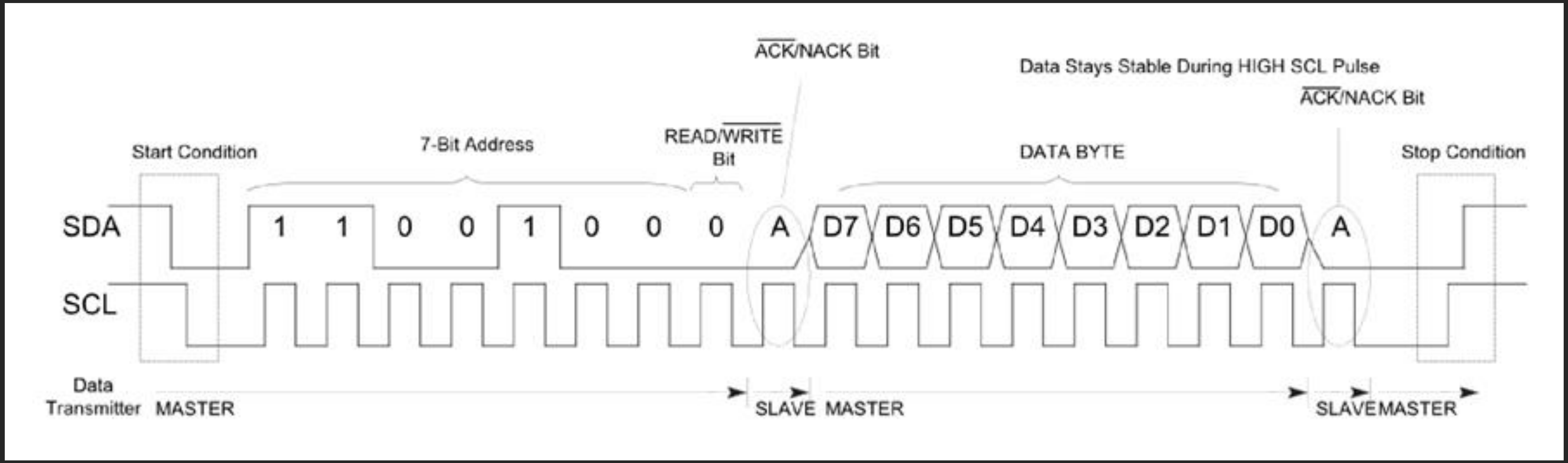


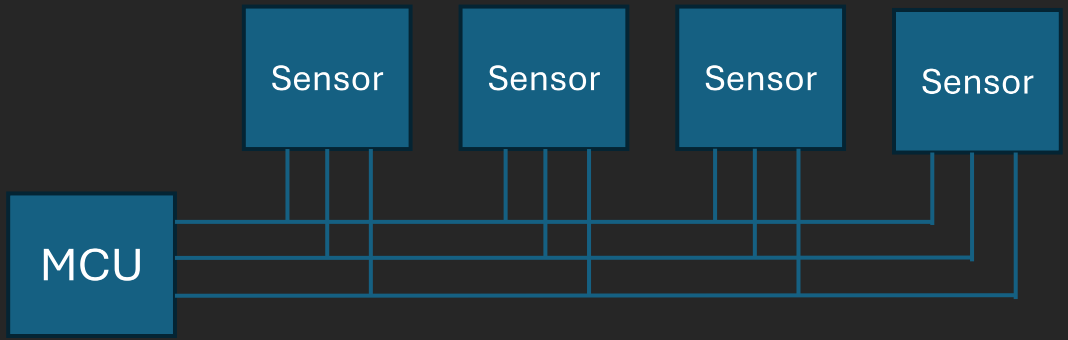
Wired Communication Protocols

Inter-Integrated Circuit (I2C)

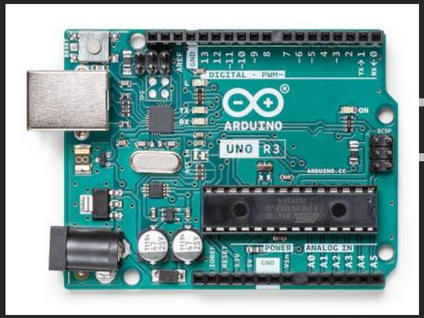
- Short distance, low-speed communication between circuit board components
- Open drain, synchronous, master-slave bus topology
- 2 wires (SCL – Serial Clock, SDA – Serial Data)
- Speeds – 100 kbps (4.7k Ω ~ 2.4mW) -> 3.4 Mbps (1k Ω ~ 15mW)
- Faster speeds = smaller resistors = more static power
- Longer wires = more capacitance = more dynamic power
- Simple, cost effective, multiple devices
- Limited to short distances and low speeds, susceptible to noise

Inter-Integrated Circuit (I2C)

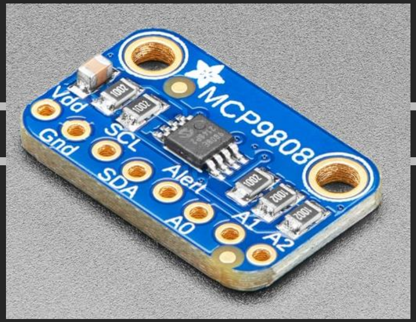




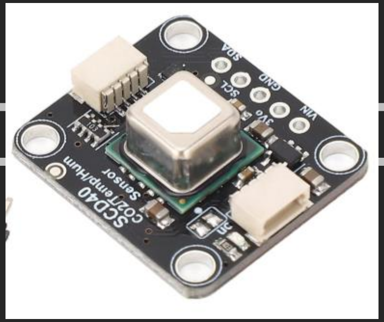
Inter-Integrated Circuit (I2C)



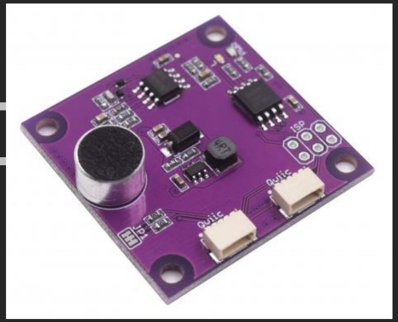
MCU



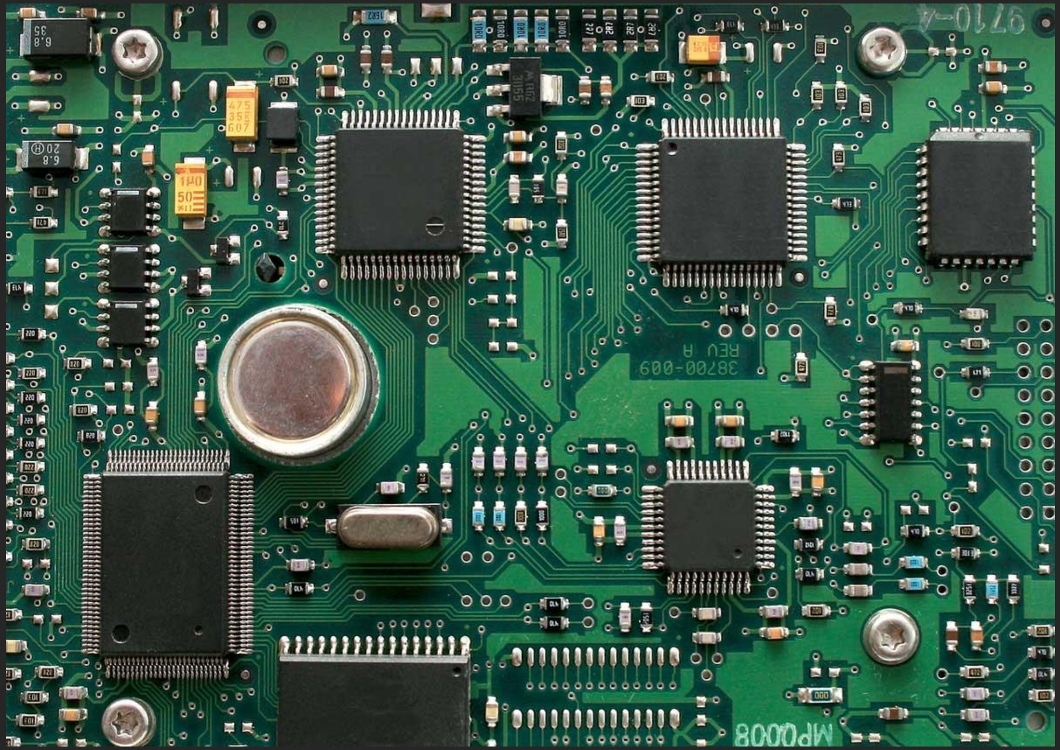
Temperature



CO2


Microphone

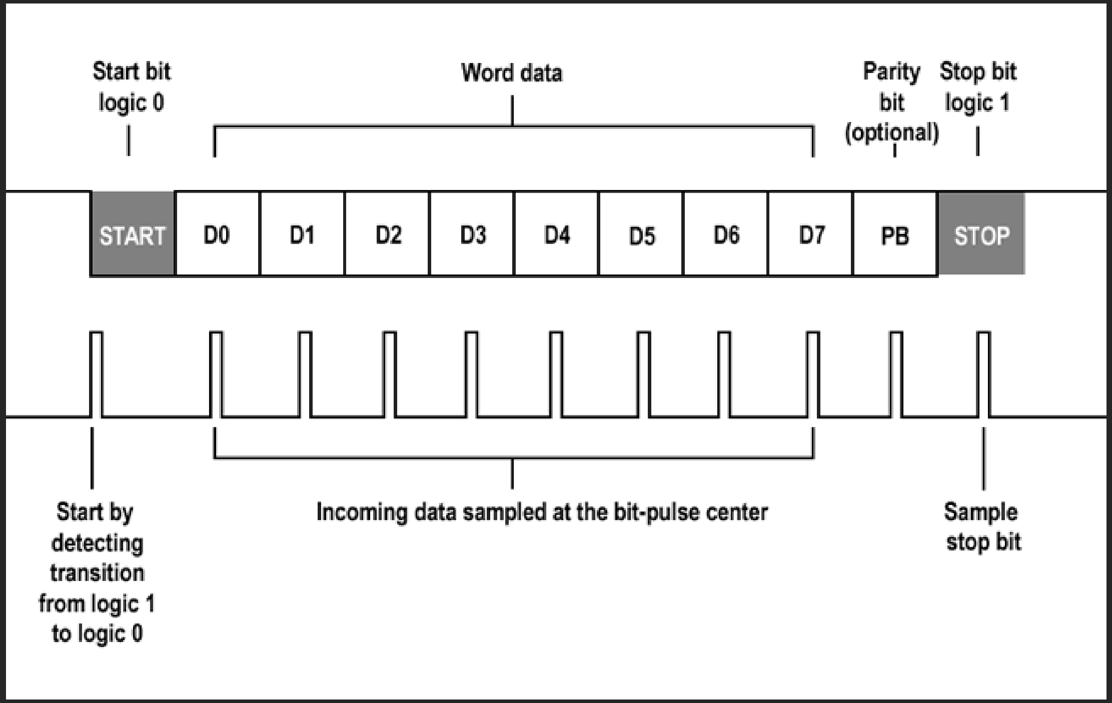
Inter-Integrated Circuit (I2C)

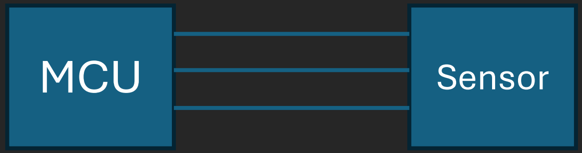


Universal Asynchronous Receiver/Transmitter

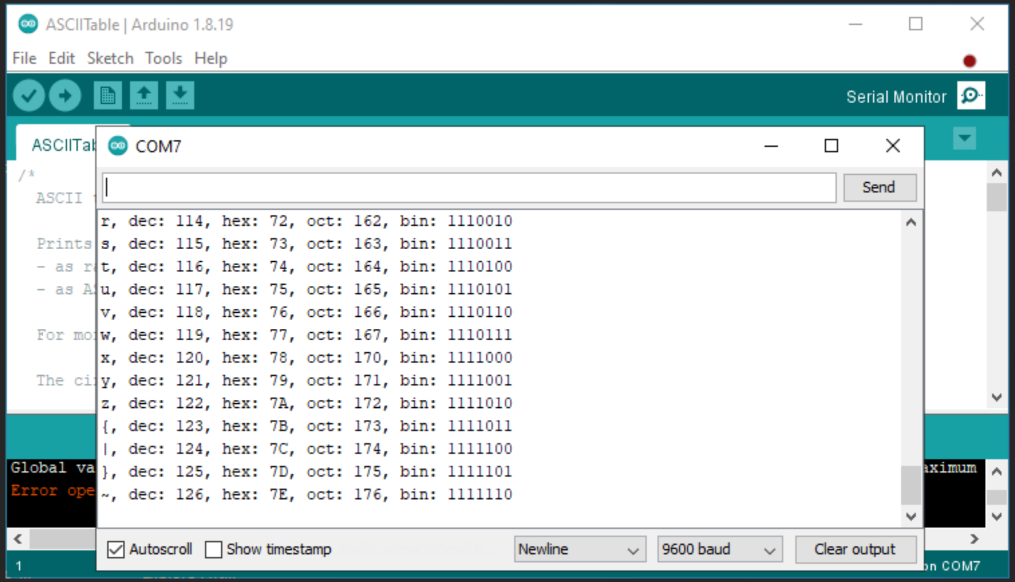
- Communication between two devices typically for debugging or low-speed data transfer
- Asynchronous point-to-point topology
- 2 wires (TX – Transfer, RX – Receive)
- Speeds – 9600 bps up to 1 Mbps
- Simple, widely supported, low resource overhead
- Limited to two devices, requires precise clock matching

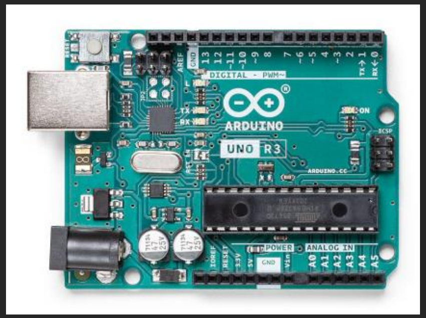
Universal Asynchronous Receiver/Transmitter





Universal Asynchronous Receiver/Transmitter

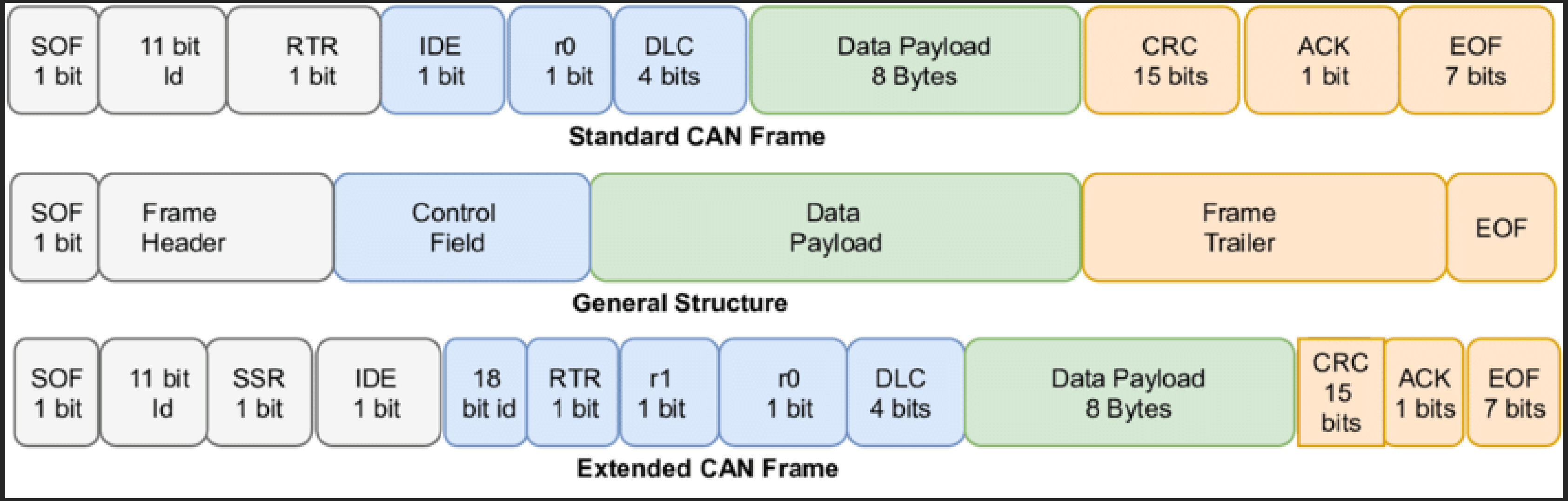


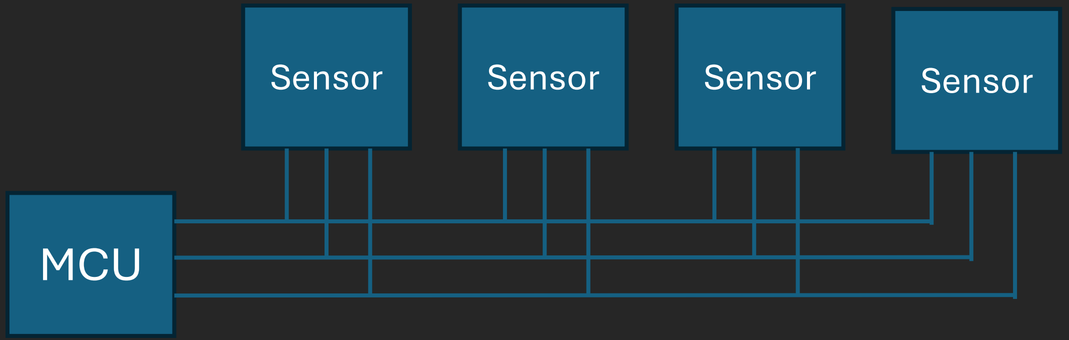


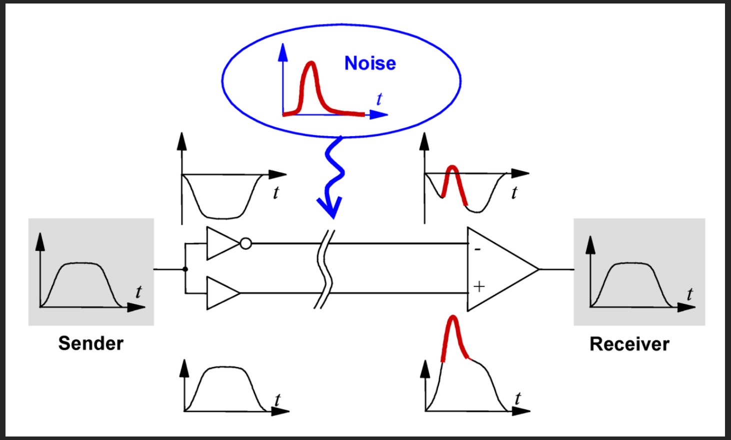
Controller Area Network (CAN Bus)

- Robust communication in noisy environment, such as automotive and industrial
- Asynchronous bus topology with support for priority-based arbitration schemes
- 2 wires (CAN_H, CAN_L), differential signaling
- Speeds – 125 kbps up to 1 Mbps
- Extremely robust, fault tolerant, arbitration (message priority)
- Higher power, slow communication speeds

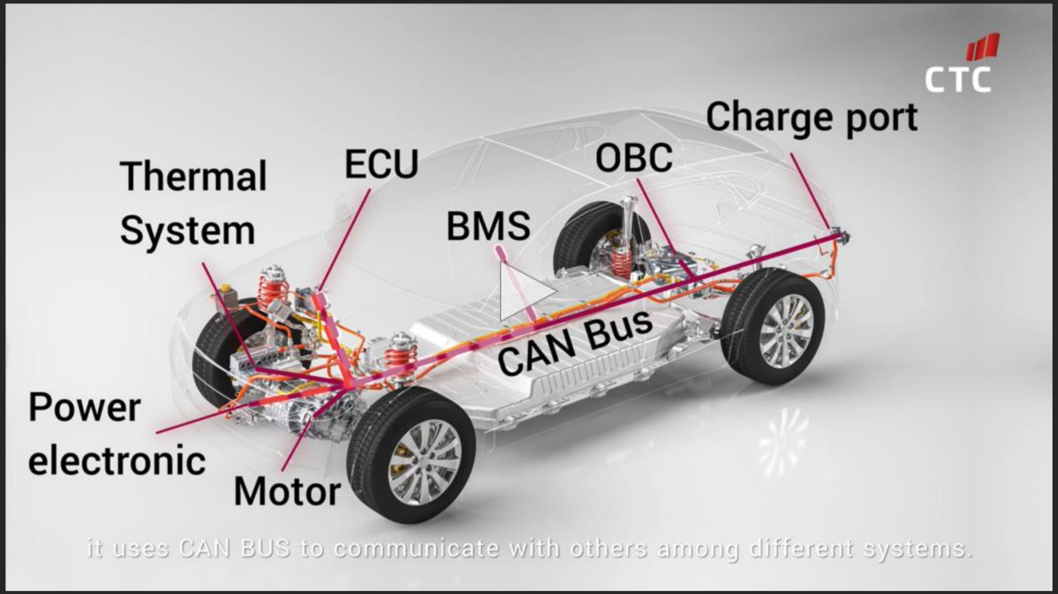
Controller Area Network (CAN Bus)







Controller Area Network (CAN Bus)



RS-485

- Designed for reliable multi-point communication over long distances in industrial environments
- Asynchronous, half or full duplex
- 2 or 4 wires – twisted pairs of differential signaling
- Speeds – up to 10 Mbps
- Long distance (up to 1200m), high noise immunity
- Slower than ethernet, requires extra hardware for multi-point

RS-485


plc247.com
plc247.com
MT8071iE 1WV
Weinview Co., Ltd
COM3
KV-L21V
PORT1
PORT2
TERM
PORT1
plc247.com
PORT2
Port.2

Universal Serial Bus (USB)

- High-speed, plug-and-play communication standard for peripherals
- Synchronous star topology using host-peripheral model
- 4 wires (VCC, GND, D+, D-), differential signaling
- Speeds – 500 Mbps (USB 2.0), 5 Gbps (USB 3.0), 40 Gbps (USB 4.0)
- High speed and versatile, supports charging and power delivery
- Limited scalability, shorted cable lengths, requires transceivers or controllers

Universal Serial Bus (USB)

- Device Configuration Descriptor
  - Transfer Type
  - Endpoint Address
  - Maximum Packet Size

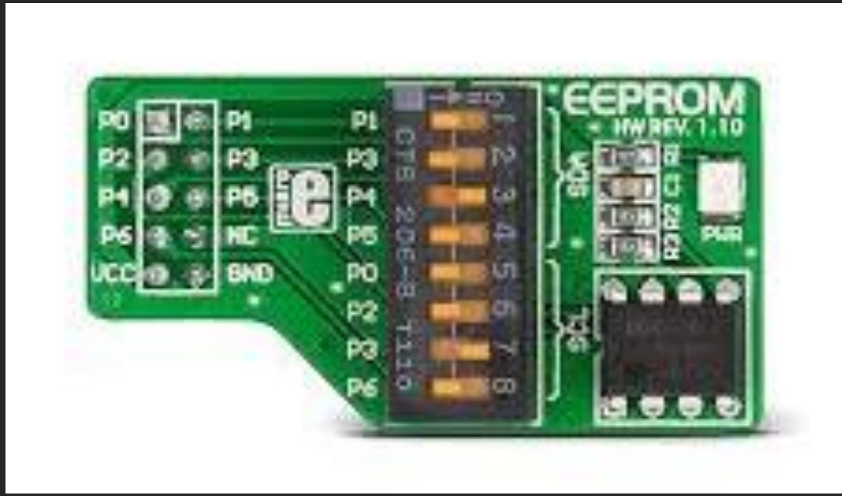
Universal Serial Bus (USB)

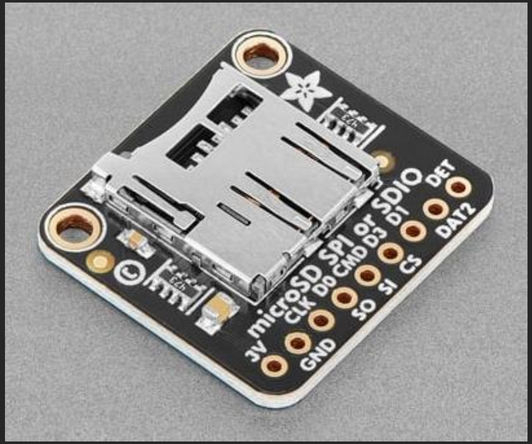
- Control Transfer
  - Device configuration and setup
- Interrupt Transfer
  - Small, time-sensitive packets (e.g., keyboard strokes)
- Bulk Transfer
  - Large, non-time sensitive data
- Isochronous Transfer
  - Time-critical data without error checking (e.g., video/audio streaming)

Serial Peripheral Interface (SPI)

- High-speed, short distance communication for MCUs and peripherals
- Synchronous point-to-point (with device selection)
- 4 wires (MISO, MOSI, SCLK, SS), one SS per device
- Speeds – 50 Mbps
- High-speed, efficient continuous data transfer, simple, full duplex
- More wires than I2C, no addressing, limited to short distances

Serial Peripheral Interface (SPI)

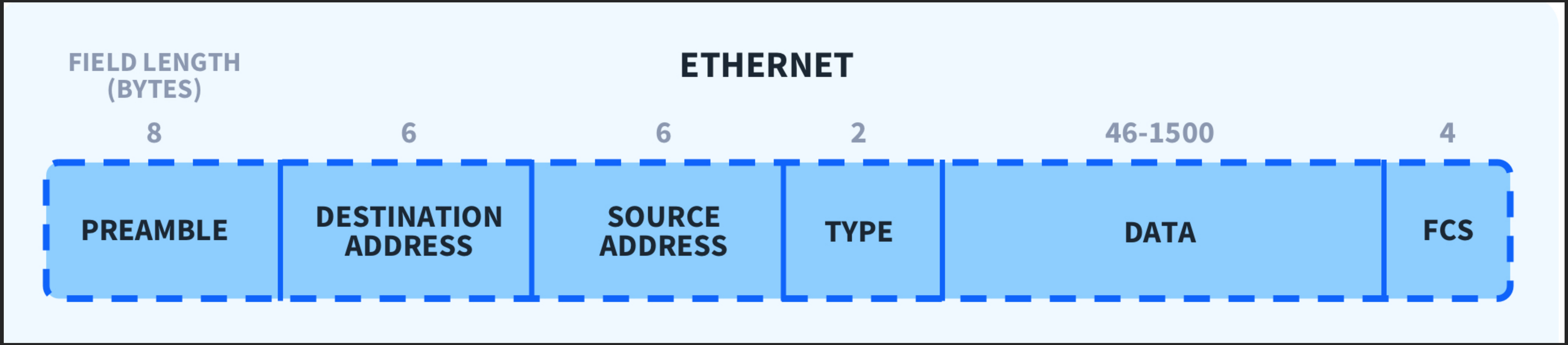




Ethernet

- Supports internet communication protocols, LANs, and industrial automation
- Pseudo-synchronous (no dedicated clock), star or tree topology
- Defines Physical Layer and Datalink Layer
- 4 or 8 wires – twisted pairs of differential signaling
- Speeds – Fast Ethernet (10/100 Mbps), Gigabit Ethernet (1000 Mbps)
- Extremely scalable, standardized, supports advanced features
- Requires switches, routers, ruggedized components, latency

Ethernet



FIELD LENGTH (BYTES)
ETHERNET
8
6
6
2
46-1500
4
PREAMBLE
DESTINATION ADDRESS
SOURCE ADDRESS
TYPE
DATA
FCS

Ethernet

Ethernet Type	Speed	Medium	Distance	Application
Fast Ethernet	100 Mbps	Copper (Cat5e)	100 m	Legacy systems, small networks
Gigabit Ethernet	1 Gbps	Copper, Fiber	100 m (copper), 5 km (fiber)	Standard LANs, industrial use
10 Gigabit Ethernet	10 Gbps	Copper, Fiber	100 m (Cat6a), 10 km (fiber)	Data centers, backbones
25/40/50 Gigabit	25–50 Gbps	Fiber	100 m–several km	High-speed interconnects
100 Gigabit Ethernet	100 Gbps	Fiber	Up to 40 km	Data centers, backbone networks
Industrial Ethernet	Varies	Rugged Copper, Fiber	Varies	Factory automation, robotics
PoE	Up to 100 Mbps	Copper	100 m	Powering IP devices (APs, cameras)

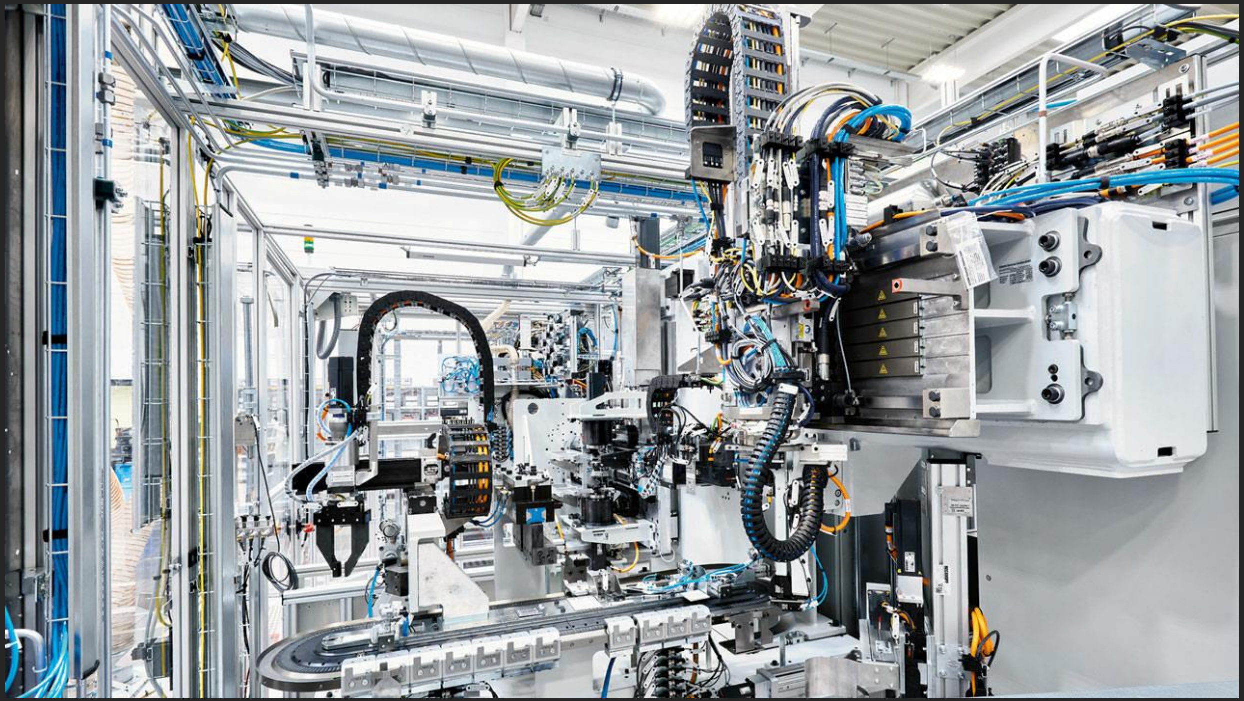
Ethernet

Standard	Medium	Data Rate	Distance
10BASE-T	Twisted-pair copper	10 Mbps	100 meters
100BASE-TX	Twisted-pair copper	100 Mbps	100 meters
1000BASE-T	Twisted-pair copper	1 Gbps	100 meters
1000BASE-SX	Multi-mode fiber	1 Gbps	550 meters
1000BASE-LX	Single-mode fiber	1 Gbps	5–10 kilometers
10GBASE-T	Twisted-pair copper	10 Gbps	100 meters
10GBASE-SR	Multi-mode fiber	10 Gbps	300 meters
10GBASE-LR	Single-mode fiber	10 Gbps	10 kilometers

Ethernet


RouterBOARD
Power
hEXs
SFP
PoE in
2
3
4
5
PoE out

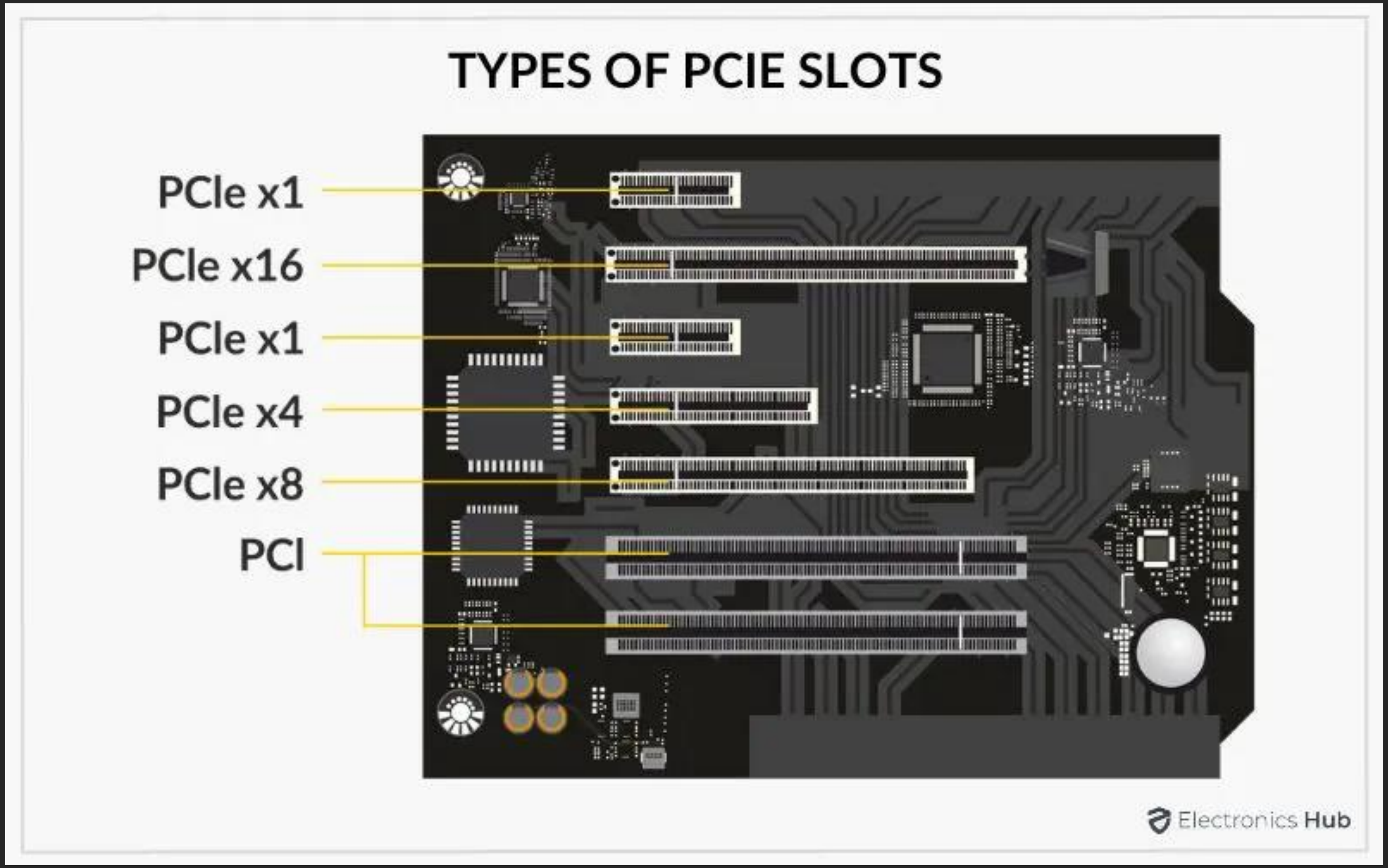

D-Link
D-Link DGS-105



Peripheral Component Interconnect (PCIe)

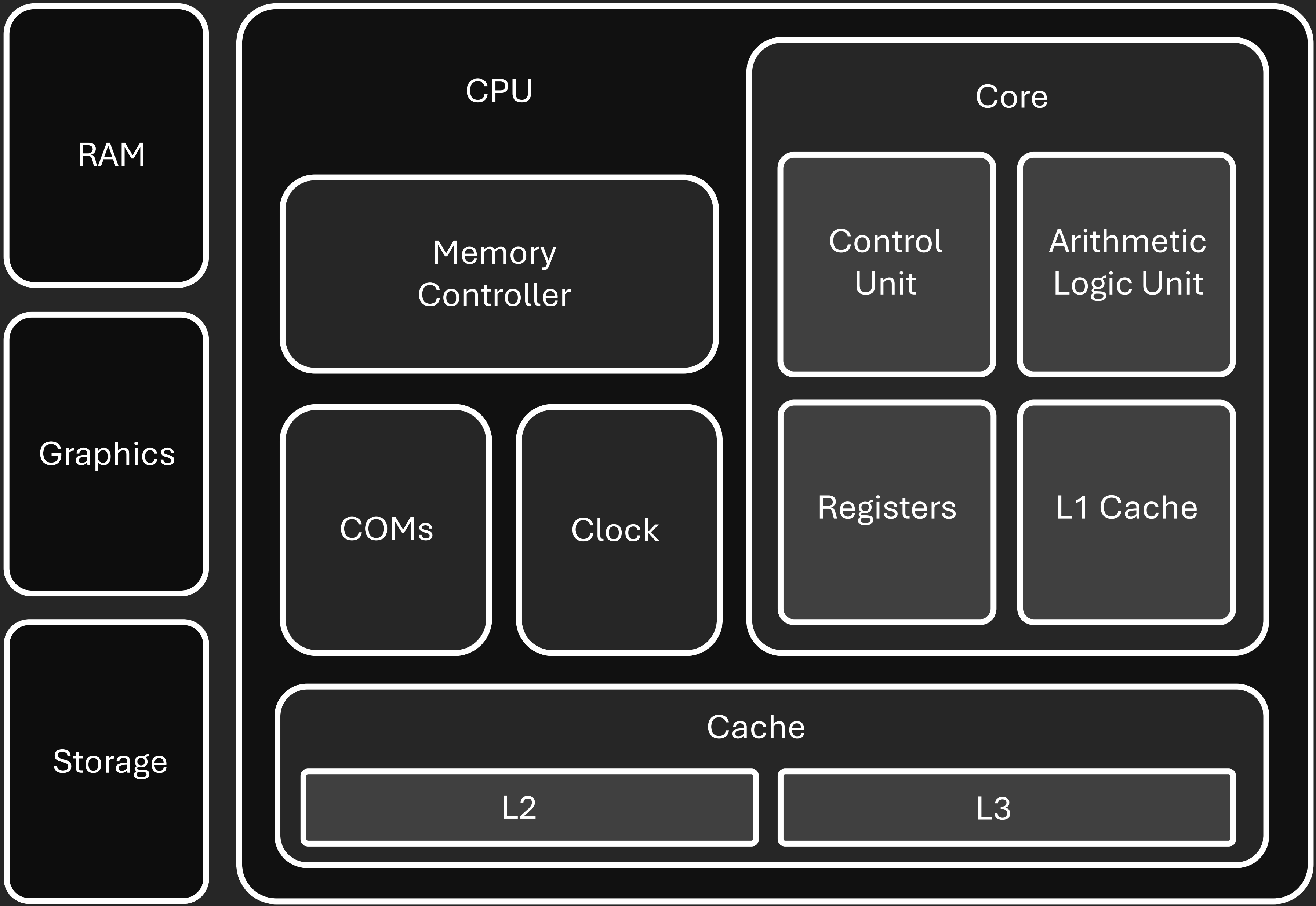
- High-speed interconnect for internal hardware within a computer over traces or dedicated connectors
- Synchronous, point-to-point
- x4, x8, or x16 slots, 4 traces (TX+, TX-, RX+, RX-) per lane
- Speeds – depends on version and number of lanes, up to 128Gbps
- Extremely high speed, low latency
- Complex and expensive implementation

Peripheral Component Interconnect (PCIe)



CPU/MCU Hardware Support

- Commonly supported protocols in hardware
  - I2C, SPI, UART, USB


RAM
Graphics
Storage
CPU
Memory
Controller
COMs
Clock
Core
Control
Unit
Arithmetic
Logic Unit
Registers
L1 Cache
Cache
L2
L3

CPU/MCU Hardware Support

- Commonly supported protocols in hardware
  - I2C, SPI, UART, USB
- Advantages
  - Offloading workload
  - Precise timing
  - Reduced Latency
  - Reliability
- Bit-Banging
- Hardware Abstraction Layer (HAL) and Drivers

Code Example – IMU over I2C

```python
import machine
import utime

# Initialize I2C on the Pico.
# Change the pin numbers if you're using different GPIOs.
i2c = machine.I2C(0, scl=machine.Pin(1), sda=machine.Pin(0),
freq=400000)
# MPU6050 device I2C address (default is 0x68)
MPU6050_ADDR = 0x68

# MPU6050 register addresses
PWR_MGMT_1    = 0x6B   # Power management register
ACCEL_XOUT_H = 0x3B   # Starting register for accelerometer data
GYRO_XOUT_H   = 0x43   # Starting register for gyroscope data

# Wake up the MPU6050 (it starts in sleep mode)
i2c.writeto_mem(MPU6050_ADDR, PWR_MGMT_1, b'\x00')
utime.sleep_ms(100)  # short delay to allow the sensor to wake up
```

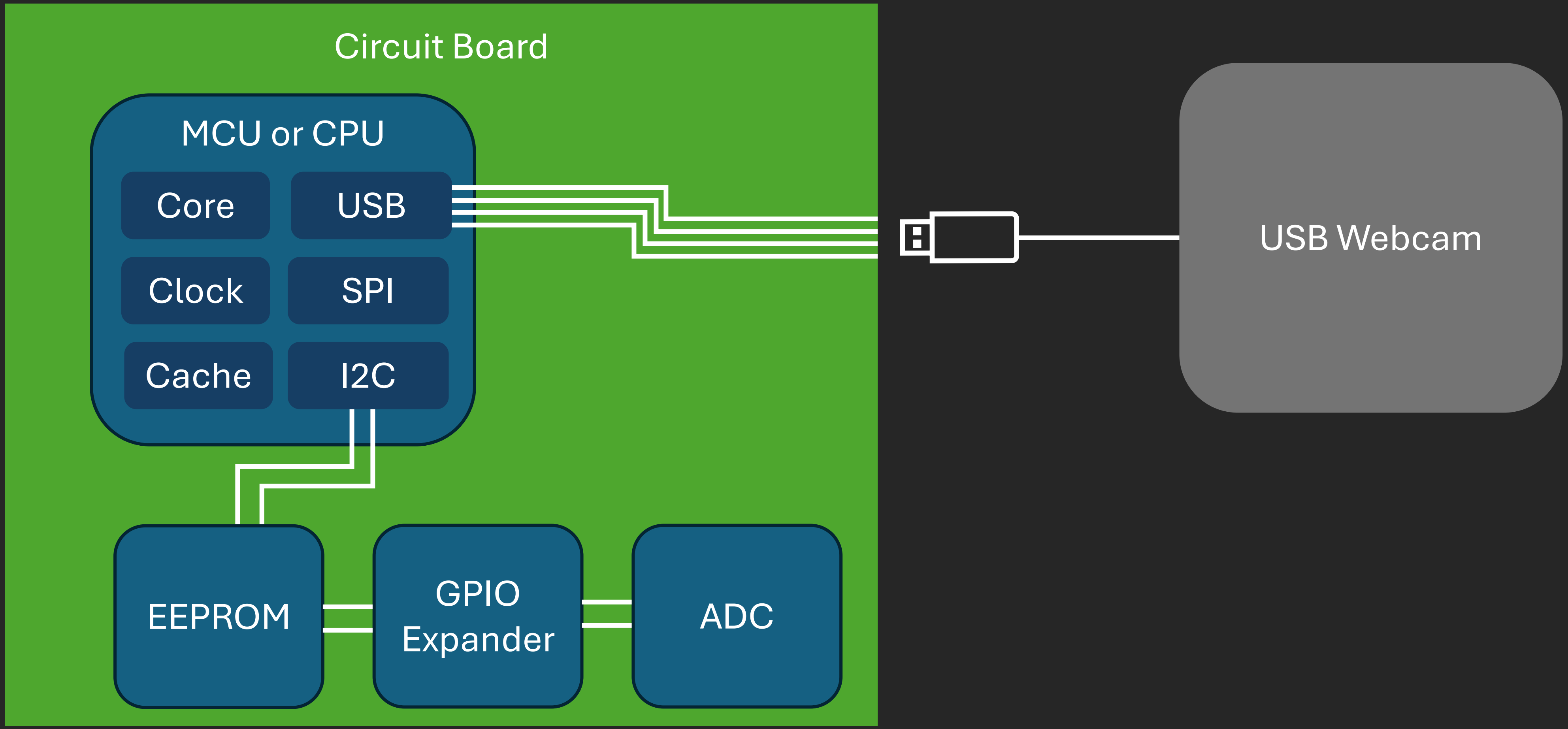
Code Example – IMU over I2C

```python
def read_raw_data(register):
    """
    Read two bytes of data from the given register and combine them into a signed integer.
    """
    # Read 2 bytes from the specified register
    data = i2c.readfrom_mem(MPU6050_ADDR, register, 2)
    # Combine the two bytes (big-endian)
    value = data[0] << 8 | data[1]
    # Convert unsigned value to signed (16-bit)
    if value > 32767:
        value -= 65536
    return value
```

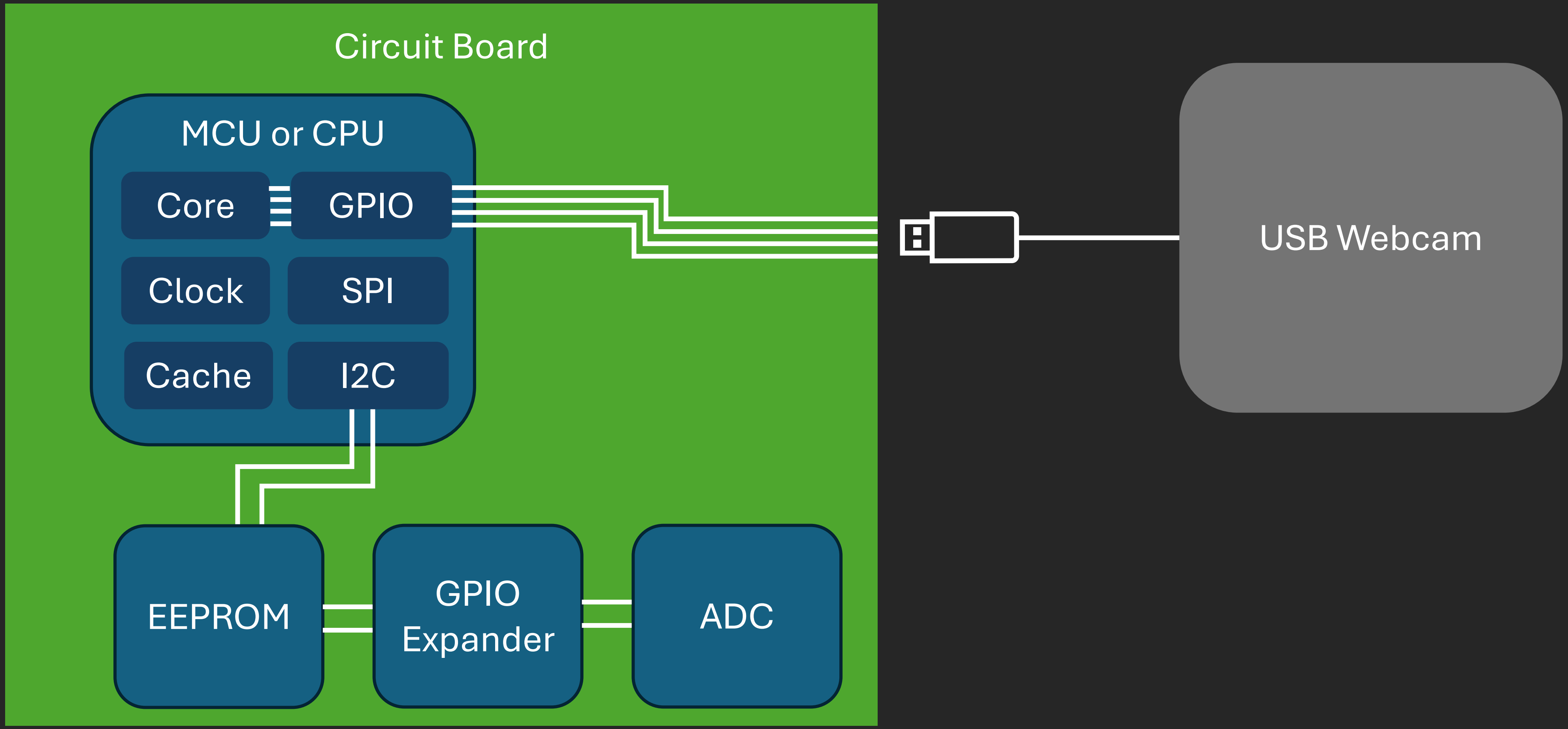
Code Example – IMU over I2C

```
while True:
    # Read raw accelerometer data for X, Y, Z axes.
    acc_x = read_raw_data(ACCEL_XOUT_H)
    acc_y = read_raw_data(ACCEL_XOUT_H + 2)
    acc_z = read_raw_data(ACCEL_XOUT_H + 4)

    # Read raw gyroscope data for X, Y, Z axes.
    gyro_x = read_raw_data(GYRO_XOUT_H)
    gyro_y = read_raw_data(GYRO_XOUT_H + 2)
    gyro_z = read_raw_data(GYRO_XOUT_H + 4)

    # Optionally, convert raw data to physical units.
    # For example, with the default sensitivity settings:
    #   - Accelerometer: 16384 LSB/g (i.e. ax = acc_x/16384.0 gives acceleration in g)
    #   - Gyroscope: 131 LSB/(°/s) (i.e. gx = gyro_x/131.0 gives angular velocity in °/s)
    ax = acc_x / 16384.0
    ay = acc_y / 16384.0
    az = acc_z / 16384.0
    gx = gyro_x / 131.0
    gy = gyro_y / 131.0
    gz = gyro_z / 131.0

    # Print the sensor readings
    print("Accelerometer (g): X={:.2f}, Y={:.2f}, Z={:.2f}".format(ax, ay, az))
    print("Gyroscope (°/s):  X={:.2f}, Y={:.2f}, Z={:.2f}".format(gx, gy, gz))
    print("-" * 50)

    utime.sleep(1)  # Delay 1 second before the next reading767:
        value -= 65536
    return value
```

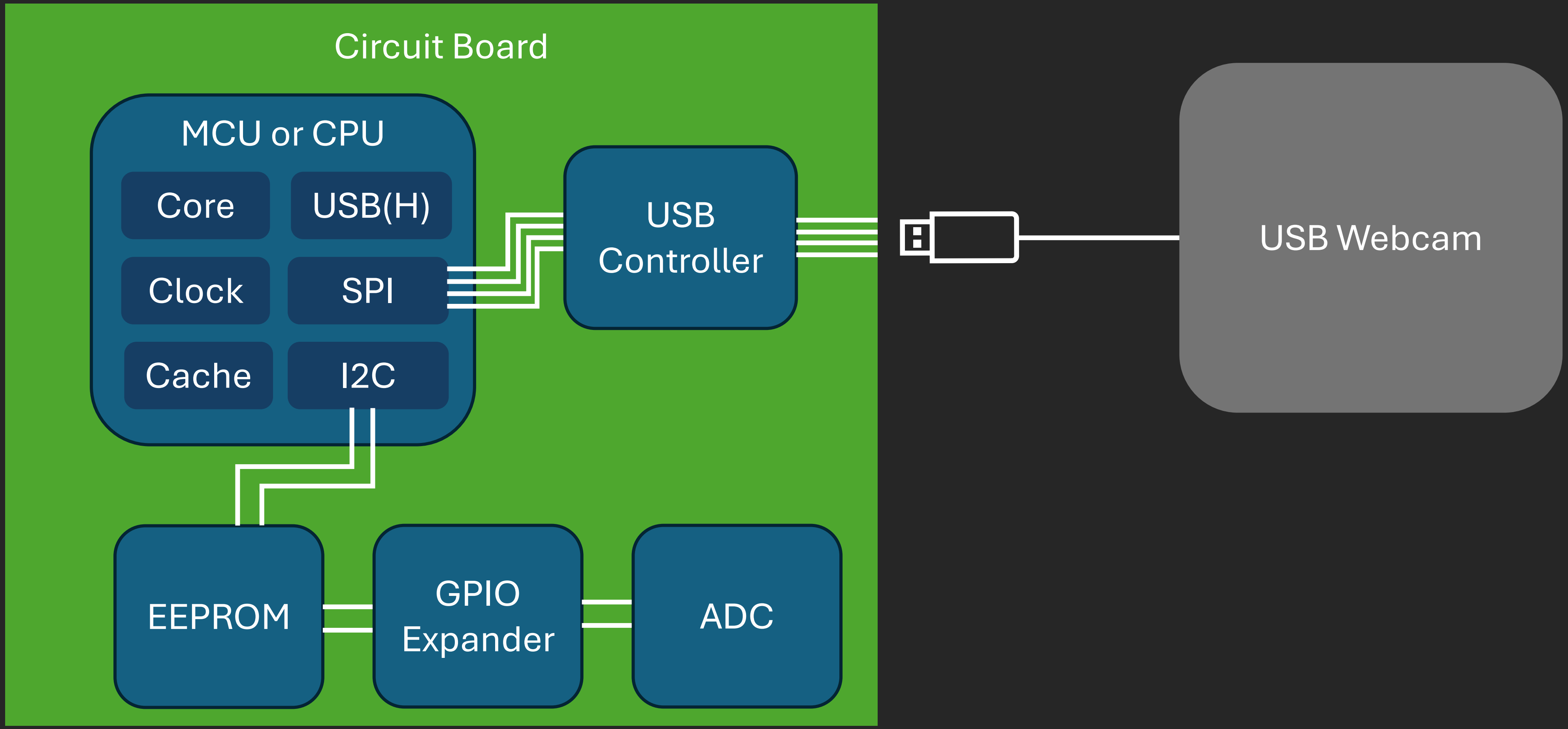
System Design Considerations



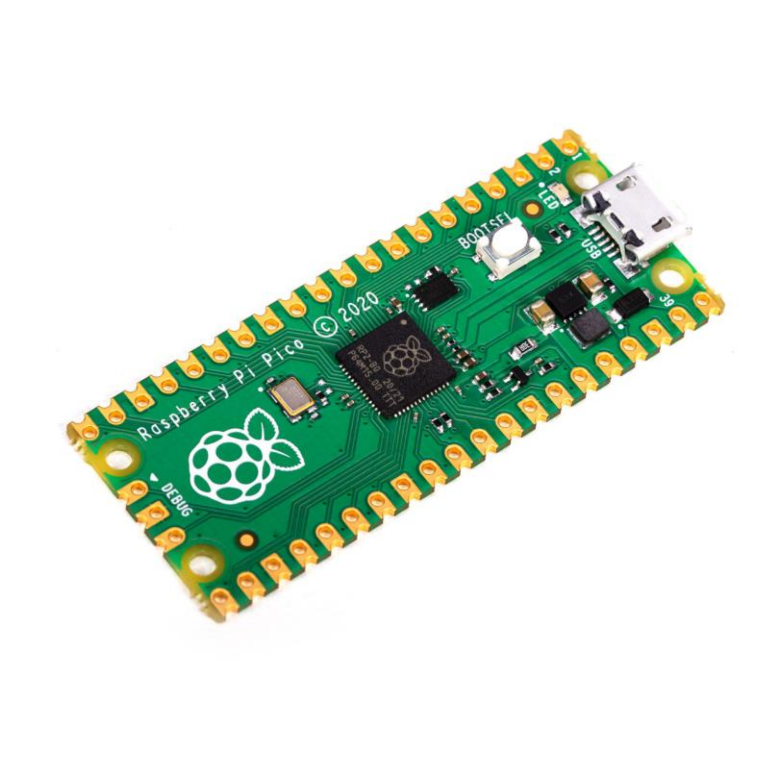
System Design Considerations

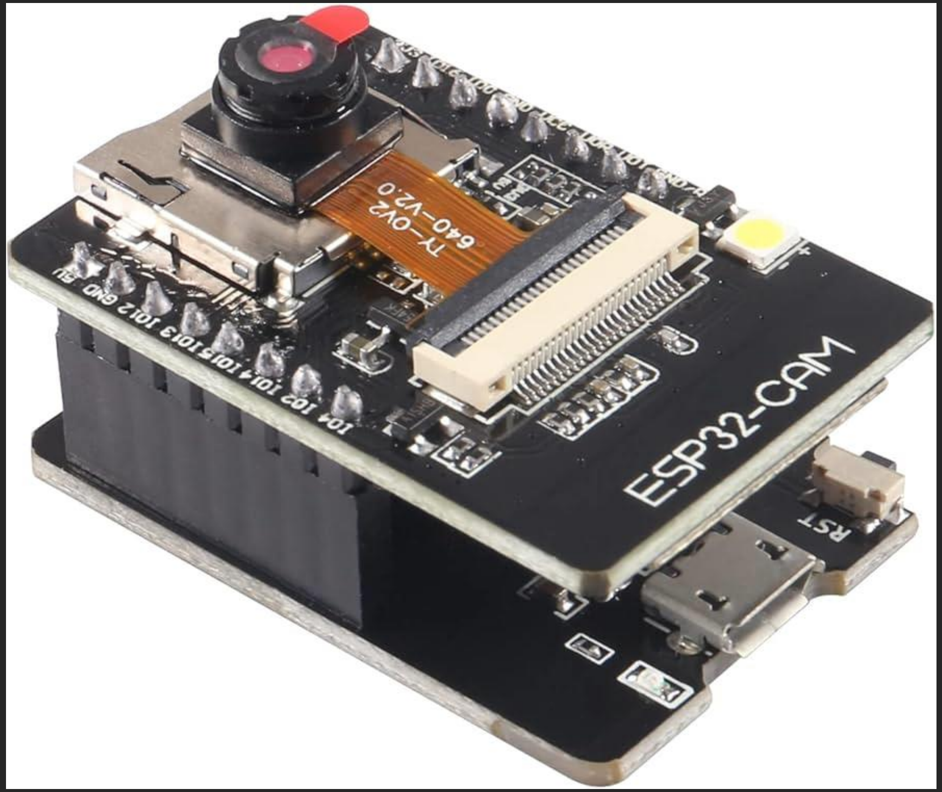


System Design Considerations

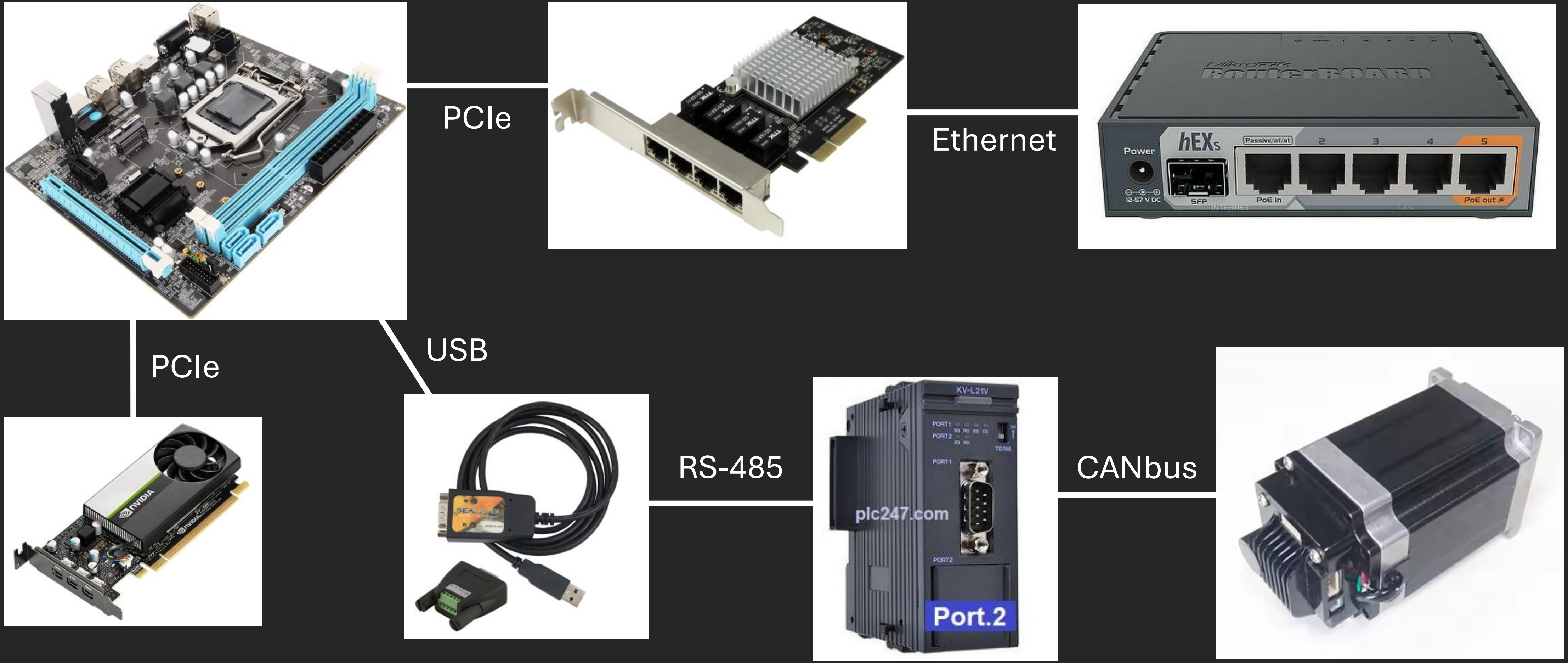


System Design Considerations





System Design Considerations



Wireless Communication

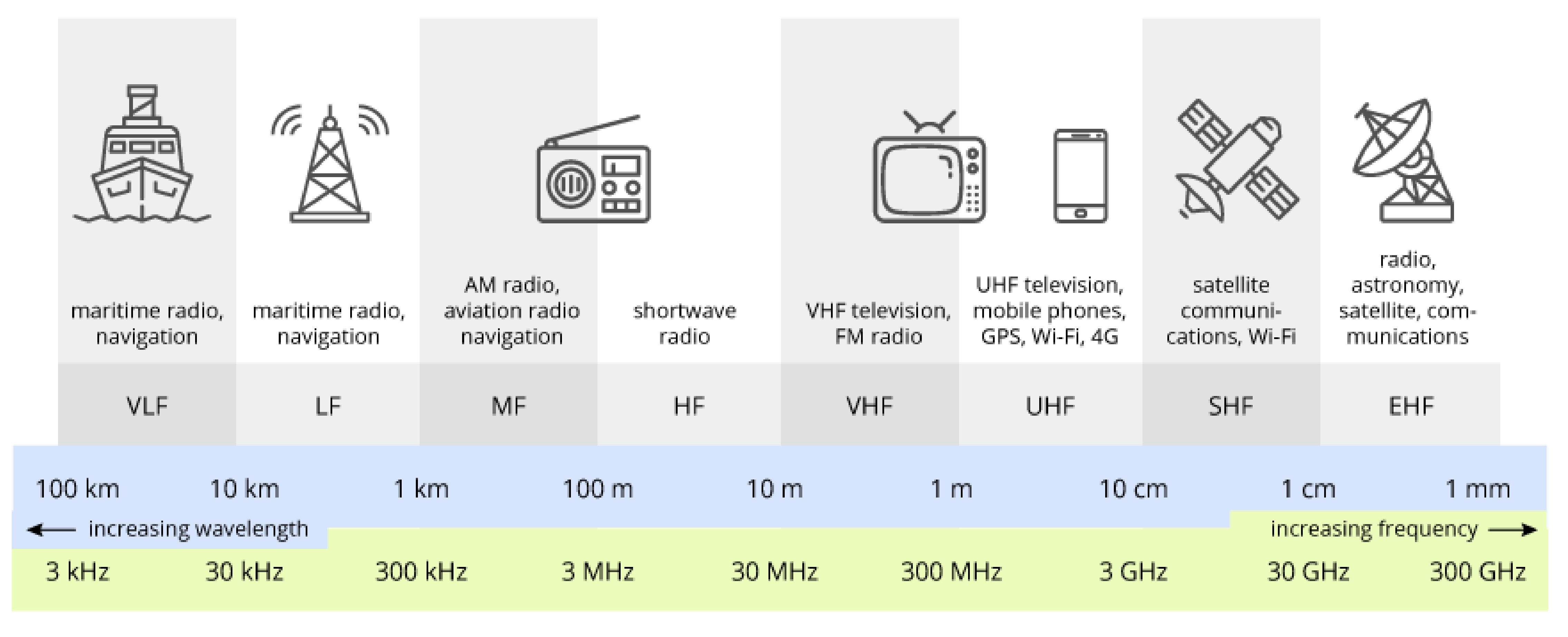
Wireless Communication Considerations

- Flexibility
  - No physical wiring, easy deployment and scalability
- Mobility
  - Connectivity even while in motion
- Diverse Range
  - Short to long distances
- Adaptability
  - Accommodates requirements such as low poser, high reliability, low latency, high throughput

Challenges of Wireless Communication

- Latency and Reliability
  - Applications require ultra-low latency and deterministic communication
- Interference
  - Crowded environments can degrade performance
- Security
  - Eavesdropping, spoofing, and other cyberattacks
- Power Consumption
  - Battery-operated devices require low-power protocols
- Bandwidth

Electromagnetic Frequency Band



International Telecommunications Union

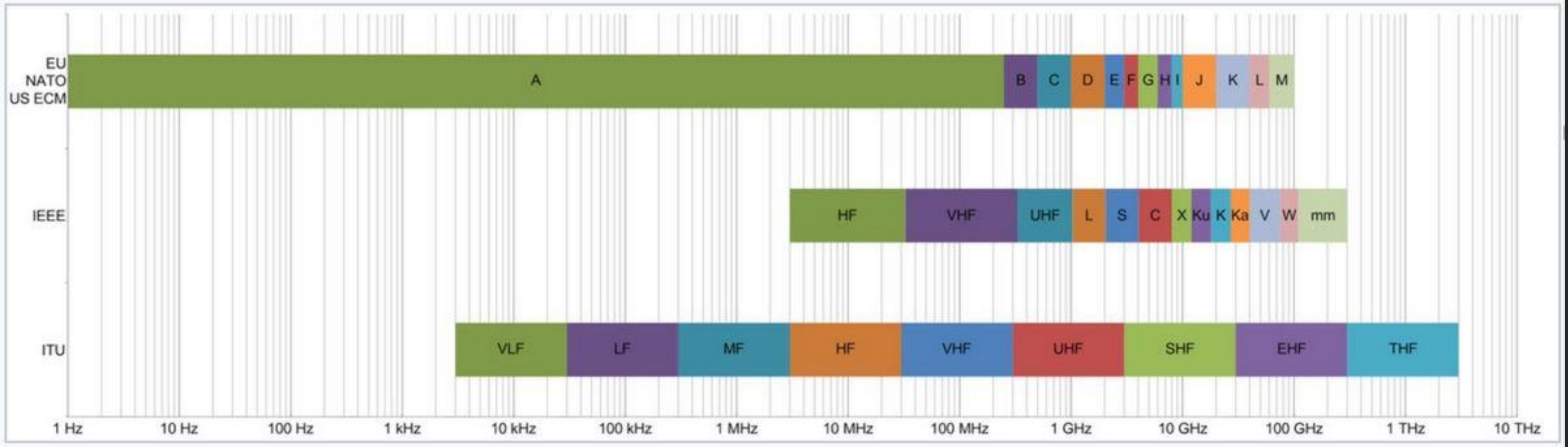
Band name	Abbreviation	ITU band number	Frequency	Wavelength	Example Uses
Extremely low frequency	ELF	1	3–30 Hz	100,000–10,000 km	Communication with submarines
Super low frequency	SLF	2	30–300 Hz	10,000–1,000 km	Communication with submarines
Ultra low frequency	ULF	3	300–3,000 Hz	1,000–100 km	Submarine communication, communication within mines
Very low frequency	VLF	4	3–30 kHz	100–10 km	Navigation, time signals, submarine communication, wireless heart rate monitors, geophysics
Low frequency	LF	5	30–300 kHz	10–1 km	Navigation, time signals, AM longwave broadcasting (Europe and parts of Asia), RFID, amateur radio
Medium frequency	MF	6	300–3,000 kHz	1,000–100 m	AM (medium-wave) broadcasts, amateur radio, avalanche beacons
High frequency	HF	7	3–30 MHz	100–10 m	Shortwave broadcasts, citizens band radio, amateur radio and over-the-horizon aviation communications, RFID, over-the-horizon radar, automatic link establishment (ALE) / near-vertical incidence skywave (NVIS) radio communications, marine and mobile radio telephony
Very high frequency	VHF	8	30–300 MHz	10–1 m	FM, television broadcasts, line-of-sight ground-to-aircraft and aircraft-to-aircraft communications, land mobile and maritime mobile communications, amateur radio, weather radio
Ultra high frequency	UHF	9	300–3,000 MHz	1–0.1 m	Television broadcasts, microwave oven, microwave devices/communications, radio astronomy, mobile phones, wireless LAN, Bluetooth, ZigBee, GPS and two-way radios such as land mobile, FRS and GMRS radios, amateur radio, satellite radio, Remote control Systems, ADSB
Super high frequency	SHF	10	3–30 GHz	100–10 mm	Radio astronomy, microwave devices/communications, wireless LAN, DSRC, most modern radars, communications satellites, cable and satellite television broadcasting, DBS, amateur radio, satellite radio
Extremely high frequency	EHF	11	30–300 GHz	10–1 mm	Radio astronomy, high-frequency microwave radio relay, microwave remote sensing, amateur radio,

IEEE Designation

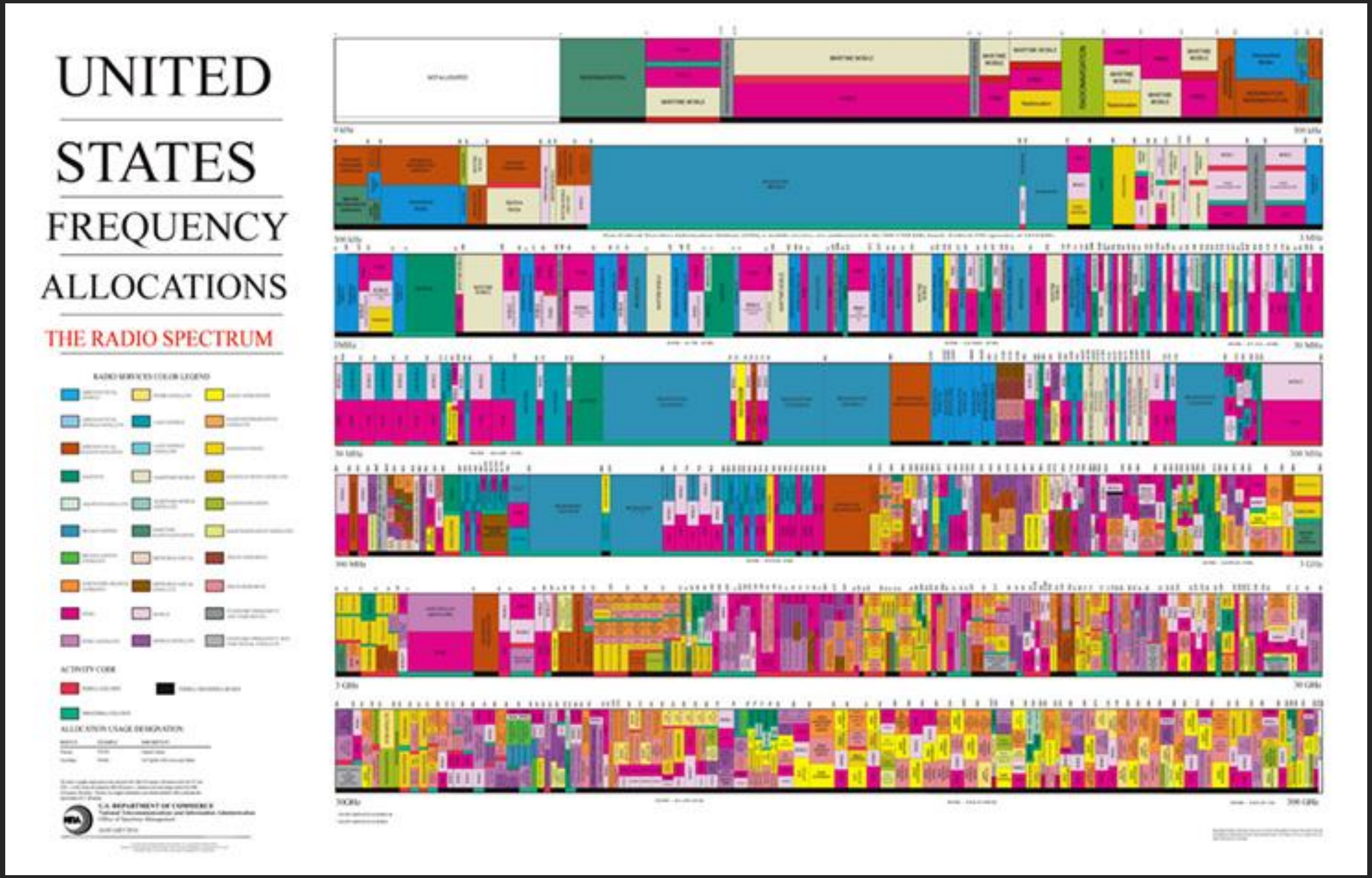
Band name	Abbreviation	ITU band number	Frequency	Wavelength	Example Uses
Extremely low frequency	ELF	1	3–30 Hz	100,000–10,000 km	Communication with submarines
Super low frequency	SLF	2	30–300 Hz	10,000–1,000 km	Communication with submarines
Ultra low frequency	ULF	3	300–3,000 Hz	1,000–100 km	Submarine communication, communication within mines
Very low frequency	VLF	4	3–30 kHz	100–10 km	Navigation, time signals, submarine communication, wireless heart rate monitors, geophysics
Low frequency	LF	5	30–300 kHz	10–1 km	Navigation, time signals, AM longwave broadcasting (Europe and parts of Asia), RFID, amateur radio
Medium frequency	MF	6	300–3,000 kHz	1,000–100 m	AM (medium-wave) broadcasts, amateur radio, avalanche beacons
High frequency	HF	7	3–30 MHz	100–10 m	Shortwave broadcasts, citizens band radio, amateur radio and over-the-horizon aviation communications, RFID, over-the-horizon radar, automatic link establishment (ALE) / near-vertical incidence skywave (NVIS) radio communications, marine and mobile radio telephony
Very high frequency	VHF	8	30–300 MHz	10–1 m	FM, television broadcasts, line-of-sight ground-to-aircraft and aircraft-to-aircraft communications, land mobile and maritime mobile communications, amateur radio, weather radio
Ultra high frequency	UHF	9	300–3,000 MHz	1–0.1 m	Television broadcasts, microwave oven, microwave devices/communications, radio astronomy, mobile phones, wireless LAN, Bluetooth, ZigBee, GPS and two-way radios such as land mobile, FRS and GMRS radios, amateur radio, satellite radio, Remote control Systems, ADSB
Super high frequency	SHF	10	3–30 GHz	100–10 mm	Radio astronomy, microwave devices/communications, wireless LAN, DSRC, most modern radars, communications satellites, cable and satellite television broadcasting, DBS, amateur radio, satellite radio
Extremely high frequency	EHF	11	30–300 GHz	10–1 mm	Radio astronomy, high-frequency microwave radio relay, microwave remote sensing, amateur radio,

Band designation	Frequency range	Explanation of meaning of letters
HF	0.003 to 0.03 GHz	High Frequency
VHF	0.03 to 0.3 GHz	Very High Frequency
UHF	0.3 to 1 GHz	Ultra High Frequency
L	1 to 2 GHz	Long wave
S	2 to 4 GHz	Short wave
C	4 to 8 GHz	Compromise between S and X
X	8 to 12 GHz	Used in WW II for fire control, X for cross (as in crosshair). Exotic.
Ku	12 to 18 GHz	Kurz-under
K	18 to 27 GHz	Kurz (German for "short")
Ka	27 to 40 GHz	Kurz-above
V	40 to 75 GHz	
W	75 to 110 GHz	W follows V in the alphabet
mm or G	110 to 300 GHz	Millimeter

Conventions



Frequency Allocations



Design Considerations

Higher frequencies

- Higher data throughput - faster communication speeds
- More energy required
- Shorter range - best for line of sight
- Smaller antennas
- Less congestions

Lower frequencies

- Lower data throughput
- Less energy required
- Longer range – more diffraction
- Obstacle penetration
- Operates better in harsh conditions
- More congestion

Frequency Band	Frequency Range	Licensed/ Unlicensed	Common Applications	Key Design Considerations
Low Frequency (LF)	30-300 kHz	Licensed	Subsurface communications, RFID, long-distance telemetry	Long range, low data rate, susceptible to noise, good penetration in water and ground
High Frequency (HF)	3-30 MHz	Licensed	Long-range telemetry, maritime/aviation communication	Ionospheric reflection enables long distances, low data rate
Very High Frequency (VHF)	30-300 MHz	Licensed	Industrial automation, TV and radio broadcasts	Good range, requires minimal line of sight, interference-prone
Ultra High Frequency (UHF)	300 MHz - 3 GHz	Mixed (depends on application)	IoT (Zigbee, LPWAN), RFID, cellular (4G/5G), Wi-Fi (2.4 GHz)	Short-medium range, higher data rates, obstacle attenuation becomes significant
Industrial, Scientific, and Medical (ISM) - Sub-GHz	433 MHz, 868 MHz (EU), 915 MHz (US)	Unlicensed (region-specific)	LoRaWAN, LPWAN, Zigbee, low-power sensor networks	Long range, low power, good penetration through obstacles, may face interference
2.4 GHz ISM Band	2.4-2.5 GHz	Unlicensed	Wi-Fi (802.11b/g/n), Bluetooth, Zigbee, drones, consumer IoT	High interference (congested band), moderate range, supports high data rates
5 GHz ISM Band	5.15-5.825 GHz	Unlicensed	Wi-Fi (802.11ac/ax), high-speed wireless communication	Shorter range than 2.4 GHz, less interference, high throughput
Cellular Bands (3G/4G/5G)	600 MHz - 6 GHz (region-specific)	Licensed	Mobile networks, autonomous vehicles, smart grids	Guaranteed QoS, medium to long range, high reliability, costly spectrum licensing
Millimeter-wave (mmWave)	24-30 GHz, 60 GHz, 77 GHz	Licensed/ Unlicensed	5G ultra-fast links, radar (automotive), high-bandwidth sensing	Very high data rates, short range, requires line of sight, affected by atmospheric absorption
60 GHz (V-band)	57-64 GHz	Unlicensed (region-specific)	High-speed indoor wireless links, ultra-fast IoT	Line of sight critical, very high data rate, low interference but range-limited
77 GHz (Automotive Radar)	76-81 GHz	Licensed	Advanced driver assistance systems (ADAS), collision detection	High resolution sensing, short range, high susceptibility to atmospheric attenuation
Sub-Terahertz (THz)	100 GHz - 1 THz	Emerging (experimental)	High-resolution imaging, future high-speed wireless	Experimental, short-range communication, atmospheric absorption challenges

Multiple Access Techniques

- Frequency Division Multiple Access (FDMA)
  - Divide a band into smaller bands with no interference between sub-bands
- Time Division Multiple Access (TDMA)
  - Communication channel is divided into time slots
- Code Division Multiple Access (CDMA)
  - Each uses is assigned a unique orthogonal code
  - All users transmit using the same frequency, signal is decoded
- Orthogonal Frequency Division Multiple Access (OFDMA)
  - Frequency is divided into orthogonal subcarriers

Multiple Access Techniques

Technique	Resource Division	Efficiency	Synchronization	Complexity	Key Applications
FDMA	Frequency	Moderate (wastes bandwidth due to guard bands)	Low	Low	Early cellular networks, satellite
TDMA	Time	Higher than FDMA (but requires overhead for synchronization)	High (precise time control)	Medium	GSM (2G), satellite, private radio
CDMA	Code (spread spectrum)	High (can degrade if many users share spectrum)	Low-moderate	High	3G networks, GPS, military comms
OFDMA	Frequency + Time (subcarriers)	Very high (dynamic allocation, minimal interference)	High	High	4G LTE, 5G, Wi-Fi 6

Modulation

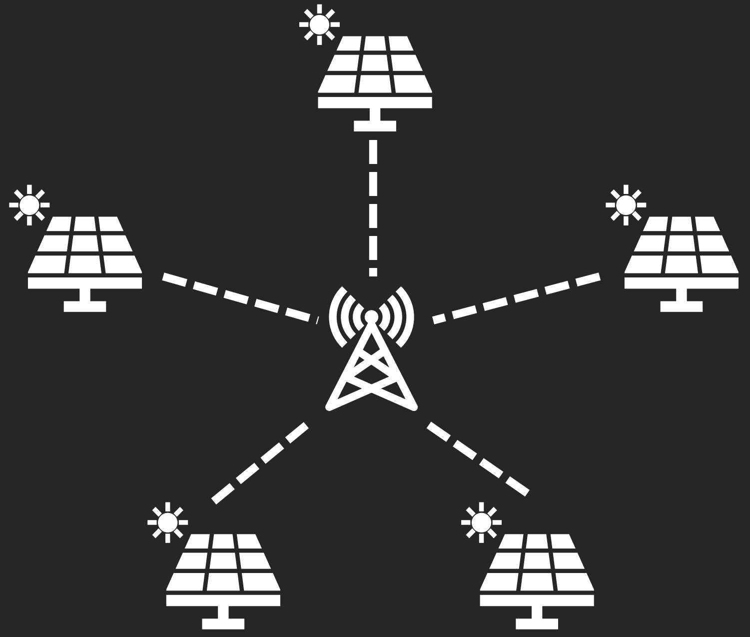
- Amplitude Modulation
- Frequency Modulation
- Phase Shift Keying
  - Binary phase shift keying
  - Quadrature Phase shift keying
- Quadrature Amplitude Modulation
  - Amplitude and Phase are modulated
  - 16 symbol (4 bits per symbol) and 64 symbol (6 bits per symbol) QAM
- Baud rate vs bit rate

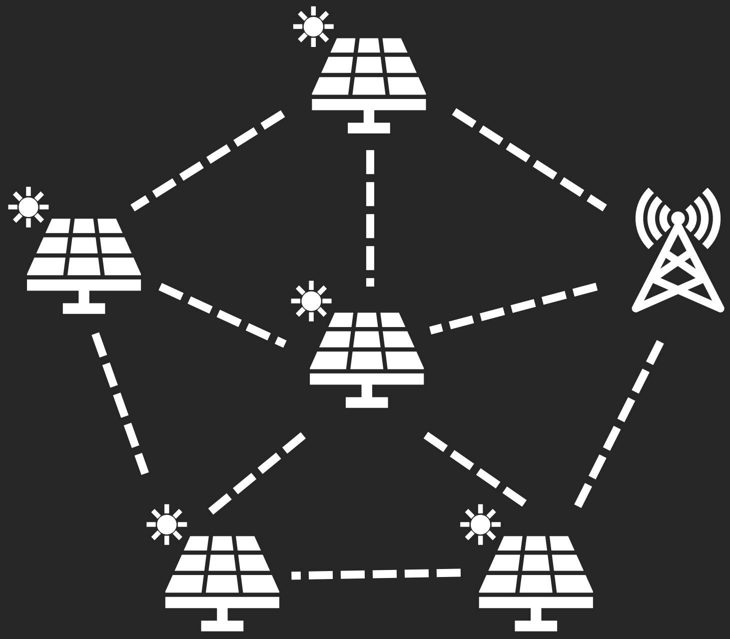
Antennas

- Omnidirectional Antenna
  - 360 degree – low range, wide coverages
  - Wifi routers, cell towers
- Directional Antenna
  - Concentrate power in a single direction, point to point
  - Radar, satellite uplinks
- Patch Antenna
  - Radiates in one direction with a wide beam
  - Wireless devices, GPS, drones

Topology

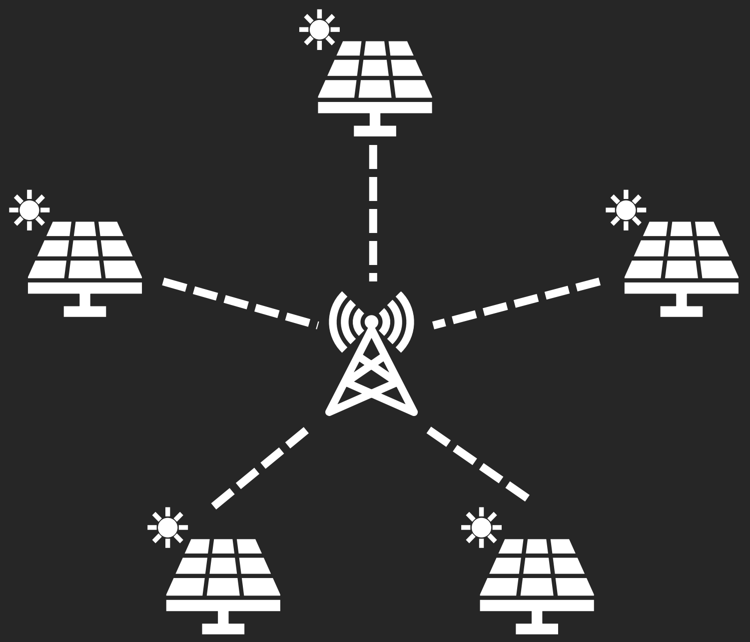
- Star – all devices connected to centralized node
- Mesh – all devices connected to all other devices (within range)

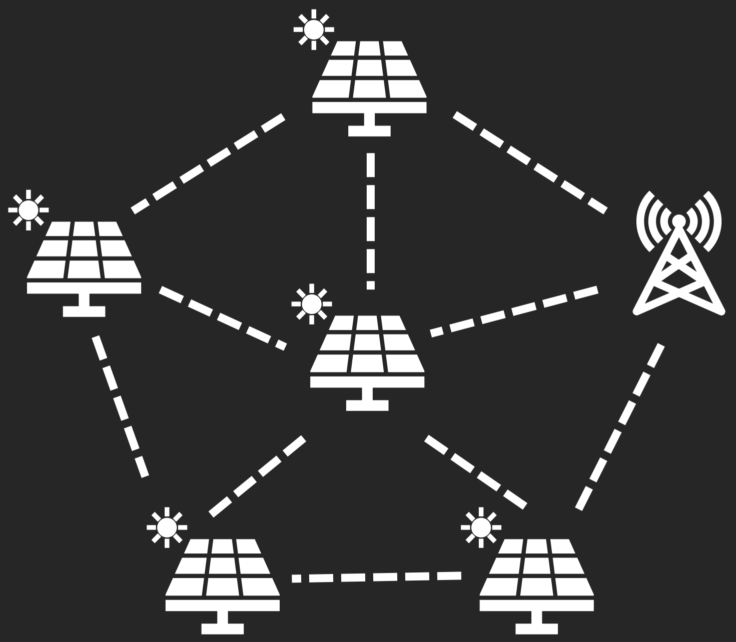




Topology

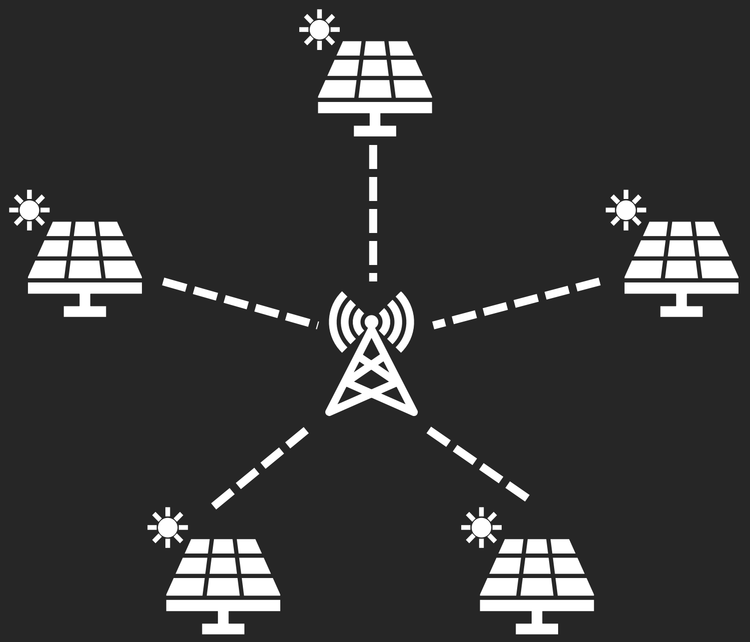
- Star – Simpler, cheaper, each device supports a single connection
- Mesh – More robust, adaptable, expandable range

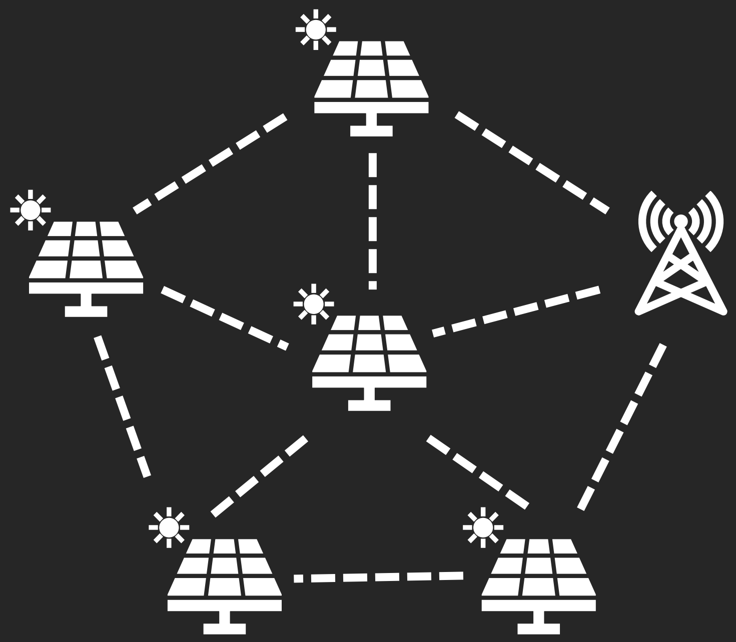




Topology

- Star – Single point of failure, expensive base station infrastructure
- Mesh – Expensive, complex device hardware





Wireless Communication Protocols

- Bluetooth
- Wifi
- Smart-home Protocols
- Cellular
- Low-Power Wide Area Networks
- Radio Frequency ID

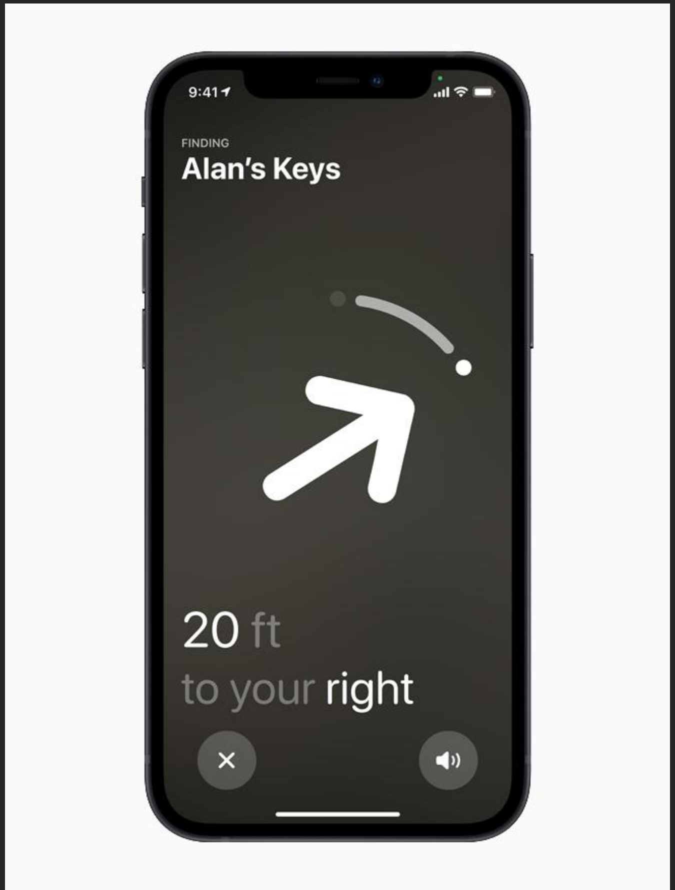
Bluetooth

- 2.4 GHz with typical range of 10m but can be extended to 100m
- Bandwidth of 1-2 Mbps
- Versions
  - 2.0+: wireless headphones, keyboards, mice
  - 4.0 BLE: ultra low power consumption (fitness devices, battery powered)
  - 5.0: mesh network, enhanced coexistence, extended range and bandwidth
  - 5.1 & 5.2: direction finding
- Bluetooth Profiles for specific applications
- Bluetooth Special Interest Group define standards

Bluetooth


SONY


RGBCW
7W
MESH


9:41
FINDING
Alan's Keys
20 ft
to your right


Friencity
Power PC OBD
OBD
CHECK
Fault Codes
Realtime Information
Bluetooth OBD Scanner

Wifi

- 2.4 GHz, 5 GHz, 6 GHz
- Bandwidth of 11 Mbps up to 9.6 Gbps
- Versions
  - Wifi 4 (2009): 2.4 and 5 GHz, 600 Mbps (MIMO)
  - Wifi 5 (2014): 5 GHz, beamforming, mesh
  - Wifi 6 (2019): 2.4 and 5 GHz, Orthogonal Frequency-Division Multiple Access and Target Wake Time for efficiency in dense environments
- Bluetooth Profiles for specific applications

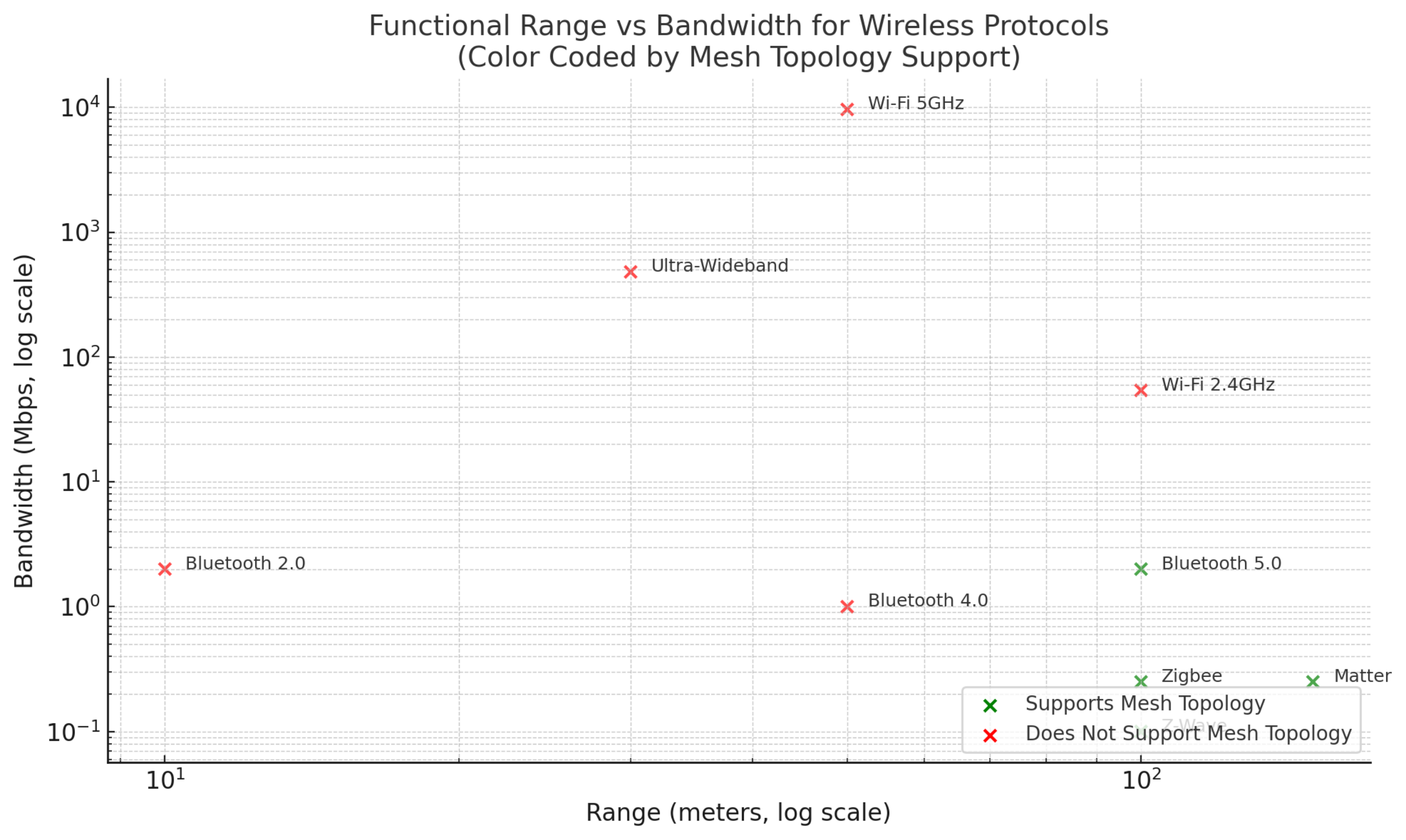
Wifi

Smart-Home Protocols

- Low-power, mesh topology, 10-100m range

- Zigbee – 2.4 GHz, 250 kbps
  - Open standard, supports up to 65,000 devices
- Z-Wave – Sub-GHz band, 100 kbps
  - Less interference, highly standardized, good interoperability, proprietary
- Matter – Uses Wifi, Thread, Ethernet
  - Easily interactable, adaptable depending on protocol

Range vs Bandwidth



Cellular

- 5G – Low latency, up to 10Gbps, large-scale deployment (1 million devices per km^2)
  - Real time, dense, high data throughput
- 4G – 30-50ms latency, 10-100Mbps, excellent coverage
  - Rural deployment, monitoring and control
- Cellular V2X
  - Direct – Communication between vehicles
  - Network-based – Centralized communication with cellular towers
  - Supports vehicle to vehicle, infrastructure, pedestrian, network, etc.

Cellular


10
36 AM
08/16
WED


12:00 PM
Get the latest weather updates!
Configure now

Low-Power Wide Area Networks (LPWAN)

- Base stations or cellular towers, ultra-low power, very-low bandwidth, excellent range, poor mobility

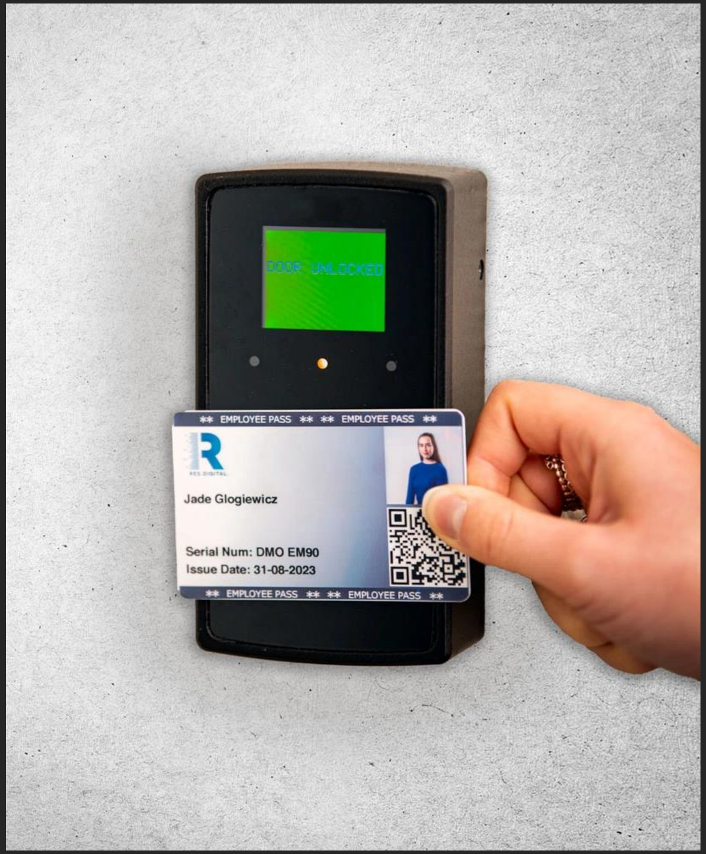
- Sigfox – Proprietary tower network
  - 50km range, 100 bps
- LoRaWAN – open standard, private or public towers
  - 15km range, 0.3-50 kbps
- NB-IoT – cellular-based (LTE)
  - LTE coverage, 250kbps, SIM card

Low-Power Wide Area Networks (LPWAN)


Radio Frequency ID

Frequency Band	Range	Data Rate	Penetration	Applications in CPS
Low-Frequency (LF)	10 cm to 1 meter	Low	Strong penetration through materials	Access control, livestock tracking, industrial automation
High-Frequency (HF)	10 cm to 1.5 meters	Moderate	Good but affected by metals/water	Smart cards, inventory tracking, healthcare
Ultra-High Frequency (UHF)	Up to 12 meters (passive) / 100 meters (active)	High	Affected by metals/water but suitable for long-range tracking	Supply chain, logistics, vehicle tracking
Microwave RFID	Up to 30 meters	Very High	Susceptible to interference	Real-time location systems (RTLS), high-value asset tracking

Radio Frequency ID



Networks

Open Systems Interconnection

OSI is a reference model from the International Organization of Standardization (ISO)

"Provides a common basis for the coordination of standards development for the purpose of systems interconnection."

ISO/IEC 7498-1:1994 Information technology — Open Systems Interconnection — Basic Reference Model: The Basic Model. June 1999. Introduction. Retrieved 26 August 2022.

Communication Architectures

- Application
- Presentation
- Session
- Transport
- Network
- Data Link
- Physical

Communication Architectures

Application	
Presentation	
Session	
Transport	
Network	
Data Link	
Physical	• Physical layer responsible for connection between devices • Controls transmission and reception of raw bits

Communication Architectures

Application	
Presentation	
Session	
Transport	
Network	
Data Link	• Establishes, maintains, and decides how data is transferred between devices on a network • Controls framing, MAC, error detection/correction, and flow control
Physical	• Physical layer responsible for connection between devices • Controls transmission and reception of raw bits

Communication Architectures

Application	
Presentation	
Session	
Transport	
Network	• Determines the best path to travel from source to destination via logical addressing and routing • Controls IP addressing, packet fragmentation and reassembly, routing and forwarding
Data Link	• Establishes, maintains, and decides how data is transferred between devices on a network • Controls framing, MAC, error detection/correction, and flow control
Physical	• Physical layer responsible for connection between devices • Controls transmission and reception of raw bits

Communication Architectures

Application	
Presentation	
Session	
Transport	• Ensures reliable data transfer between devices and segmentation of data for easier transmission • Provides end-to-end connection management, error recovery, flow control, and data integrity
Network	• Determines the best path to travel from source to destination via logical addressing and routing • Controls IP addressing, packet fragmentation and reassembly, routing and forwarding
Data Link	• Establishes, maintains, and decides how data is transferred between devices on a network • Controls framing, MAC, error detection/correction, and flow control
Physical	• Physical layer responsible for connection between devices • Controls transmission and reception of raw bits

Communication Architectures

Application	
Presentation	
Session	• Establishes, manages, and terminates communication sessions between applications • Handles dialog control, allowing multiple applications to communicate over a network
Transport	• Ensures reliable data transfer between devices and segmentation of data for easier transmission • Provides end-to-end connection management, error recovery, flow control, and data integrity
Network	• Determines the best path to travel from source to destination via logical addressing and routing • Controls IP addressing, packet fragmentation and reassembly, routing and forwarding
Data Link	• Establishes, maintains, and decides how data is transferred between devices on a network • Controls framing, MAC, error detection/correction, and flow control
Physical	• Physical layer responsible for connection between devices • Controls transmission and reception of raw bits

Communication Architectures

Application	
Presentation	• Translates data between application layer and network, ensuring compatibility • Data compression/decompression, encryption/decryption, format translation and binary encoding
Session	• Establishes, manages, and terminates communication sessions between applications • Handles dialog control, allowing multiple applications to communicate over a network
Transport	• Ensures reliable data transfer between devices and segmentation of data for easier transmission • Provides end-to-end connection management, error recovery, flow control, and data integrity
Network	• Determines the best path to travel from source to destination via logical addressing and routing • Controls IP addressing, packet fragmentation and reassembly, routing and forwarding
Data Link	• Establishes, maintains, and decides how data is transferred between devices on a network • Controls framing, MAC, error detection/correction, and flow control
Physical	• Physical layer responsible for connection between devices • Controls transmission and reception of raw bits

Communication Architectures

Layer	Description
Application	• Provides network services directly to applications and handles high-level protocols for data transfer • Responsible for user interfaces such as email, file transfer, and web browsing
Presentation	• Translates data between application layer and network, ensuring compatibility • Data compression/decompression, encryption/decryption, format translation and binary encoding
Session	• Establishes, manages, and terminates communication sessions between applications • Handles dialog control, allowing multiple applications to communicate over a network
Transport	• Ensures reliable data transfer between devices and segmentation of data for easier transmission • Provides end-to-end connection management, error recovery, flow control, and data integrity
Network	• Determines the best path to travel from source to destination via logical addressing and routing • Controls IP addressing, packet fragmentation and reassembly, routing and forwarding
Data Link	• Establishes, maintains, and decides how data is transferred between devices on a network • Controls framing, MAC, error detection/correction, and flow control
Physical	• Physical layer responsible for connection between devices • Controls transmission and reception of raw bits

Communication Architectures

- Application
- Presentation
- Session
- Transport
- Network
- Data Link
- Physical

Abstract
Easier to use
Functionality

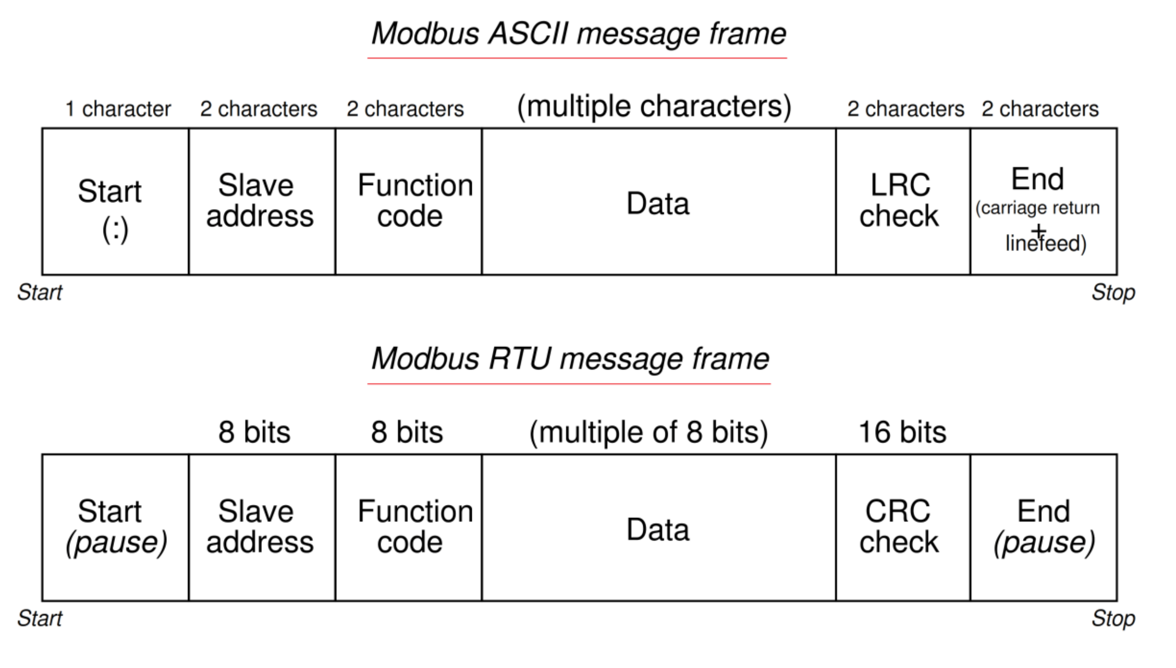
Simpler
Hardware Specific
Less Features

Communication Architectures

Application	• HTML, SCP, SSH, SMTP, DNS, FTP
Presentation	• SSL/TLS, JPEG, GIF, MPEG
Session	• SMB (server message block), NetBIOS, RPC (remote procedure call)
Transport	• TCP (transmission control protocol), UDP (user datagram protocol)
Network	• IP (internet protocol), ICMP (internet control message protocol), routers
Data Link	• Ethernet, MAC addressing, Wi-fi, Bluetooth, UART
Physical	• Radio wave, cables, fiberoptic, transistor logic

Example - Modbus

- Modbus RTU: Serial Communication (RS-485)
  - Datalink layer for framing and physical layer (RS-485) for serial communication



Example - Modbus

- Modbus RTU: Serial Communication (RS-485)
  - Datalink layer for framing and physical layer (RS-485) for serial communication
- Modbus TCP/IP: Ethernet Based
  - Application layer (data structure), Transport layer (TCP), Network Layer (IP), Datalink layer (ethernet)
  - What is the physical layer?

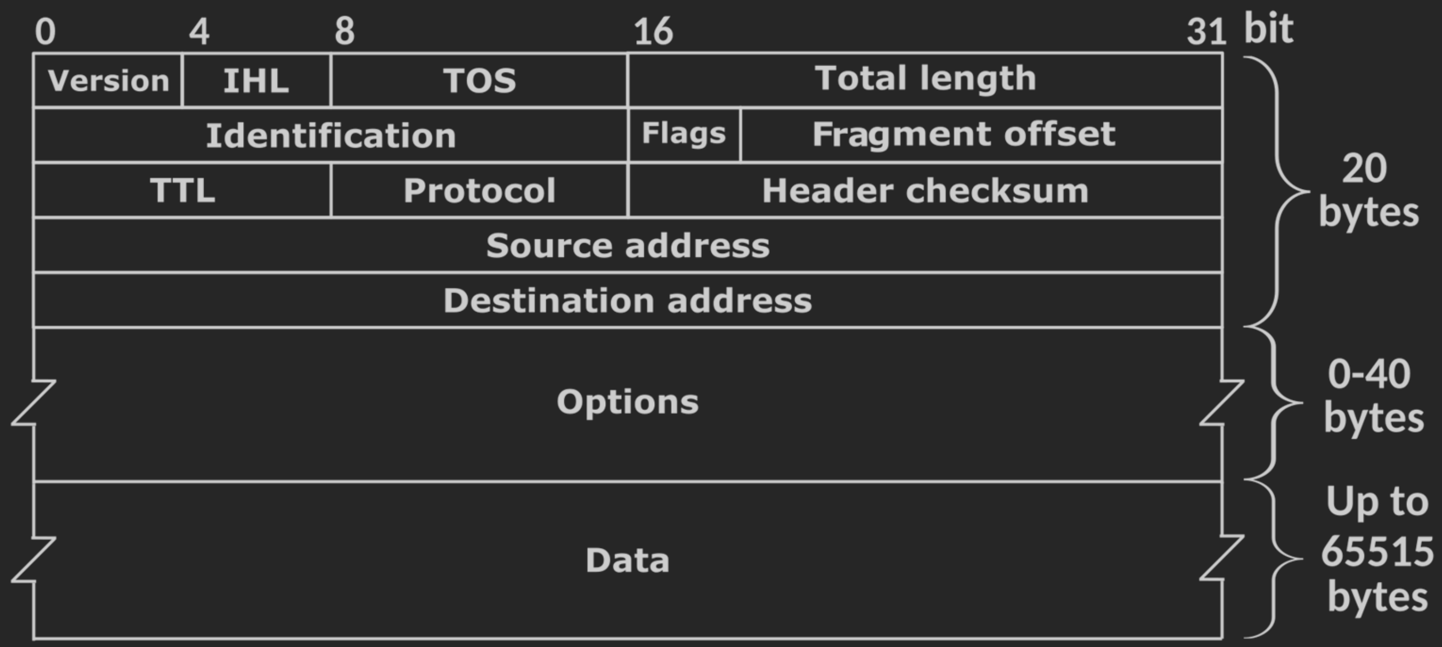
Data Frame

- Definition – Unit of data in the Data Link Layer (layer 2)
- Components
  - Header – source/destination MAC addresses, other transmission info
  - Payload – Variable length, contains “packets”
  - Frame Check Sequence (FCS) – cyclic redundancy check

2	2	6	6	6	0 or 2	6	0 or 2	0 or 4	0 - 2312	4
Frame Control	Duration /ID	Address 1	Address 2	Address 3	Sequence Control	Address 4	QoS Control	HT Control	Frame Body	FCS

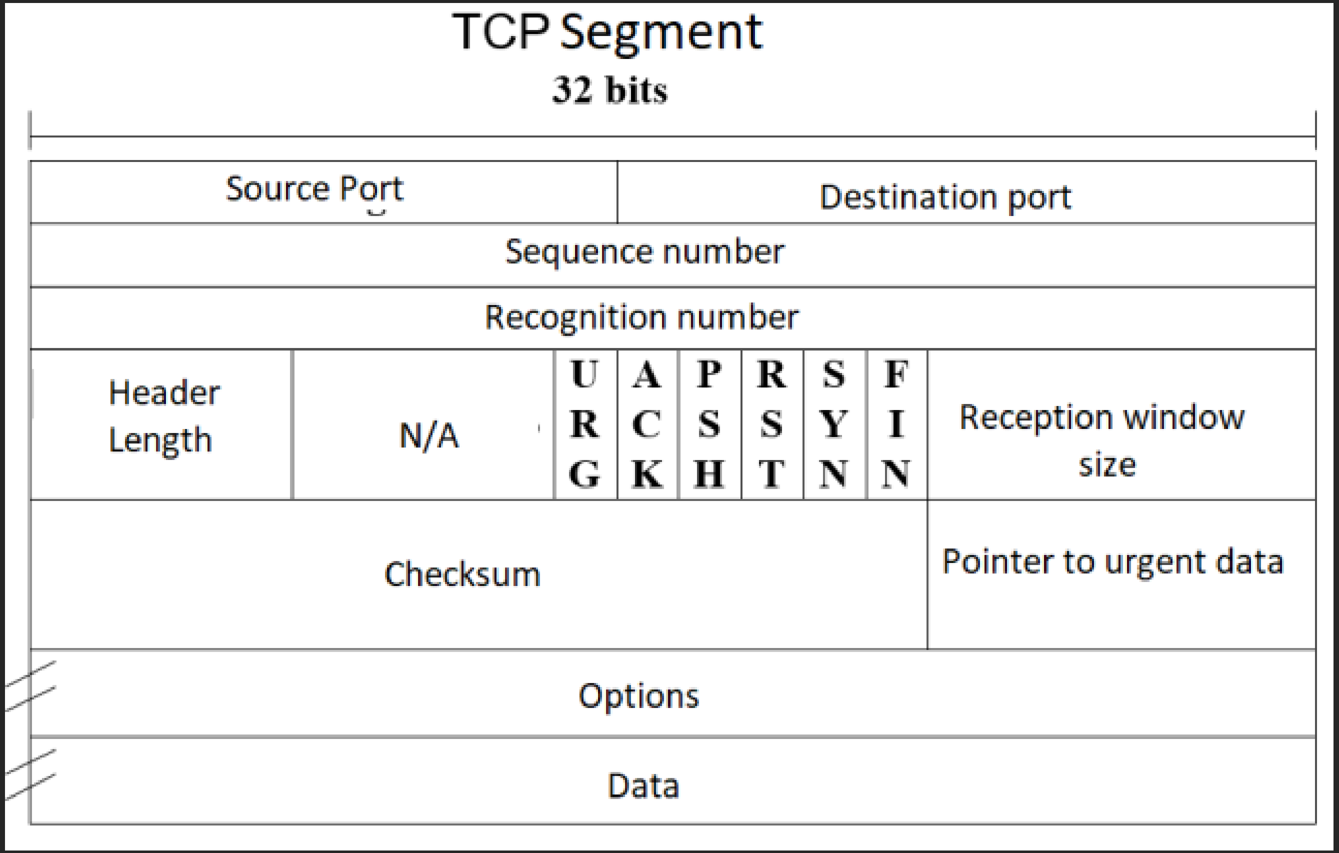
Data Packet

- Definition – Unit of data in the Network Layer (layer 3)
- Components
  - Header – source/destination IP addresses, other transmission info
  - Payload – Variable length, contains “segments” or “datagrams”



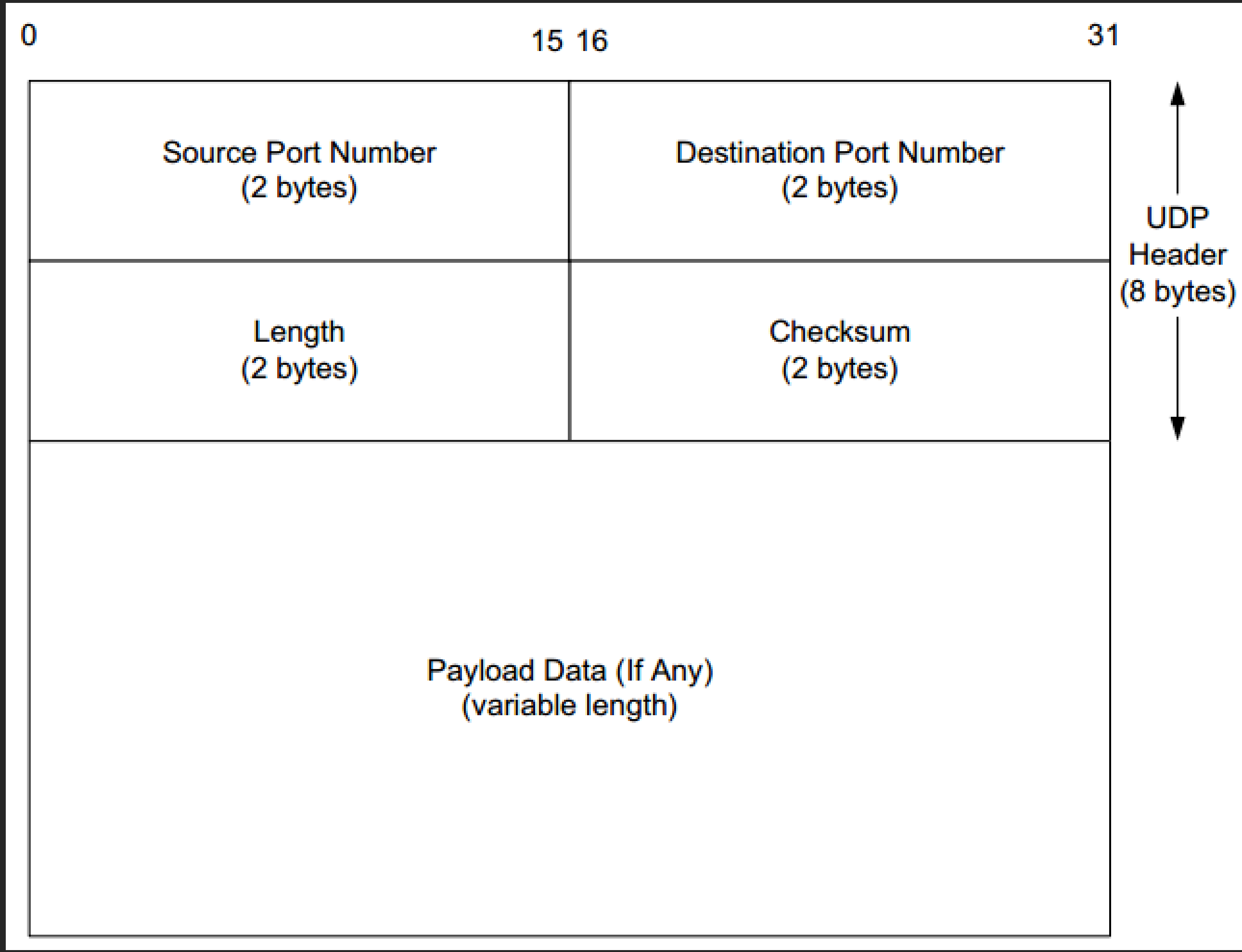
TCP Segment

- Definition – Unit of data in the Transport Layer (layer 4)
- Components
  - Header – source/destination port addresses, other transmission info
  - Payload – Variable length, contains data generated in higher layers



UDP Datagram

- Definition – Unit of data in the Transport Layer (layer 4)
- Components
  - Header – source/destination port addresses, length, checksum
  - Payload – Variable length, contains data generated in higher layers



Example – Accessing a Website

Application	• Provides network services directly to applications and handles high-level protocols for data transfer • Responsible for user interfaces such as email, file transfer, and web browsing
Presentation	• Translates data between application layer and network, ensuring compatibility • Data compression/decompression, encryption/decryption, format translation and binary encoding
Session	• Establishes, manages, and terminates communication sessions between applications • Handles dialog control, allowing multiple applications to communicate over a network
Transport	• Ensures reliable data transfer between devices and segmentation of data for easier transmission • Provides end-to-end connection management, error recovery, flow control, and data integrity
Network	• Determines the best path to travel from source to destination via logical addressing and routing • Controls IP addressing, packet fragmentation and reassembly, routing and forwarding
Data Link	• Establishes, maintains, and decides how data is transferred between devices on a network • Controls framing, MAC, error detection/correction, and flow control
Physical	• Physical layer responsible for connection between devices • Controls transmission and reception of raw bits

Layer 7 – Application Layer

- User types www.example.com into their web browser
- Chrome/Safari generates an HTTPS request for the webpage

Layer 6 – Presentation Layer

- Text is formatted using HTML, images and video compressed.
- Data is encrypted as needed

Layer 5 – Session Layer

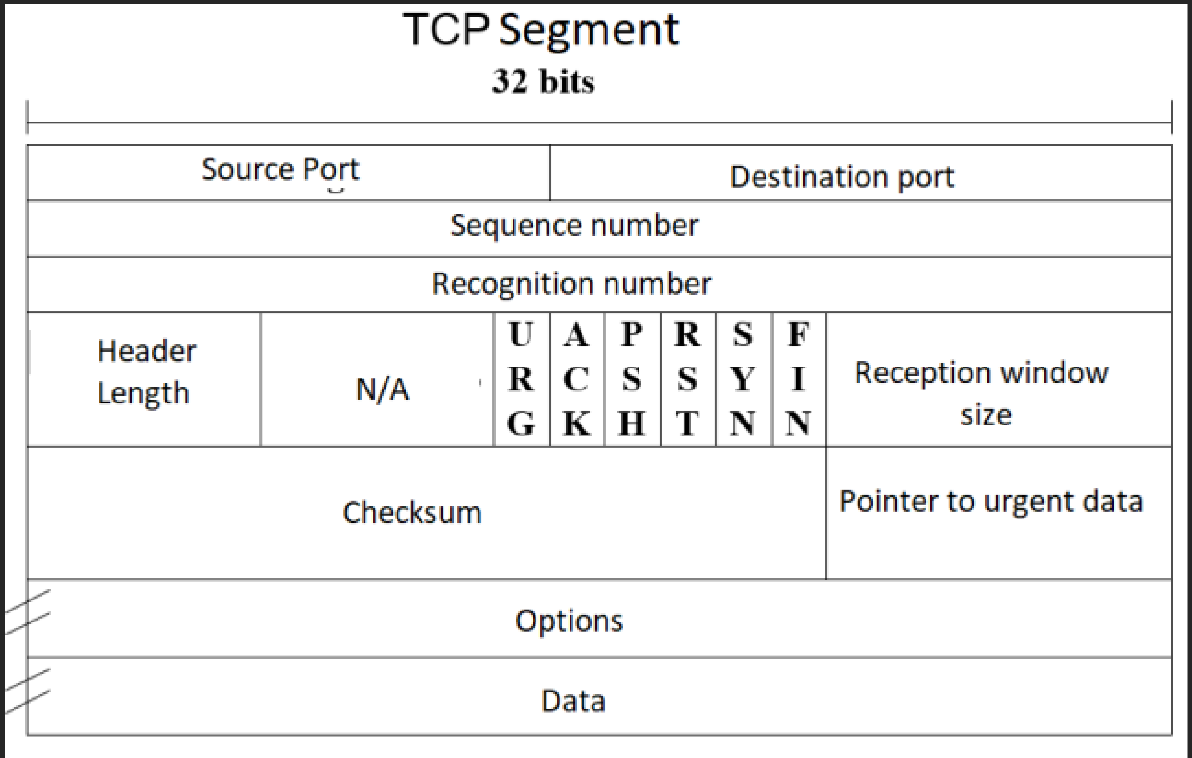
- A session is established, allowing for continuous interactions
  - Butten presses
  - Text boxes

Layer 4 – Transport Layer

- Data is broken into smaller segments
- Transport Control Protocol (TCP) is used for errors and reliability checks
- Specifies port
- Three-way handshake
    - Device sends a synchronization request
    - The sever acknowledges
    - Your device confirms and the connection is established

Layer 4 – Transport Layer

- Segments of encrypted HTML data go into the “Data” field of the TCP packet



Layer 3 – Network Layer

- Handles converting domain names to IP addresses
- Handles Network Address Translation (NAT)
- IPv4 address shortages
- Switches IP address by using ports
  - TCP message 192.10.143.17:50000 -> www.example.com
  - Gateway device will readdress 203.10.45.11:60000 -> www.example.com
  - Upon response it readdress the response by checking the NAT

Layer 2 – Datalink Layer

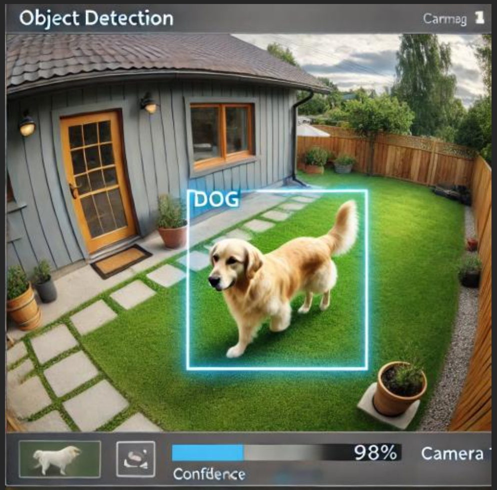
- TCP Packet is placed inside of a data frame and sent to the correct machine
- MAC address is used to identify machine
- Wifi uses frames defined by IEEE 802.11
- Ethernet uses frames defined by IEEE 802.3

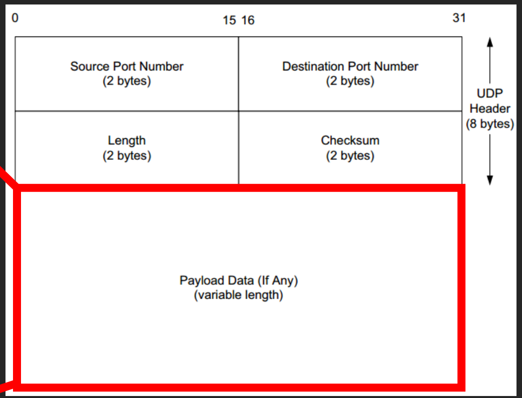
Layer 1 – Physical Layer

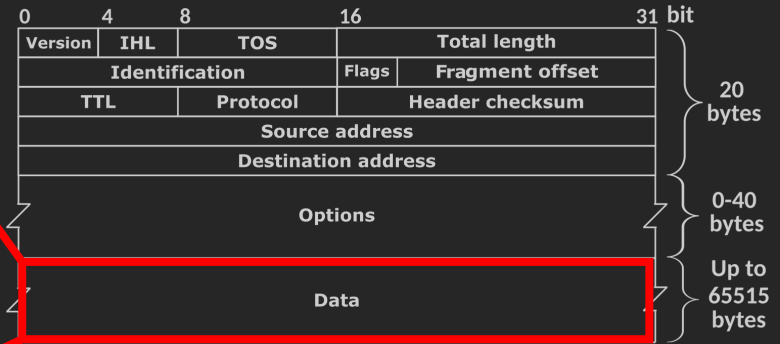
- Radio waves or electrical voltages are used to transmit the signal between machines

Abstraction

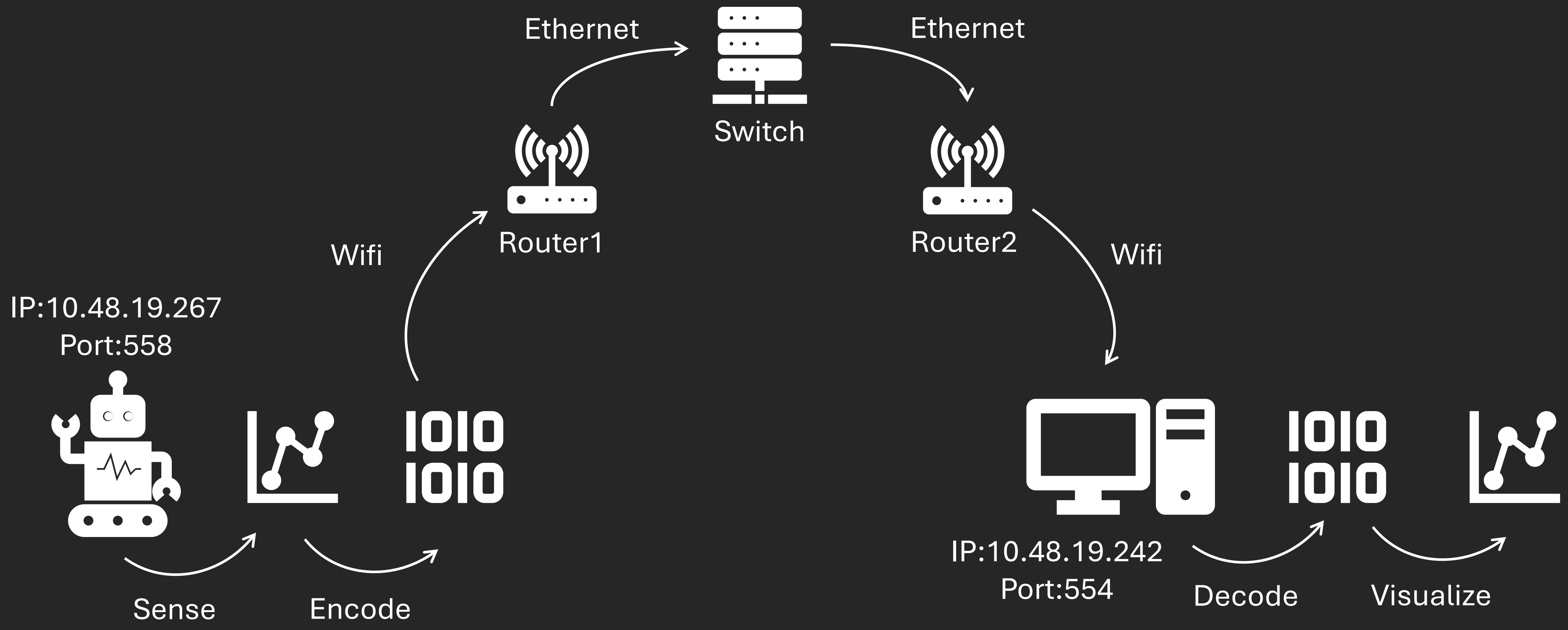
Frame Control	Duration /ID	Address 1	Address 2	Address 3	Sequence Control	Address 4	QoS Control	HT Control	Frame Body	FCS
2	2	6	6	6	0 or 2	6	0 or 2	0 or 4	0 - 2312	4



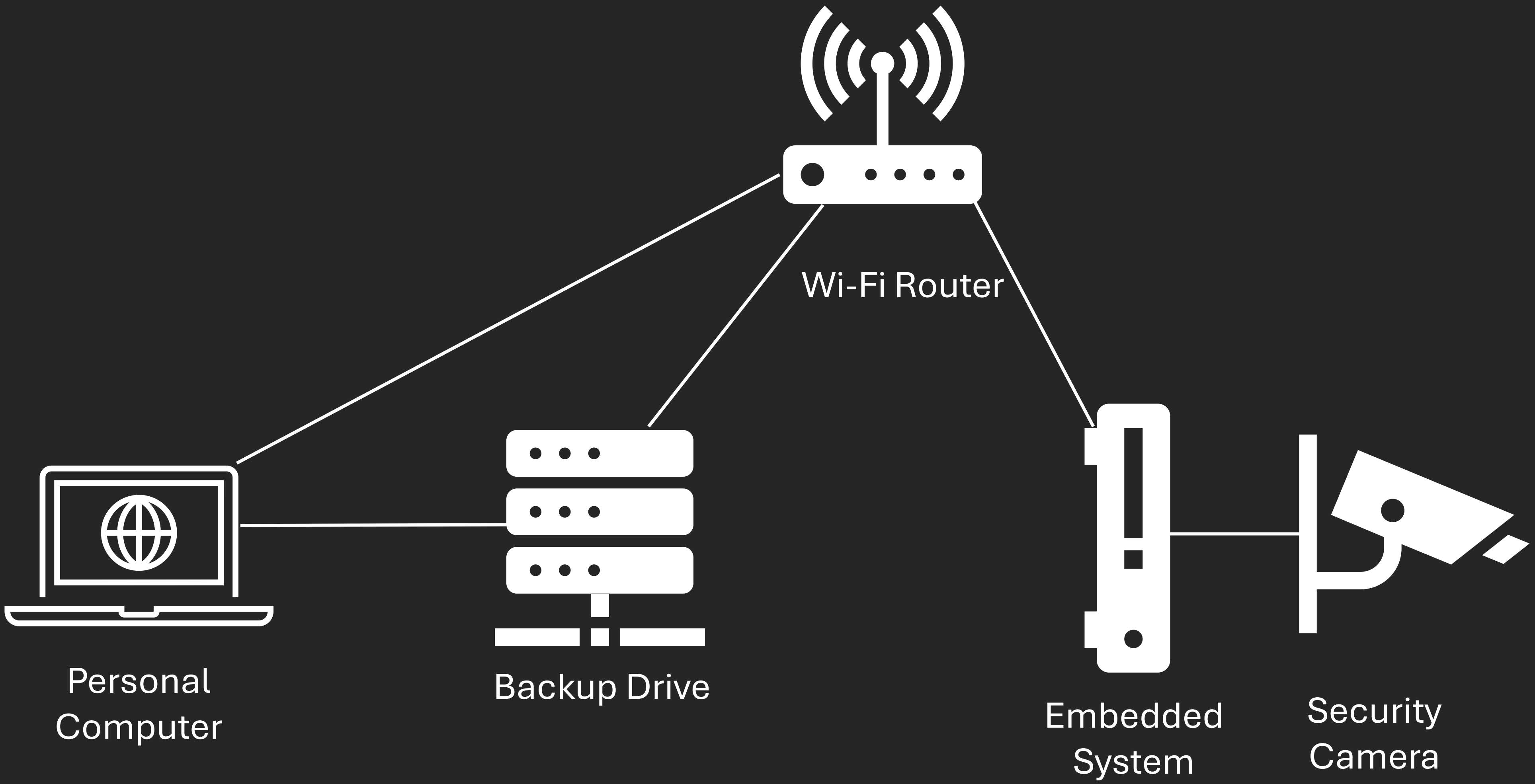




Abstraction

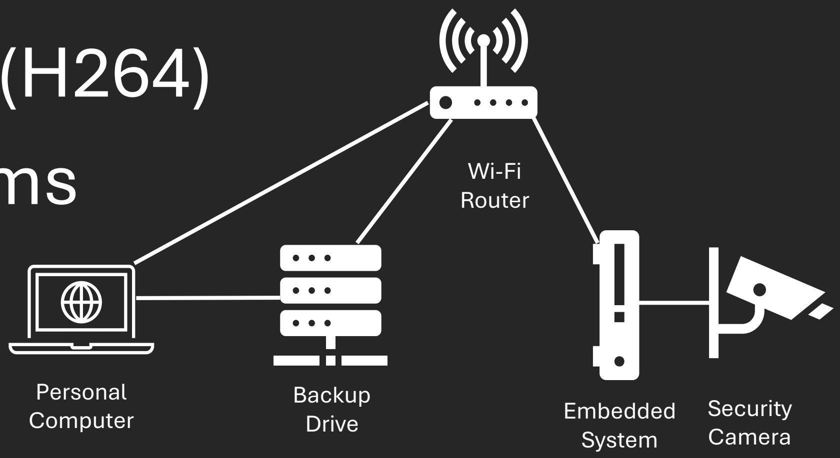


Communication Architectures



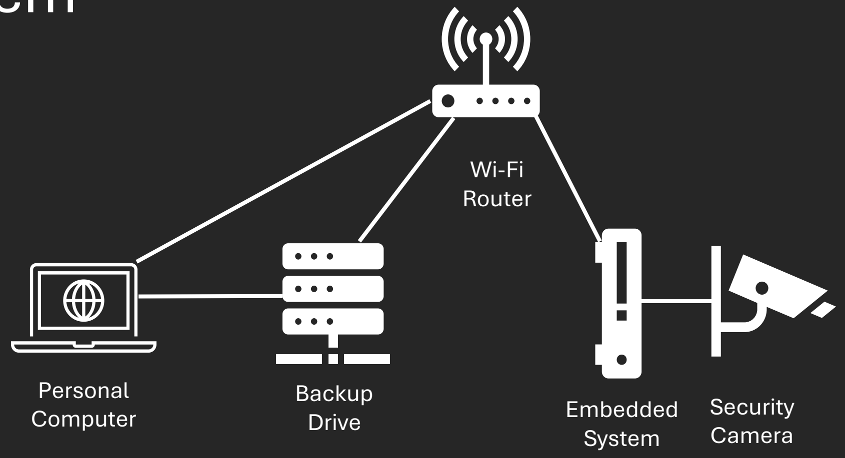
ISO Model

1. Camera captures video
2. Embedded system compresses using code (H264)
3. Compressed data is broken in UDP datagrams
4. UDP datagrams are added to IP packets
5. IP packets are added to Wi-fi frames
6. Wi-fi router removes frame header to get destination IP address
7. IP packet is added to new frame and sent to backup drive
8. Backup drive removes frame and IP packet heads and saves data

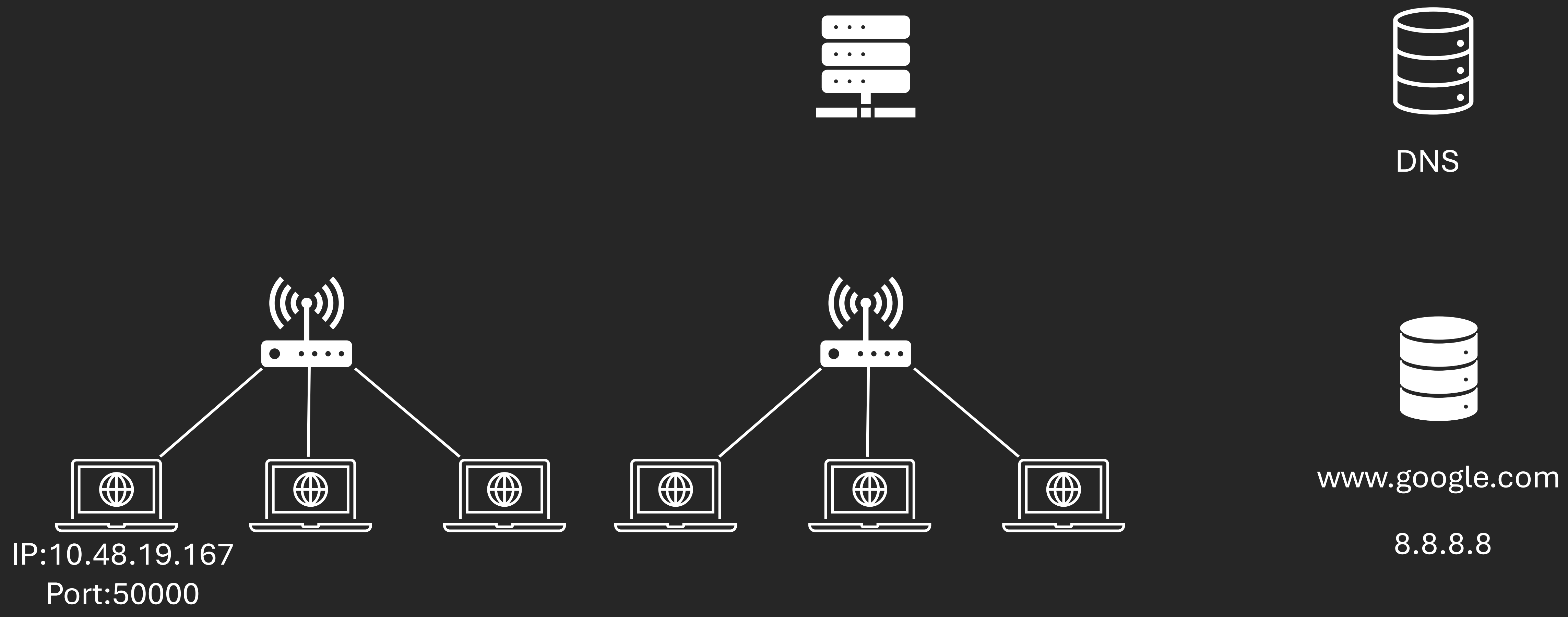


ISO Model

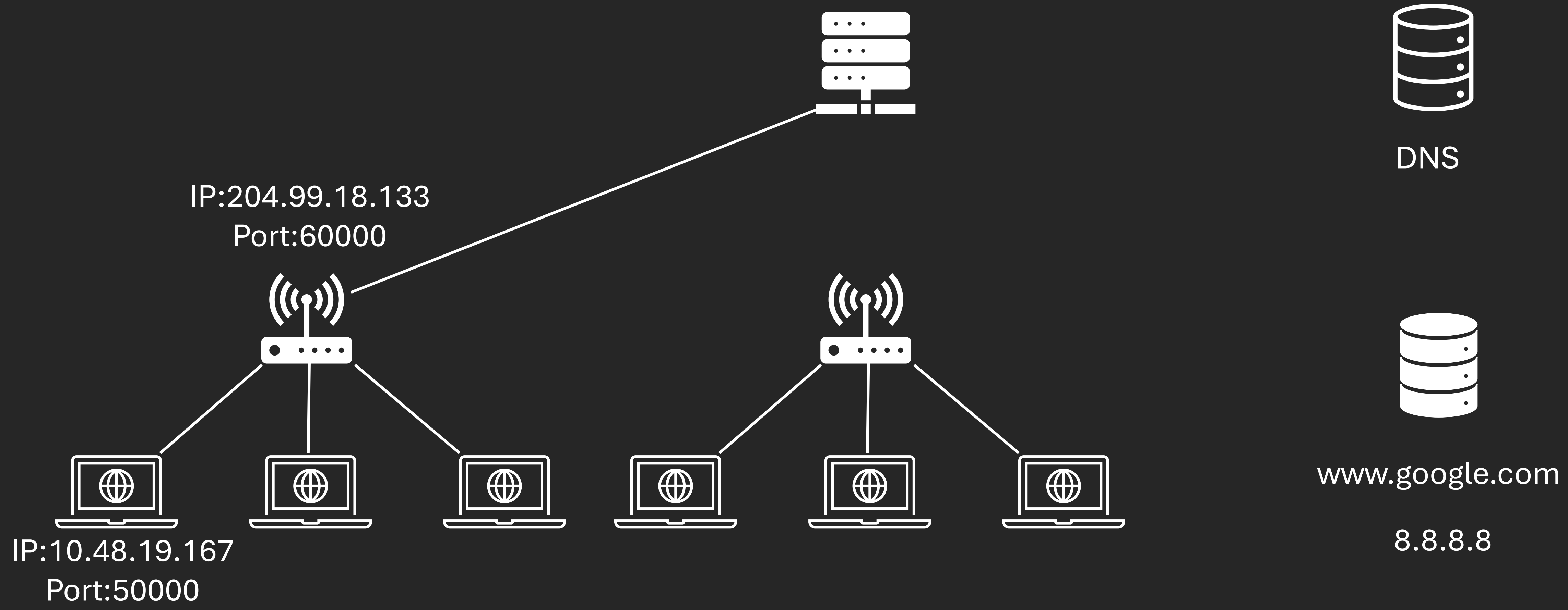
1. Physical Layer
   - Radio waves
2. Data Link Layer
   - Wi-fi (IEEE 802.11) and MAC addresses
3. Network Layer
   - IP addresses
4. Transport Layer
   - UDP
5. Session Layer
   - RTSP (Setup, play, pause)
6. Presentation Layer
   - Codec (H246)
7. Application Layer
   - RTSP and video management system



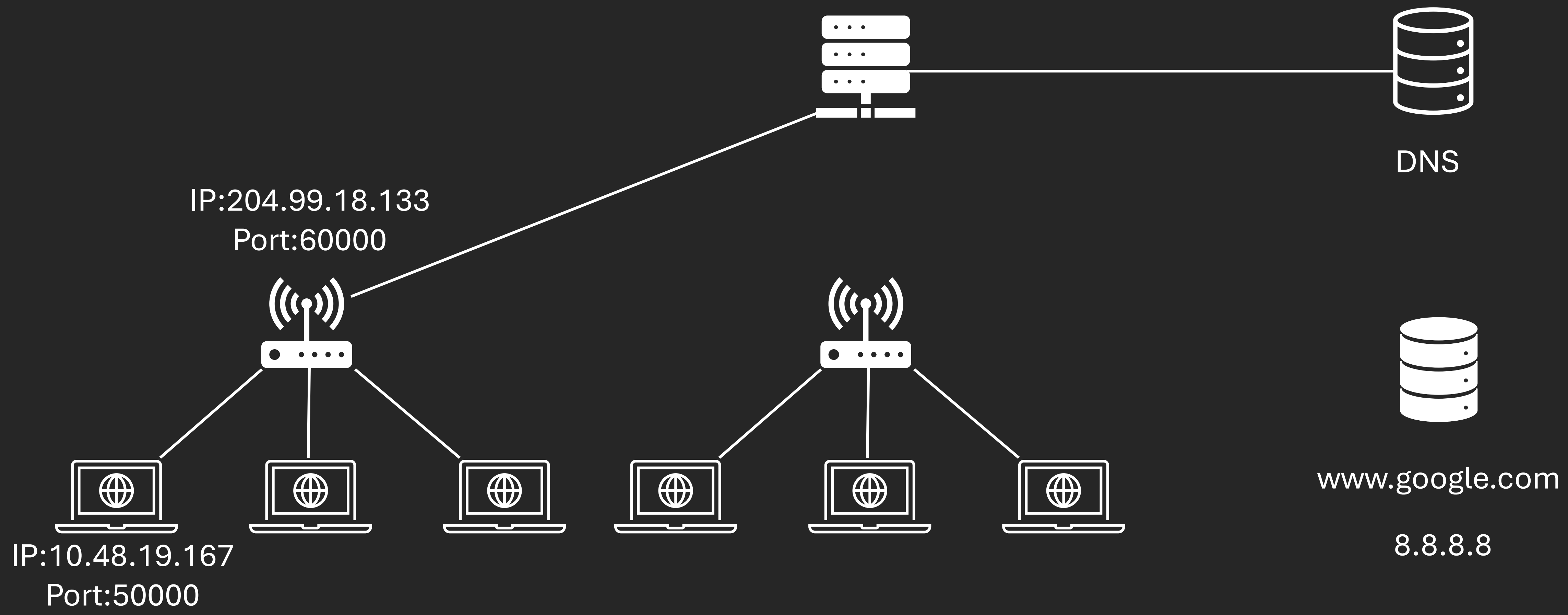
Communication Architectures



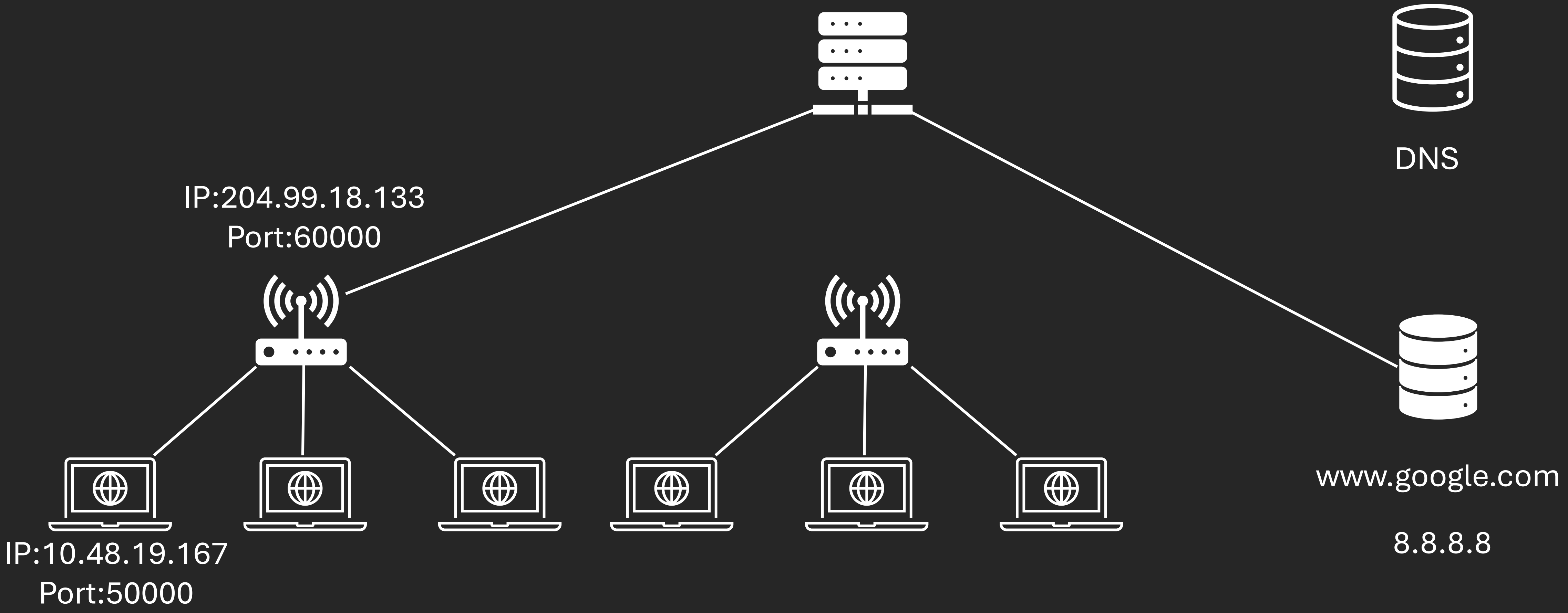
Communication Architectures



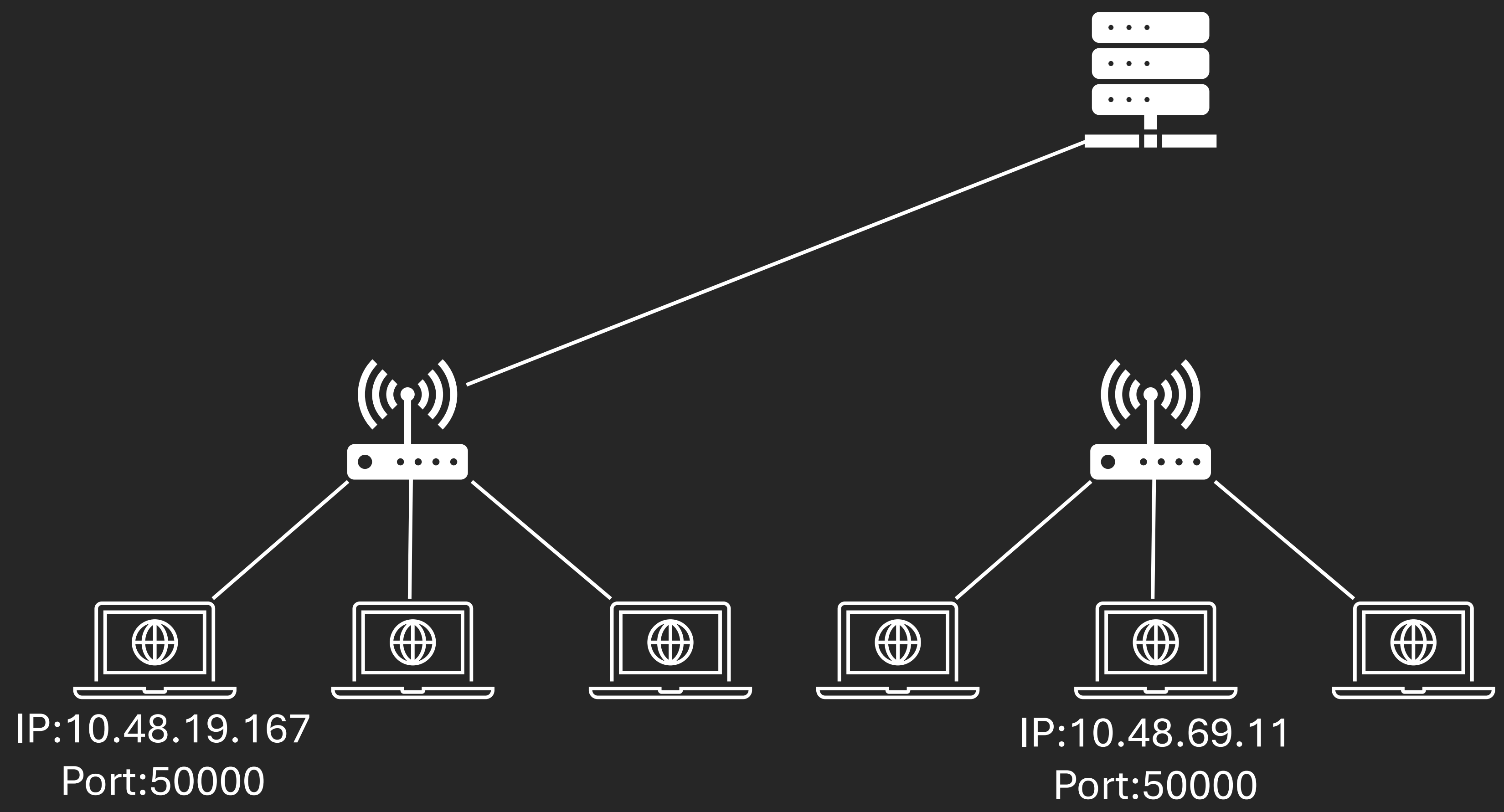
Communication Architectures



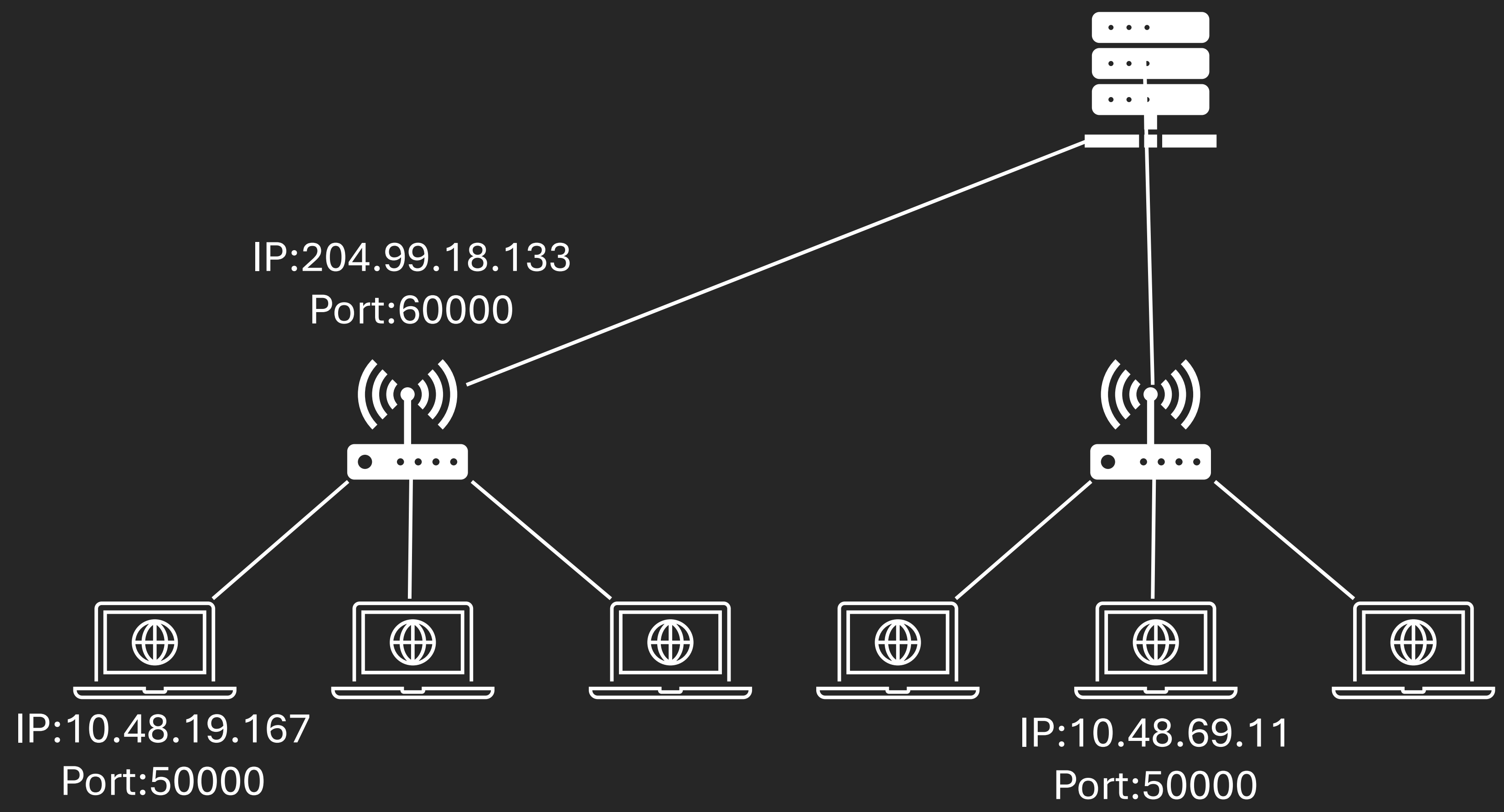
Communication Architectures



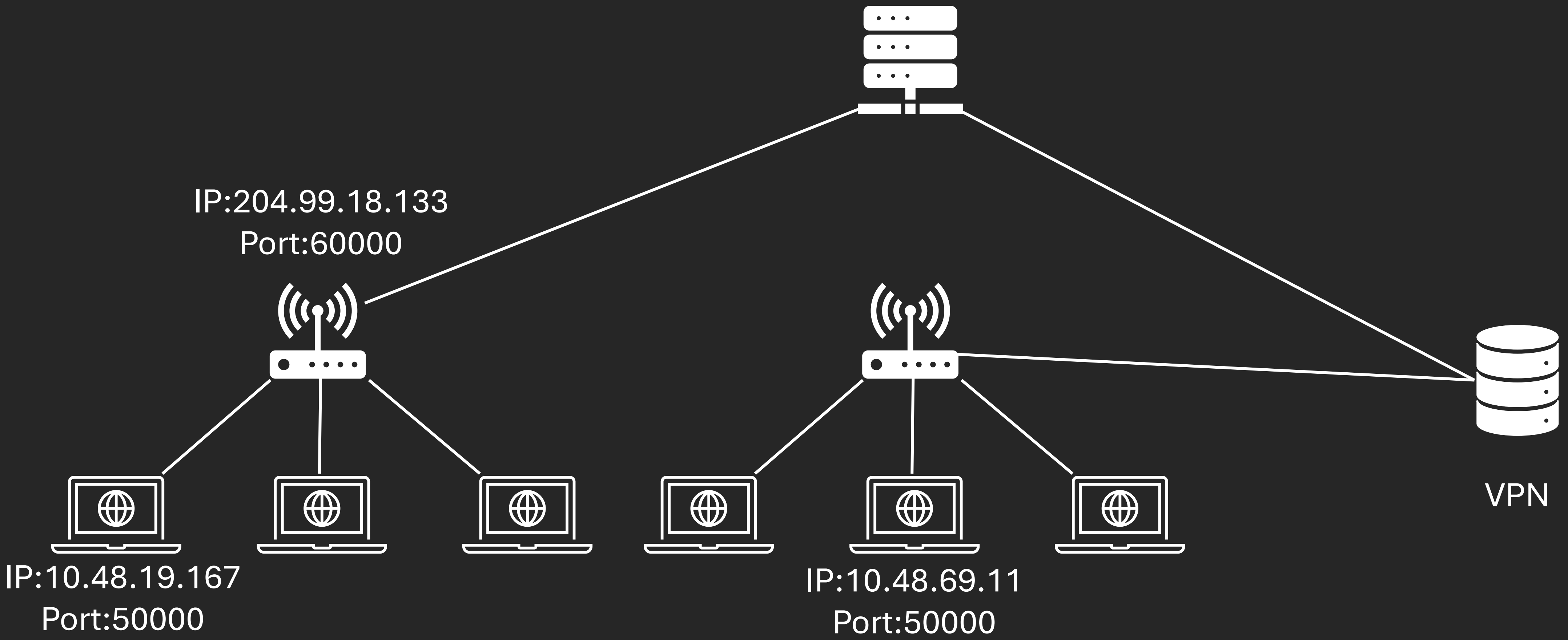
Communication Architectures



Communication Architectures



Communication Architectures



Example – Accessing a Website

Application	• Provides network services directly to applications and handles high-level protocols for data transfer • Responsible for user interfaces such as email, file transfer, and web browsing
Presentation	• Translates data between application layer and network, ensuring compatibility • Data compression/decompression, encryption/decryption, format translation and binary encoding
Session	• Establishes, manages, and terminates communication sessions between applications • Handles dialog control, allowing multiple applications to communicate over a network
Transport	• Ensures reliable data transfer between devices and segmentation of data for easier transmission • Provides end-to-end connection management, error recovery, flow control, and data integrity
Network	• Determines the best path to travel from source to destination via logical addressing and routing • Controls IP addressing, packet fragmentation and reassembly, routing and forwarding
Data Link	• Establishes, maintains, and decides how data is transferred between devices on a network • Controls framing, MAC, error detection/correction, and flow control
Physical	• Physical layer responsible for connection between devices • Controls transmission and reception of raw bits

Communication Architectures