Chapter-5

Mandip Rai

Transmission Media

Definition:

- Transmission media is the complete path through which data travels from the sender to receiver.
- It includes all physical channels and cables involved in data transmission.
- Acts as the communication channel when data is transmitted via electromagnetic waves.

Role in Data Communication:

- It transfers information from one device to another.
- Essential in enabling data flow between networked devices.
- Exists at the Physical Layer (Layer 1) of the OSI model.

Factors Affecting Transmission Quality:

1. **Bandwidth:**

- Higher bandwidth means stronger and faster transmission.
- Allows more data to be sent over the medium in a given time.

2. **Interference:**

- Unwanted noise or signals can distort data during transmission
- Good transmission media should minimize interference.

3. **Signal Quality:**

- Quality of the signal (strength, clarity) and medium determines the efficiency of data flow.

Types of Transmission Media:

1. **Wired Communication Media (Also called Guided Media):**

- Uses physical cables or wires to transmit data.
- Examples: Twisted Pair, Coaxial Cable, Fiber Optic Cable.

2. **Wireless Communication Media (Also called Unguided Media):**

- Uses electromagnetic waves (no physical medium).
- Examples: Radio waves, Microwaves, Infrared, Satellite.

Wired Communication

Definition & Nature:

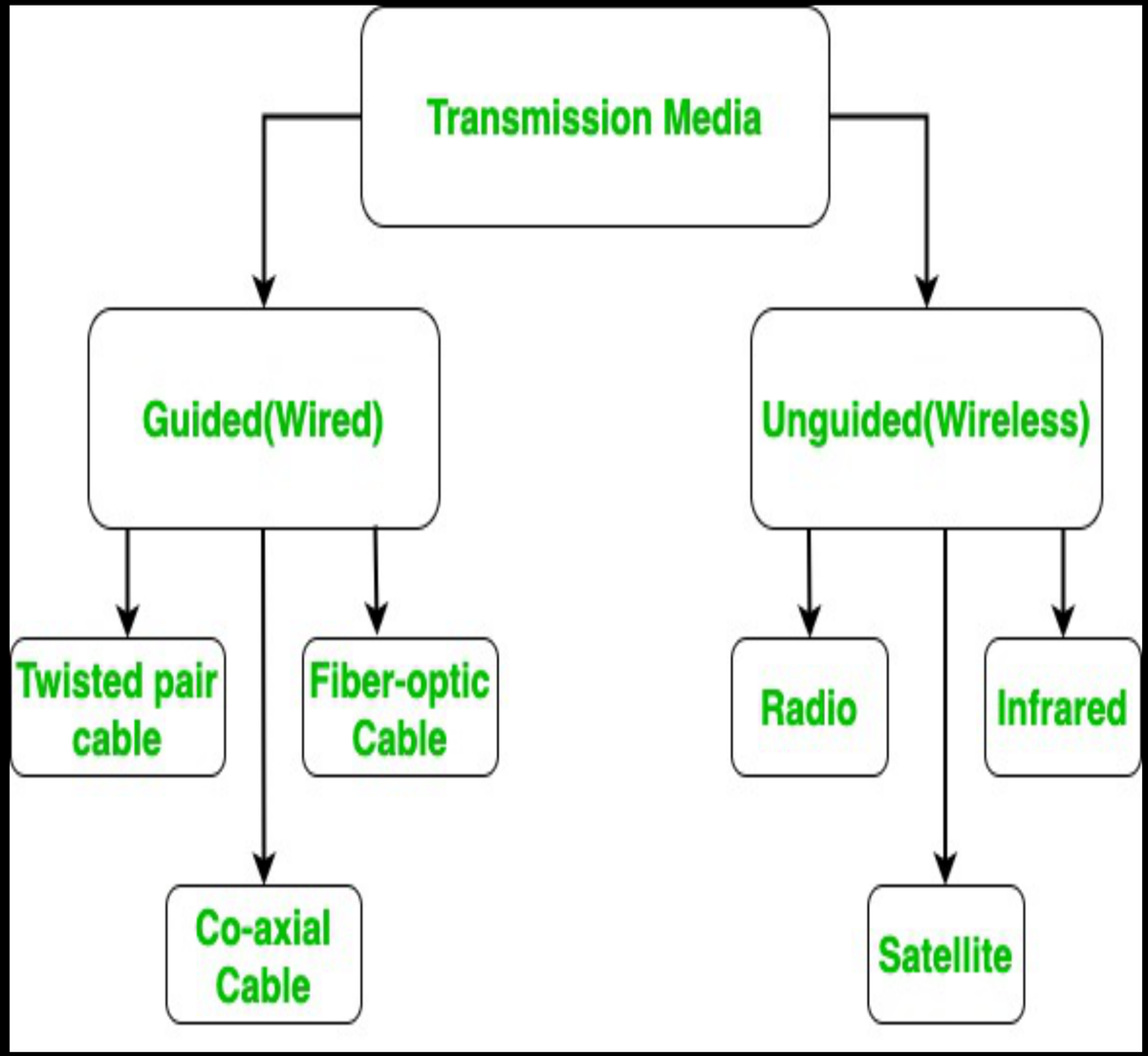
- Also known as Guided Media.
- A type of transmission media that uses physical wires or cables to transmit data.
- Provides a stable and reliable connection.

Advantages:

- More stable than wireless communication.
- Less prone to interference from external signals.
- Faster data transmission speeds compared to wireless.
- Ideal for professional and enterprise-level applications.

Disadvantages:

- Not suitable for public/mobile use, as it requires physical connections.
- Limited mobility – devices must be physically connected.
- Higher setup cost, especially over long distances.
- Requires more cables, ports, and installation effort.
- Fiber optic cables, though high-performing, are expensive.



Properties	Twisted Pair	Co-axial Cable	Fiber optic cable
Cost	Inexpensive	Twice or Thrice than twisted pair	Expensive
Installation	Easy	Easy	Difficult
Attenuation	More	More	Very Less
EMI Effect	Maximum	Minimum	No effect
Bandwidth	1 to 100 Mbps/100m	500 Mbps/100m	Gega bps/km
Signal Type	Electrical	Electrical	Light Signals

Wireless Communication

Definition:

- Also known as Unguided Media or Unbounded Transmission Media.
- No physical medium (like cables) is used.
- Data is transmitted through electromagnetic waves.

Mediums Used:

- Transmits signals through: Air, Water, Vacuum
- Common wave types: Infrared, Radio Waves, Microwaves

Advantages:

- No need for cables – saves on installation and maintenance.
- Enables mobility and flexibility – data can be accessed from anywhere.
- Can cover large distances, especially with satellite or cellular systems.

Disadvantages:

- Less secure – signals can be intercepted more easily.
- Susceptible to interference from weather, walls, or other wireless devices.
- May have lower speeds and higher latency compared to wired media.

USART (Universal Synchronous Asynchronous Receiver Transmitter)

UNIVERSAL SYNCHRONOUS ASYNCHRONOUS RECEIVER TRANSMITTER (USART) – 5251A

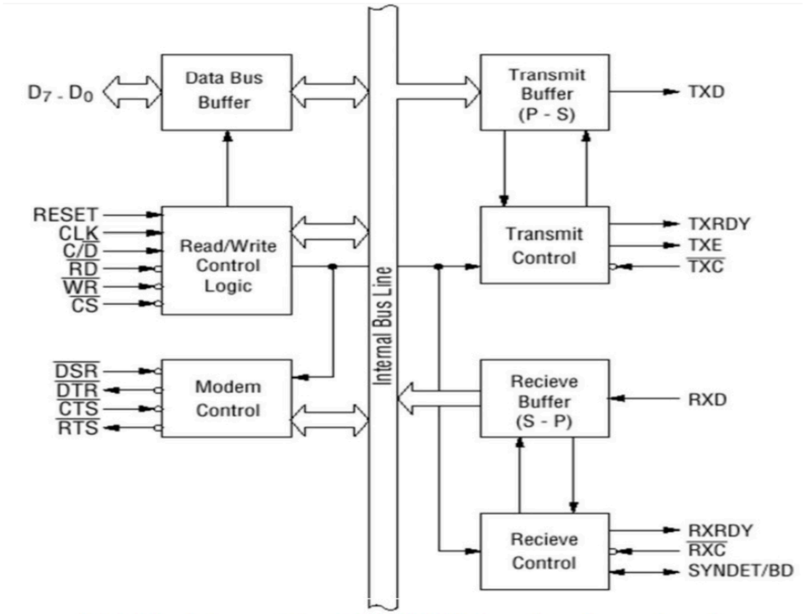


Fig 3.7 Block diagram of the 8251 USART (Universal Synchronous Asynchronous Receiver Transmitter)

The 8251 is a USART (Universal Synchronous Asynchronous Receiver Transmitter) for serial data communication. As a peripheral device of a microcomputer system, the 8251 receives parallel data from the CPU and transmits serial data after conversion. This device also receives serial data from the outside and transmits parallel data to the CPU after conversion.

The functional block diagram of 825 1A consists five sections:

- Read/Write control logic
- Transmitter
- Receiver
- Data bus buffer
- Modem control.

√ Read/Write control logic:

- Consist of three registers:
  - Control register (*Mode instruction, Command*)
  - Status register
  - Data buffer.
- $\overline{RD}$,$\overline{WR}$,$\overline{CS}$ *and* $\overline{C/D}$ - for Read/Write operations with these three registers.
  - $\overline{C/D}$ =1 => *Control register is selected.*
  - $\overline{C/D}$ =0 => *Data buffer is selected.*
- RST - For idle mode of chip.
- CLK - Clock input for communication with CPU.

$\overline{CS}$	$C/\overline{D}$	$\overline{RD}$	$\overline{WR}$	Input-Output Operation
1	x	x	x	Data bus tri-state
0	x	1	1	Data bus tri-state
0	1	0	1	Status --> CPU
0	1	1	0	CPU --> Control word
0	0	0	1	Data bus --> CPU
0	0	1	0	CPU --> Data bus

√ Transmitter section:

- Parallel data from CPU --> Serial data.
- RxD - Receives serial data from peripheral and buffered.
- Double buffered:
  - Buffer register: *Holds 8-bit parallel data from CPU.*
  - Output register: *Holds converted serial data for transmission.*
- TxRDY: If buffer register is empty.
- TxEMPTY: If output register is empty.
- $\overline{TxC}$: Gives clock refrence for reciever.

✓ **Receiver Section:**

- Accepts serial data --> parallel data.
- RxD - Receives serial data from peripheral and buffered.
- Double buffered:
  - Input register: *Receives and holds serial data.*
  - Buffer register: *Holds the converted parallel data.*
- RxRDY: Indicates input register loads a parallel data to buffer register.
- $\overline{\text{RxC}}$: Inputs clock refrence form transmitter.
- SYNDET/BRKDET: - (Asynchronous mode) Indicates break in data transmission.
  - (Synchronous mode) Indicate the reception of SYNC.

✓ **MODEM Control:**

- Allows to interface a MODEM over telephone lines.
- This unit takes care of handshake signals for MODEM interface.
- $\overline{\text{DTR}}$ (Data Terminal Ready) - Tells USART is ready for transmit data to MODEM.
- $\overline{\text{DSR}}$ (Data Set Ready) - Input signal for MODEM condition (ready or not).
- $\overline{\text{RTS}}$ (Request to Send): requests the MODEM prepare to transmit data.
- $\overline{\text{CTS}}$ (Clear to Send): MODEM is ready to accept data from the DTE.

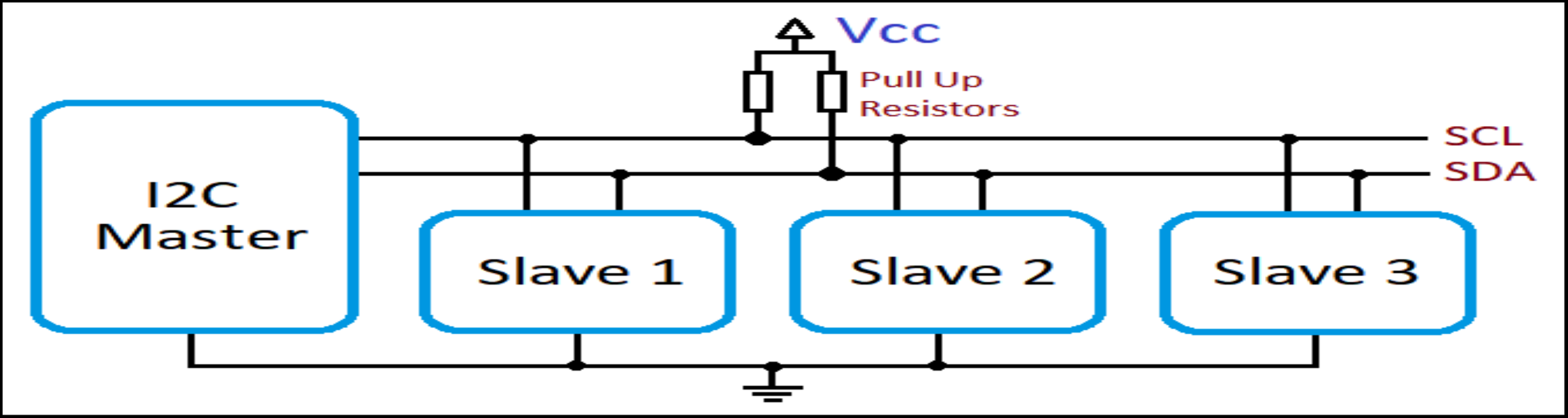
- **Bit Rate** *is how many data bits are transmitted per second.*
- **A baud Rate** *is the number of times per second a signal in a communications channel changes.*

I2C (Inter-Integrated Circuit)

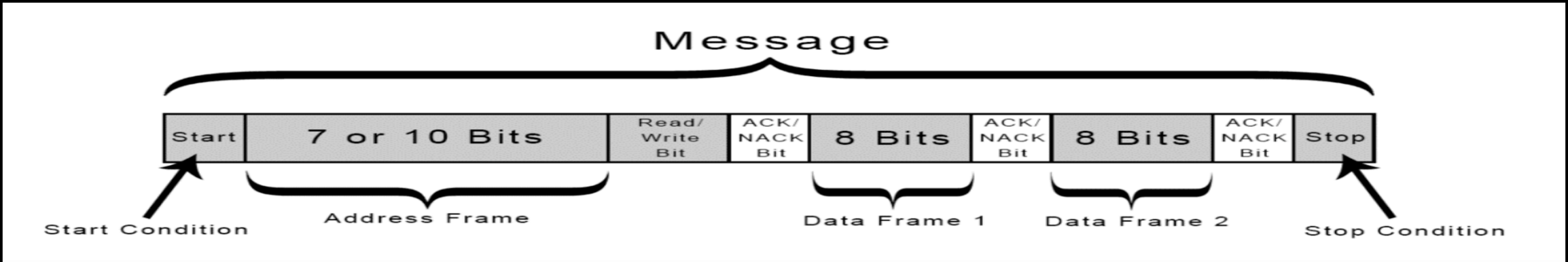
- I2C stands for Inter-Integrated Circuit. It is a bus interface connection protocol incorporated into devices for serial communication.
- It is a widely used protocol for short-distance communication. It is also known as Two Wired Interface(TWI).

Working of I2C Communication Protocol

- It uses only 2 bi-directional open-drain lines for data communication called SDA and SCL. Both these lines are pulled high.
- Serial Data (SDA) : Transfer of data takes place through this pin.
- Serial Clock (SCL) : It carries the clock signal.
- I2C operates in 2 modes: Master mode and Slave mode.



Data Frame



- **Start Condition:** The start condition initiates the data frame and indicates the beginning of a new transmission. It is generated by the master device and consists of a high-to-low transition on the SDA (Serial Data Line) while the SCL (Serial Clock Line) is high. The start condition prepares the bus for transmitting the address and data.

- **Addressing:** After the start condition, the master device transmits the address of the target slave device it wishes to communicate with. The address typically consists of 7 or 10 bits, depending on the addressing mode (7-bit or 10-bit) used in the specific I2C implementation. The address bits are transmitted from the most significant bit (MSB) to the least significant bit (LSB).

- **Read/Write Bit:** Following the address, the master device sends a single bit known as the Read/Write (R/W) bit. This bit determines the direction of data transfer. When the R/W bit is set to 0, it indicates a write operation (master sending data to the slave). Conversely, when the R/W bit is set to 1, it signifies a read operation (master requesting data from the slave).

- **Data Transfer:** Once the address and R/W bit have been transmitted, the actual data transfer takes place. Both the master and slave devices can send and receive multiple bytes of data. Each data byte consists of 8 bits transmitted from the MSB to the LSB. After transmitting each byte, the receiver (master or slave) provides an acknowledgement (ACK) to confirm the successful reception of the data. If the ACK is not received, it indicates a transmission error.

- **Stop Condition:** The stop condition concludes the data frame and signifies the end of the transmission. It is generated by the master device and consists of a low-to-high transition on the SDA line while the SCL line is high. The stop condition releases the bus, allowing other devices to initiate new communications.

Standard Mode

Standard Mode is the original and most commonly used mode in I2C communication. It supports a maximum data transfer rate of 100 kilobits per second (Kbps). In this mode, both the master and slave devices adhere to the timing specifications defined by the I2C standard.

Key Features

- **Clock Frequency:** The clock frequency in Standard Mode is limited to 100 kHz, meaning the clock signal toggles at a maximum rate of 100,000 times per second.
- **Rise and Fall Times:** The rise and fall times of the signals on the I2C bus are relatively relaxed in Standard Mode, typically ranging between a few microseconds to tens of microseconds.
- **Noise Immunity:** Standard Mode provides a reasonable level of noise immunity, ensuring reliable communication in most common operating environments.
- **Compatibility:** Standard Mode is supported by virtually all I2C-compatible devices, making it the go-to mode for most general-purpose I2C applications.

Fast Mode

Fast Mode is an enhanced version of I2C communication that offers higher data transfer rates compared to Standard Mode. It supports a maximum data transfer rate of **400 kilobits** per second (Kbps). Fast Mode is backwards compatible with Standard Mode, allowing devices to communicate with each other regardless of the mode they operate in.

Key Features

- **Clock Frequency:** In Fast Mode, the clock frequency is increased to a maximum of **400 kHz**, enabling faster data transfer between devices.
- **Rise and Fall Times:** The rise and fall times of the signals on the I2C bus are typically faster in Fast Mode compared to Standard Mode, ranging between a few hundred nanoseconds to a few microseconds.
- **Noise Immunity:** Fast Mode retains a good level of noise immunity, ensuring reliable communication even at higher data rates.
- **Compatibility:** Fast Mode is supported by a wide range of I2C devices. However, it is important to note that older or more specialized devices may only support Standard Mode.

Advantages of I2C

Simplicity: The I2C protocol is relatively straightforward and easy to implement, requiring minimal hardware overhead.

Flexibility: With its support for multiple masters and up to 128 slave devices, I2C allows for versatile system designs, accommodating a wide range of applications.

Wide Adoption: I2C has gained widespread popularity and support from semiconductor manufacturers, ensuring a vast array of compatible devices available in the market.

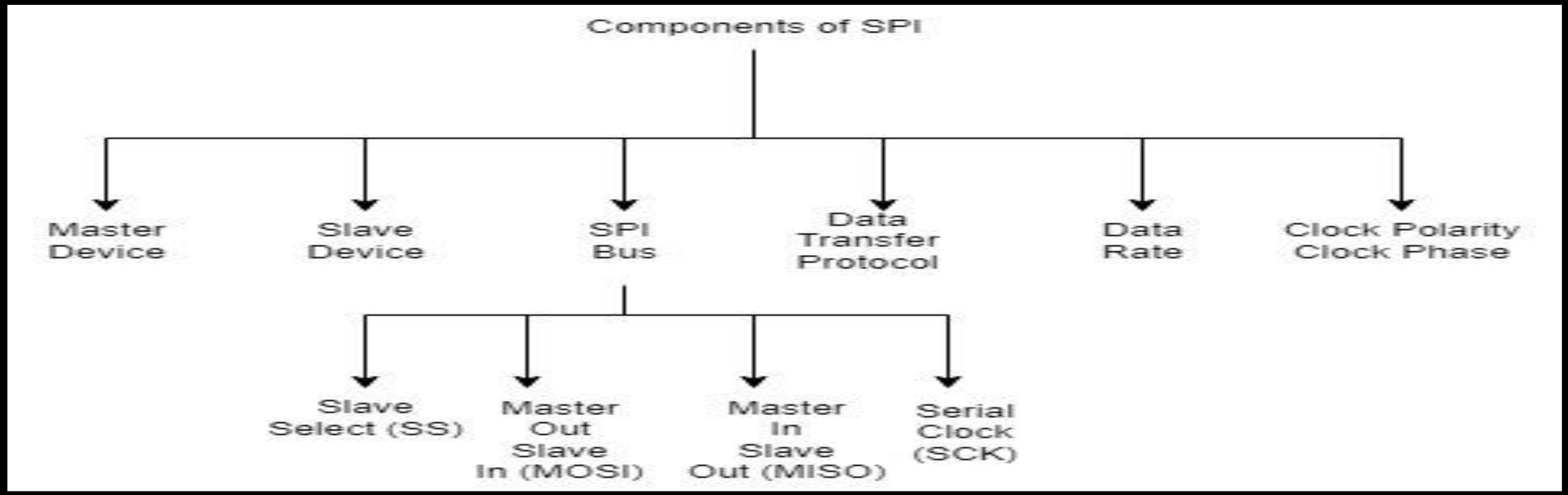
Disadvantage of I2C

Limited Distance: One of the drawbacks of the I2C protocol is its limited communication distance. The I2C bus is designed for short-distance communication within a system, typically a few meters. An excessive cable length or interference can degrade signal quality and lead to communication errors. Therefore, for longer distances, additional measures such as signal boosters or other communication protocols may be necessary.

Slower Speed Compared to Other Protocols: While I2C provides a straightforward and easy-to-use interface, it operates at lower data transfer rates compared to some other communication protocols. The maximum speed in Standard Mode is limited to 100 kilobits per second (Kbps), and in Fast Mode, it reaches a maximum of 400 Kbps. For applications requiring high-speed data transfer, other protocols like SPI (Serial Peripheral Interface) or UART (Universal Asynchronous Receiver-Transmitter) may be more suitable.

SPI (Serial Peripheral Interface)

- SPI stands for Serial Peripheral Interface. It is a protocol that is synchronous serial communication. It is used to communicate between the peripheral devices i.e. input and output devices and microcontrollers. It is allowed to transfer high-speed data. It is popular with digital communication applications and embedded systems. SPI can transfer the data and receive data from one device to another device at a time.



Components of SPI

- **Master Device:** The master device is nothing but it controls the process of transformation of data on the SPI bus. It controls the data flow and it generates the clock signal. In most of the applications, the master device is the microcontroller or specialized SPI controller.

- **Slave Device:** Slave devices are peripheral devices that are connected to the SPI bus and controlled by master devices. Every slave device has a different slave select (SS) line, allowing the master to select which device it wants to communicate with.

- **SPI Bus:** SPI bus is a physical connection over the data transferring between the slave devices and the master. It contains four signal lines as below.

  - **Slave Select (SS):** In SPI, each slave device has a dedicated Slave Select (SS) pin. When the master communicates with a specific slave, it activates that slave's SS line. Multiple slave devices can share the same MOSI, MISO, and SCK lines, but each must have its own separate SS line.

  - **Master Out Slave In (MOSI):** In Master Out Slave In, MOSI can share the data or information from the master to other slave devices.

  - **Master In Slave Out (MISO):** In Master In Slave Out, MISO can share the data or information from the slave device with the master.

  - **Serial Clock (SCK):** In Serial Clock, this clock signal is used by the master and the slave devices for coordinating the data transfer timings.

Components of SPI

- **Data Transfer Protocol:** SPI is a synchronous serial communication protocol used for simple and efficient data transfer. Data is transmitted and received simultaneously in full-duplex mode. The master generates clock pulses to initiate data transfer, and during each clock cycle, one bit of data is exchanged both from master to slave and from slave to master.

- **Data Rate:** The SPI bus can support different data transfer rates depending on the capabilities of the master and slave devices, as well as the length and quality of the transmission lines. The data rate is typically specified in bits per second (bps) or in terms of clock frequency, such as megahertz (MHz).

- **Clock Polarity (CPOL) and Clock Phase (CPHA):** CPOL and CPHA are used to define the relationship between the data signals and the clock signal in SPI communication. The data signals—MOSI (Master Out Slave In) and MISO (Master In Slave Out)—carry the actual data, while SCK (Serial Clock) serves as the clock signal. There are four possible combinations of CPOL and CPHA settings, allowing flexibility in configuring the SPI interface to work with different devices.

Advantages of SPI

- **High Speed Data Transfer:** SPI supports high-speed communication, making it suitable for applications that require rapid data transfer. The actual data transfer speed depends on the capabilities of the microcontroller and the connected peripheral devices. High-speed communication is especially useful in scenarios such as real-time data acquisition or interfacing with high-performance sensors.

- **Simple Hardware Requirements:** SPI requires only a few hardware components. It uses four signal lines —SCK (Serial Clock), MOSI (Master Out Slave In), MISO (Master In Slave Out), and SS (Slave Select) —for data transmission without the need for complex protocols. These minimal requirements help keep hardware costs low and make implementation easier compared to other communication protocols.

- **Full-Duplex Communication:** SPI supports full-duplex communication, meaning it can transmit and receive data simultaneously, enabling true bidirectional communication. This feature allows efficient data transfer, making SPI suitable for applications that require high-speed communication.

- **Multi Slave Devices:** SPI supports multiple slave devices using a single master device. Each slave is assigned a Slave Select (SS) line, allowing the master to select and communicate with one slave at a time as needed. This capability enables SPI to interface with multiple peripheral devices within a system without requiring complex additional hardware.

Advantages of SPI

- **Widespread Adoption:** SPI is a widely adopted communication protocol in the embedded systems industry, supported by most microcontrollers and peripheral devices. This widespread adoption ensures compatibility between different hardware components, making SPI a reliable choice for communication in a variety of applications.

- **Low Overhead:** SPI has low overhead compared to other communication protocols and does not require complex addressing or data packetization. This low overhead simplifies software implementation, making SPI suitable for applications with limited processing resources.

- **Flexible Configurability:** SPI offers flexibility in configuration parameters such as clock polarity (CPOL) and clock phase (CPHA), allowing it to accommodate various types of peripheral devices. This configurability enables SPI to interface with a wide range of devices—including sensors, memory chips, displays, and other integrated circuits—without requiring significant changes to the software or hardware.

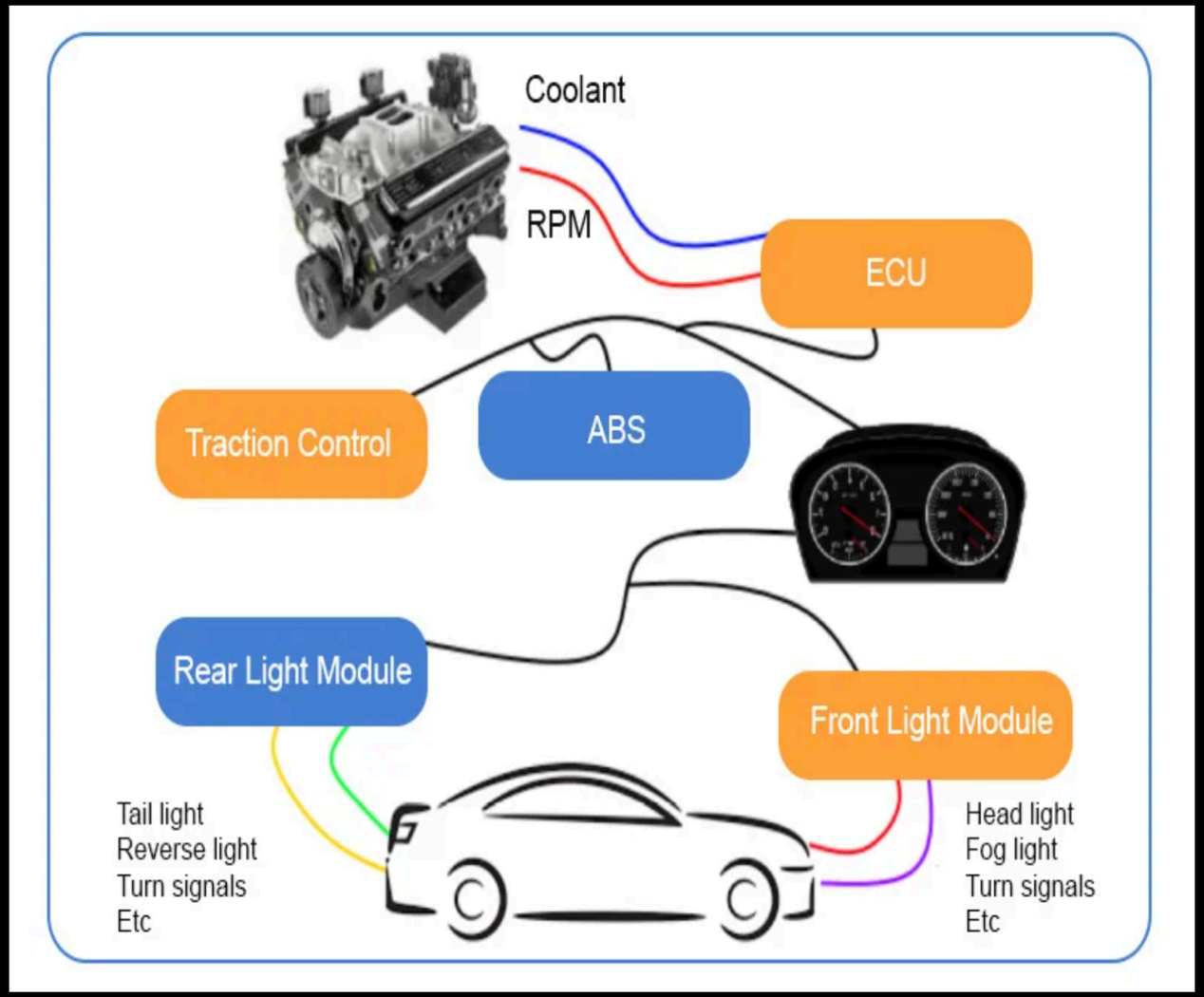
CAN (Controller Area Network)

- **Definition**: The Controller Area Network (CAN) is a robust, high-speed serial communication protocol designed for real-time control applications, particularly in automotive and industrial systems.

- **Purpose**: Facilitates efficient communication between Electronic Control Units (ECUs) without the need for a host computer, reducing wiring complexity and enhancing system reliability.

- Key communication stages include:
  - **Arbitration**: Prioritizes messages by identifier to avoid transmission collisions.
  - **Error Detection**: Ensures data integrity using frame check sequences, acknowledgments, and CRC.
  - **Fault Confinement**: Isolates malfunctioning nodes by switching them to an “error passive” state.

CAN (Controller Area Network)



CAN (Controller Area Network)

The key components that form the core of a CAN Bus system, ensure its efficient and reliable operation.

- **Electronic Control Units (ECUs):** The ‘brains’ of the CAN Bus, or ECUs, are responsible for regulating certain operations like airbag activation and engine management in cars. They receive data over the CAN Bus, process it, and take appropriate action.
- **CAN Controller:** This part serves as a link between the CAN network and the ECUs. It oversees the sending and receiving of data packets, making sure that messages are sent and structured correctly.
- **CAN Transceiver:** The CAN Transceiver transforms digital data into signals for network transmission with the CAN Controller, and vice versa. This is necessary for node-to-node communication within the network.
- **Bus Lines (CAN_H and CAN_L Wires):** The CAN Bus system is supported by the physical wires known as CAN_H and CAN_L. Even in settings with a lot of electrical noise, they send signals between nodes.

Data Frames in CAN

- The real data for transmission is contained in the data frame.
- The fields that make up a data frame are the Arbitration Field, Control Field, Data Field, CRC Field, 2-bit Acknowledge Field, and End of Frame. These fields offer more information about the transmission.
- There are two types of Data frames: Standard Frame or Base Frame Format and Extended Frame Format.
- The extended frame supports a 29-bit identification made up of an extended 18-bit identifier and an 11-bit identifier, while the normal frame only supports an 11-bit identifier.
- In an extended frame, the IDE bit is recessive and dominant in a standard frame.

Base Frame Format

- **SOF - Start of Frame:** Denotes the start of frame transmission.
- **Identifier:** 11-bit unique ID and also represents message priority Lower the value, the higher the priority.
- **RTR:** Remote Transmission Request. It is dominant for data frames and recessive for remote frames.
- **IDE:** Single Identification Extension. It is dominant for standard frames and recessive for extended frames.
- **R0:** Reserved bit.

Base Frame Format

- **DLC:** Data Length Code. Defines the length of the data being sent. It is of 4-bit size. Data – The data to be transmitted and its length is decided by DLC.
- **CRC:** Cyclic Redundancy Check. It contains the checksum of the preceding application data for error detection.
- **ACK:** Acknowledge. It is 2 bits in length. It is dominant if an accurate message is received.
- **EOF:** end of the frame and must be recessive.
- **IFS:** Inter Frame Space. It contains the time required by the controller to move a correctly received frame to its proper position.

Extended Frame Format

- The Extended Frame is similar to the Standard Frame but includes some additional fields.
- It contains an SRR (Substitute Remote Request) bit.
- When two messages have the same 11-bit identifier, the SRR bit is sent as a recessive bit to ensure the Standard Frame has higher priority over the Extended Frame.
- The Extended Frame uses a 29-bit identifier, which includes the usual 11-bit plus an additional 18-bit identification.

RF Modem

- Wireless data transmitters operating over UHF/VHF bands, enabling long-distance, real-time communication independently of satellite or telecom networks.
- Capable of spanning tens of kilometres, with high-end models reaching 30 km line-of-sight.
- Offer high data speeds, e.g., 115,200 bps with their 900 MHz RF-9256 unit; even “low-power” Piccolo models deliver up to 38,400 bps.
- Operate on licensed (to avoid interference) or license-free (with frequency-hopping to prevent jamming) bands.
- Provide reliable, real-time telemetry unaffected by telecom/satellite outages.
- Support autonomous operations in remote areas—crucial for mining, utilities, agriculture, fire monitoring, etc.

RF Modem

- **Converts data signals:** RF modems take data from a wired interface (like RS-232 or RS-485) and modulate it into a radio frequency signal for wireless transmission.
- **Transmits wirelessly:** The modulated signal is then transmitted via radio waves to another RF modem or a receiver.
- **Receives and demodulates:** At the receiving end, the RF modem demodulates the signal back into its original data format.
- **Enables remote communication:** This allows for communication and data exchange between devices that are not physically connected by wires.

RF Modem (Key Features)

- **Frequency range:** RF modems operate within specific frequency bands, often in the MHz or GHz range, which are chosen based on regulatory requirements and application needs.
- **Data rate:** The speed at which data can be transmitted, measured in bits per second (bps).
- **Range:** The distance over which the modem can reliably transmit data.
- **Power output:** The strength of the transmitted signal, which affects the range and power consumption.
- **Antenna:** RF modems often use external antennas to improve signal strength and range.
- **Interface:** The type of connection (e.g., RS-232, RS-485) to the host device.
- **Modulation and demodulation techniques:** Methods used to encode and decode the data onto the radio waves.
- **Error correction:** Mechanisms to detect and correct errors that may occur during transmission.

WiFi

- A wireless network uses radio waves, just like cell phones, televisions and radios do.
- In fact, communication across a wifi network is a lot like two-way radio communication.
- Here's what happens:
  - A computer's wireless adapter translates data into a radio signal and transmits it using an antenna.
  - A wireless router receives the signal and decodes it. The router sends the information to the internet using a physical, wired ethernet connection.
  - The process also works in reverse, with the router receiving information from the internet, translating it into a radio signal and sending it to the computer's wireless adapter.

WiFi

- They can transmit and receive radio waves, and they can convert 1s and 0s into radio waves and convert the radio waves back into 1s and 0s.
- But WiFi radios have a few notable differences from other radios:
  - They transmit at frequencies of 2.4 GHz or 5 GHz. This frequency is considerably higher than the frequencies used for cell phones, walkie-talkies and televisions. The higher frequency allows the signal to carry more data.
  - 2.4 GHz connections are now considered somewhat obsolete because they carry lower data speeds than 5 GHz. The 2.4 band continues to see use, however, because the lower frequency can carry over several hundred feet. In ideal conditions, the 5 GHz band has a max range of about 200 feet (61 meters), but in the real world, it is much more prone to interference from walls, doors and other objects. The 2.4 band may be faster for a user connecting to a router several rooms away, while 5 GHz will definitely be faster for a close connection.

WiFi

- 802.11b (introduced in 1999) is the slowest and least expensive standard. For a while, its cost made it popular, but now it's less common as faster standards become less expensive. 802.11b transmits in the 2.4 GHz frequency band of the radio spectrum. It can handle up to 11 megabits of data per second, and it uses complementary code keying (CCK) modulation to improve speeds.
- 802.11a (introduced after 802.11b) transmits at 5 GHz and can move up to 54 megabits of data per second. It uses orthogonal frequency-division multiplexing (OFDM), a more efficient coding technique that splits that radio signal into several sub-signals before they reach a receiver. This greatly reduces interference.
- 802.11g transmits at 2.4 GHz like 802.11b, but it's a lot faster — it can handle up to 54 megabits of data per second. 802.11g is faster because it uses the same OFDM coding as 802.11a.

WiFi

- 802.11n (introduced in 2009) is backward compatible with a, b and g. It significantly improved speed and range over its predecessors. For instance, although 802.11g theoretically moves 54 megabits of data per second, it only achieves real-world speeds of about 24 megabits of data per second because of network congestion. 802.11n, however, reportedly can achieve speeds as high as 140 megabits per second. 802.11n can transmit up to four streams of data, each at a maximum of 150 megabits per second, but most routers only allow for two or three streams.

- 802.11ac came on the scene around 2014, and operates exclusively at a 5 GHz frequency. 802.11ac is backward compatible with 802.11n (and therefore the others, too), with n on the 2.4 GHz band and ac on the 5 GHz band. It is less prone to interference and far faster than its predecessors, pushing a maximum of 450 megabits per second on a single stream, although real-world speeds may be lower. Like 802.11n, it allows for transmission on multiple spatial streams — up to eight, optionally. It is sometimes called 5G because of its frequency band, sometimes Gigabit WiFi because of its potential to exceed a gigabit per second on multiple streams and sometimes Very High Throughput (VHT) for the same reason.

WiFi

- 802.11ax, also known as WiFi 6, came to the industry in 2019. This standard extends the capabilities of 802.11ac in a few key ways. First of all, the new routers allow an even higher data flow rate, up to 9.2 Gbps (gigabits per second). WiFi 6 also lets manufacturers install many more antennas on one router, accepting multiple connections at once without any worry of interference and slowdown. Some new devices also connect on a higher 6 GHz band, which is about 20 percent faster than 5GHz in ideal conditions.

- 802.11be (or WiFi 7) started rolling out in 2024, offering even better range, more connections and faster data rates than any of the previous versions.

- Other 802.11 standards focus on specific applications of wireless networks, like wide area networks (WANs) inside vehicles or technology that lets you move from one wireless network to another seamlessly.

WiFi (Protection)

- The Wired Equivalency Privacy (WEP) security measure was once the standard for WAN security. The idea behind WEP was to create a wireless security platform that would make any wireless network as secure as a traditional wired network. But hackers discovered vulnerabilities in the WEP approach, and today it's easy to find applications and programs that can compromise a WAN running WEP security. It was succeeded by the first version of WiFi Protected Access (WPA), which uses Temporal Key Integrity Protocol (TKIP) encryption and is a step up from WEP but is also no longer considered secure.

- WiFi Protected Access version 2 (WPA2) is the successor to WEP and WPA, and is now the recommended security standard for WiFi networks. It uses either TKIP or Advanced Encryption Standard (AES) encryption, depending upon what you choose at setup. AES is considered the most secure. As with WEP and the initial WPA, WPA2 security involves signing on with a password. Public hot spots are either open or use any of the available security protocols, including WEP, so use caution when connecting away from home. WiFi Protected Setup (WPS), a feature that ties a hard-coded PIN to the router and makes setup easier, apparently creates a vulnerability that can be exploited by hackers, so you may want to turn off WPS if possible, or look into routers that do not have the feature.

WiFi (Protection)

- WPA3 was released in 2018 and became the security standard as of 2020. It aims to solve some of the vulnerabilities in WPA2 by putting much more complex encryption on both the router side and client side of the connection. This encryption also changes over time, meaning if a hacker had managed to access an unauthorized connection at one point in time, they would be locked out again the next time they try to connect. WPA3-enabled devices can also add some client-side encryption while using open public networks.

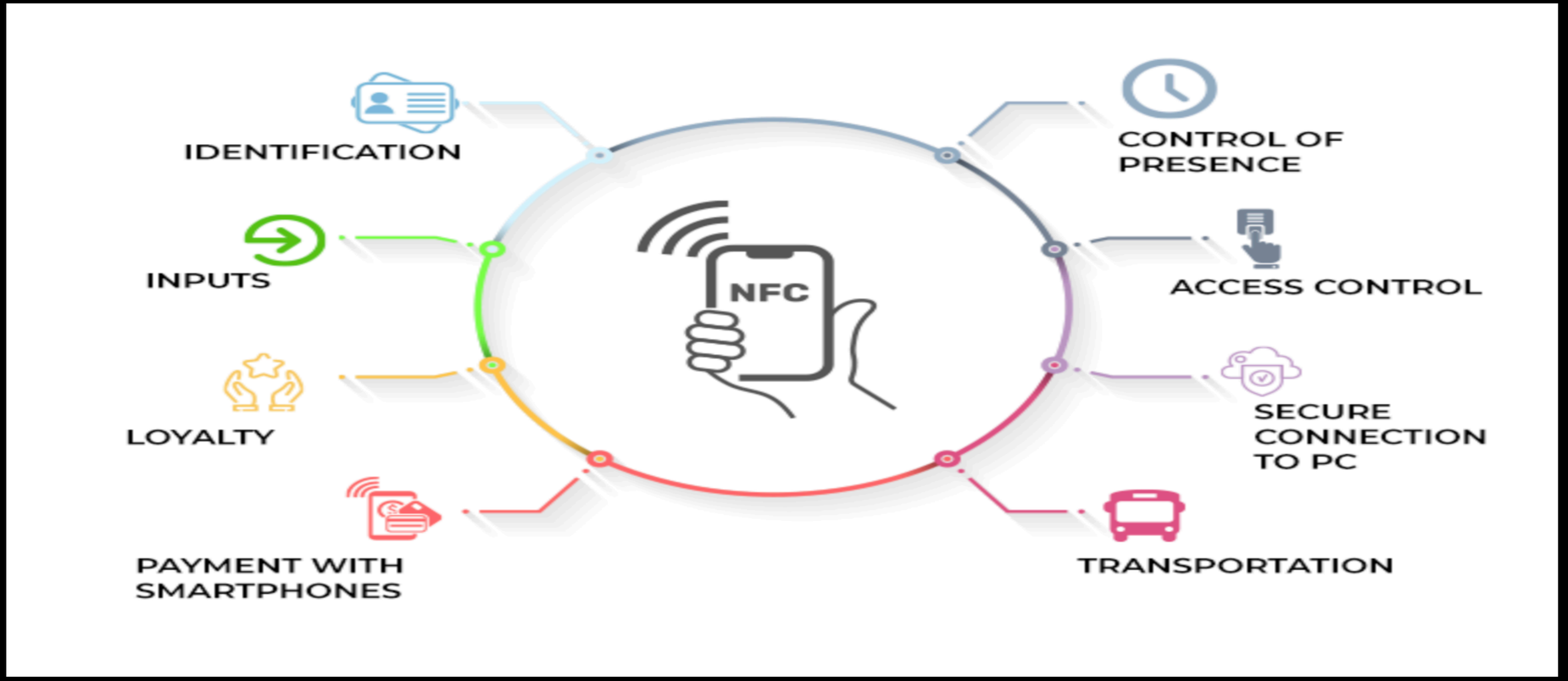
- It's worth noting that no matter how secure, a wireless network will surely have some method of exploit that can be used by hackers. When it comes to sensitive government or corporate data, a simple wired connection is the more secure alternative. In order to access or spy on a wireless network, a hacker has to be within physical range of the router, so attacks at home are not very likely to occur.

WiFi (Protection)

- Media Access Control (MAC) addresses filtering is a little different from WEP, WPA or WPA2. It doesn't use a password to authenticate users — it uses a computer's physical hardware. Each computer has its own unique MAC address. MAC address filtering allows only machines with specific MAC addresses to access the network. You must specify which addresses are allowed when you set up your router. If you buy a new computer or if visitors to your home want to use your network, you'll need to add the new machines' MAC addresses to the list of approved addresses. The system isn't foolproof. A clever hacker can spoof a MAC address — that is, copy a known MAC address to fool the network that the computer he or she is using belongs on the network.

NFC

- Near Field Communication, commonly abbreviated as NFC, is defined as a wireless personal area network (PAN) technology that connects two compatible devices in very close proximity to each other, in order to enable slow but reliable data transfer.



NFC

- Near-Field Communication (NFC) is a set of communication protocols that allow two electronic devices to exchange data over a very short distance, typically less than four centimeters.
- For NFC to work, there must be two compatible devices: an initiator that starts the communication and a target that receives it.
- The technology enables fast and effortless data sharing between mobile devices such as smartphones, often requiring just a simple tap.
- The NFC Forum was established in 2004 by Nokia, Sony, and Philips with the goal of promoting awareness of NFC and its advantages.
- This forum is also responsible for developing and maintaining NFC standards, as well as certifying devices to ensure they are NFC-compliant.
- The development of NFC standards was based on existing Radio Frequency Identification (RFID) standards, including ISO/IEC 14443 and FeliCa.
- By building on these existing standards, NFC ensures compatibility and interoperability between devices from different manufacturers.
- NFC does not include built-in encryption, which helps it remain compatible with traditional RFID technologies that also operate without encryption.

NFC

- Additional application software is necessary for NFC-enabled devices, such as smartphones, to perform the full range of functions intended by their manufacturers.
- Without this software, smartphones are unable to carry out essential NFC tasks, such as making contactless payments or reading data from smart NFC posters.
- NFC technology is widely used in contactless payment systems, such as Apple Pay and Samsung Pay, allowing users to make secure payments with a tap of their smartphones.
- It is also used for wireless charging of wearable devices, such as fitness trackers, and for providing key card access to secure areas like offices and schools.
- Communication between two NFC-compatible devices can occur in two configurations: when both devices are active, or when one is active and the other is passive.
- For data transfers at a speed of 106 kbit/s, a modified form of Miller coding with 100% modulation is used by the active NFC device.
- When the data transfer speed is increased to 212 or 424 kbit/s, Manchester coding with 10% modulation is employed instead.

NFC (Communication Mode)

- **Active communication mode:** In active mode, both devices involved in the communication are powered and capable of generating their own radio frequency (RF) fields. These devices take turns generating the RF field, allowing them to exchange data bidirectionally. A typical example is the transfer of files between two NFC-compatible smartphones or the exchange of virtual rewards between gaming controllers. When the two smartphones are brought close to each other, they automatically establish a connection. One phone temporarily stops its RF generation to receive data, while the other transmits. This process allows for fast and efficient data sharing, with transfer speeds reaching up to 424 kbit/s.

- **Passive communication mode:** In passive mode, only one device (usually a smartphone or reader) is active and capable of generating an RF field, while the other device is passive, typically an NFC tag that does not have its own power source. The active device generates a carrier electromagnetic field, which powers the passive NFC tag and enables it to modulate the signal for data transmission. This setup is commonly used for access control, such as unlocking office doors using a smartphone. When the phone is brought near the NFC tag, it reads the tag's data, and if access is granted, the system responds—such as unlocking the door—based on the information exchanged. Communication in this mode is generally one-way or simple two-way and is suited for small data transfers.

NFC (Advantages and Disadvantages)

- **Advantages of NFC:**
  - Cost-effective: NFC technology is relatively inexpensive, and the benefits it provides often outweigh the associated costs.
  - Fast and automatic communication: It enables quicker and more seamless communication between compatible devices, often with just a single tap.
  - Backward compatibility: NFC is compatible with existing RFID technologies, allowing it to work with older systems and devices.
  - User-friendly: It does not require specialized knowledge to operate. Users with basic technological skills can easily use NFC-enabled features.
- **Limitations of NFC:**
  - Limited range: NFC functions only within a very short distance, typically no more than four centimeters, which can limit its usability.
  - Security concerns: It is susceptible to security threats like eavesdropping, which may result in the unintentional loss or theft of sensitive information.
  - Slow data transfer: NFC has a low data transfer rate, making it impractical for sharing large files between devices.

NFC (Modes of Operation)

- **Peer-to-peer mode:** This mode is compliant with ISO/IEC 18092 standards. It supports communication and the transfer of information between two NFC-compatible devices. At any point, any device can act as the initiator or a target.

- **Reader/writer mode:** This mode is compatible with the standards established by ISO/IEC 14443 and FeliCa. It allows devices to read NFC tags, such as those that are integrated into smart posters.

- **Card emulation mode:** In this mode, data stored on cards such as smart cards are read by an NFC reader. In this mode, a device that is capable of NFC communication connects with an NFC reader in the same way as a smart card can. Users utilize smartphones to gain access to information, such as ticketing information.

ZigBee

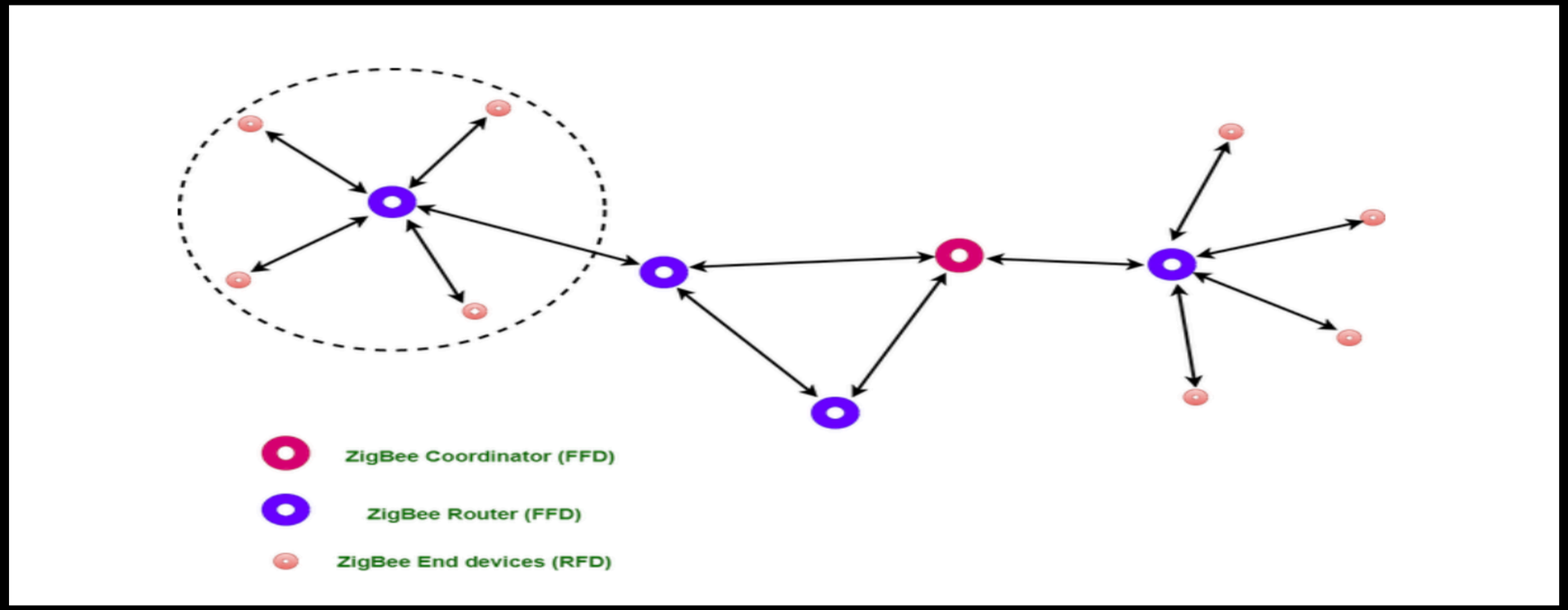
- ZigBee is a wireless communication standard developed under the Personal Area Network (PAN) Task Group 4, which focuses on low data rate and low power consumption. It is primarily used in applications such as home automation, smart lighting, and industrial monitoring.
- The technology is based on the IEEE 802.15.4 standard, which defines the Physical (PHY) and Medium Access Control (MAC) layers. The upper layers of the ZigBee protocol, including network and application layer specifications, are defined by the ZigBee Alliance.
- ZigBee is designed as an open, global, packet-based protocol that offers a flexible and easy-to-deploy architecture. It enables secure, reliable, and low-power wireless communication across a variety of devices.
- A major advantage of ZigBee networks is their ability to function independently of physical layout. Devices such as sensors, pumps, and valves can be placed or relocated freely, as the network can dynamically adjust to their new positions without requiring reconfiguration.

ZigBee

- The IEEE 802.15.4 standard handles the lower communication layers (PHY and MAC), focusing on data transmission over the wireless medium. ZigBee builds upon this by providing the upper layers needed for end-to-end communication, including routing, security, and application services.
- ZigBee addresses the need for a cost-effective wireless solution that supports devices with minimal power requirements and low data rates—typically used in short-range communications where battery life and reliability are crucial.
- In terms of network structure, IEEE 802.15.4 supports both star and peer-to-peer topologies, which provide basic connectivity options for small or simple networks.
- The ZigBee specification expands on this by supporting more advanced topologies, including star, mesh, and cluster-tree configurations. These enable scalable, self-healing networks where devices can communicate over multiple hops.
- ZigBee-compliant devices can operate in various communication modes, such as point-to-point and point-to-multipoint, depending on the specific application and network configuration.

Types of ZigBee

- **Zigbee Coordinator Device:** It communicates with routers. This device is used for connecting the devices.
- **Zigbee Router:** It is used for passing the data between devices.
- **Zigbee End Device:** It is the device that is going to be controlled.



General Characteristics of ZigBee

- Low Power Consumption
- Low Data Rate (20- 250 kbps)
- Short-Range (75-100 meters)
- Network Join Time (~ 30 msec)
- Support Small and Large Networks (up to 65000 devices (Theory); 240 devices (Practically))
- Low Cost of Products and Cheap Implementation (Open Source Protocol)
- Extremely low-duty cycle.
- 3 frequency bands with 27 channels.

Features of ZigBee

- **Stochastic addressing:** A device is assigned a random address and announced. Mechanism for address conflict resolution. Parents node don't need to maintain assigned address table.
- **Link Management:** Each node maintains quality of links to neighbors. Link quality is used as link cost in routing.
- **Frequency Agility:** Nodes experience interference report to channel manager, which then selects another channel
- **Asymmetric Link:** Each node has different transmit power and sensitivity. Paths may be asymmetric.
- **Power Management:** Routers and Coordinators use main power. End Devices use batteries.

Advantages of ZigBee

- Designed for low power consumption.
- Provides network security and application support services operating on the top of IEEE.
- Zigbee makes possible completely networks homes where all devices are able to communicate and be
- Use in smart home
- Easy implementation
- Adequate security features.
- Low cost: Zigbee chips and modules are relatively inexpensive, which makes it a cost-effective solution for IoT applications.
- Mesh networking: Zigbee uses a mesh network topology, which allows for devices to communicate with each other without the need for a central hub or router. This makes it ideal for use in smart home applications where devices need to communicate with each other and with a central control hub.
- Reliability: Zigbee protocol is designed to be highly reliable, with robust mechanisms in place to ensure that data is delivered reliably even in adverse conditions.

Disadvantages of ZigBee

- **Limited range:** Zigbee has a relatively short range compared to other wireless communications protocols, which can make it less suitable for certain types of applications or for use in large buildings.
- **Limited data rate:** Zigbee is designed for low-data-rate applications, which can make it less suitable for applications that require high-speed data transfer.
- **Interoperability:** Zigbee is not as widely adopted as other IoT protocols, which can make it difficult to find devices that are compatible with each other.
- **Security:** Zigbee's security features are not as robust as other IoT protocols, making it more vulnerable to hacking and other security threats.

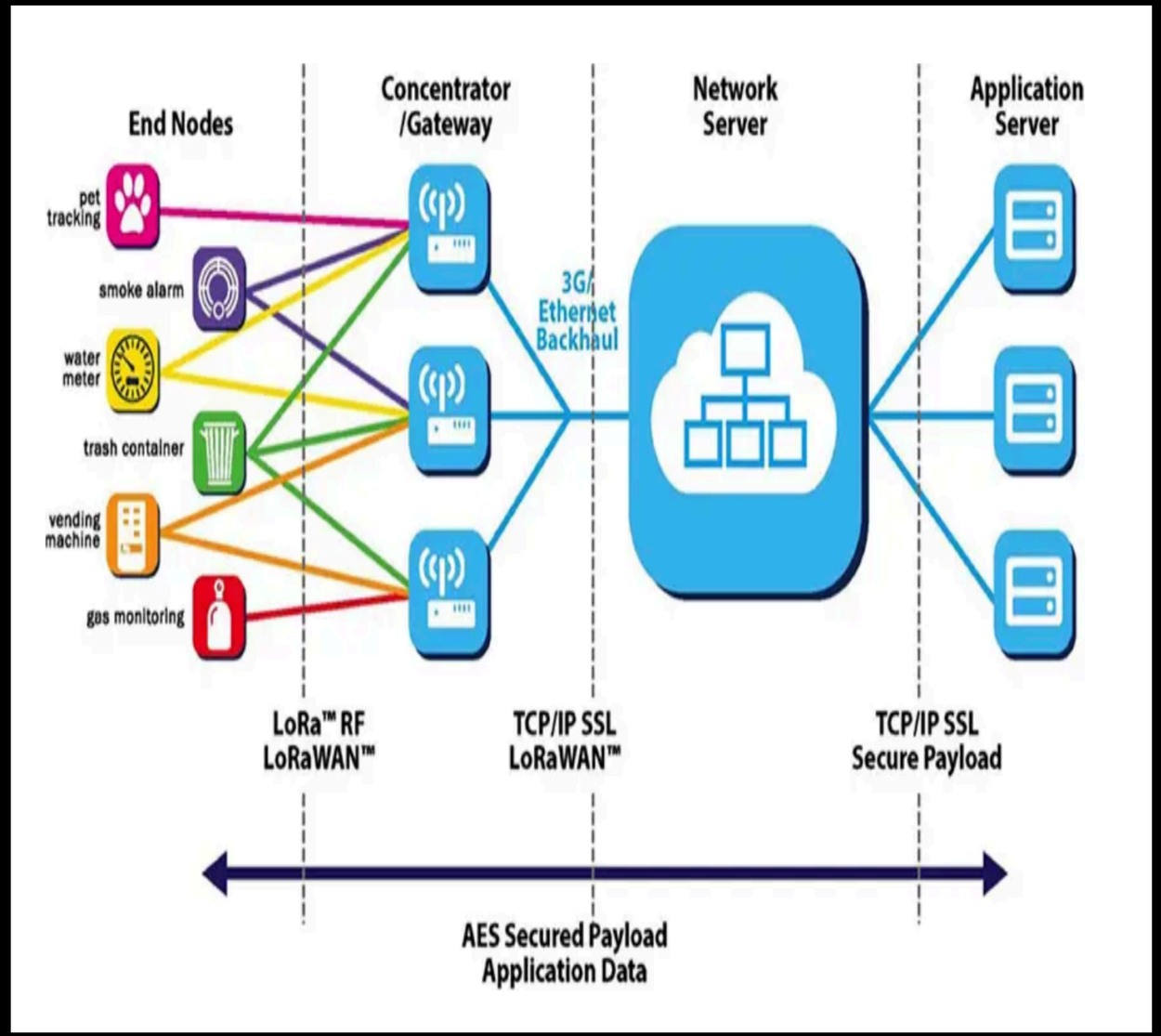
LORA

- LoRa, short for Long Range, is a wireless radio frequency technology that enables long-range, low-power communication between devices.
- LoRa is the physical layer or the wireless modulation utilized to create the long range communication link. LoRa is based on chirp spread spectrum modulation. LoRa is the first low cost implementation for commercial usage.
- LoRa is not a communication protocol but a modulation technique, a way of encoding data on radio waves so that devices can talk to each other efficiently. When combined with the LoRaWAN protocol stack, we can build a full-blown long-range communication network for IoT devices.
- Most wireless tech follows this trade-off: more range = more power. But LoRa breaks this pattern. Compared with traditional ASK and FSK modulation, LoRa is based on chirp spread spectrum (CSS) modulation, which can greatly increase the communication range, so it can achieve a transmission range of several kilometers with extremely low power consumption.

Network Architecture

- **LoRa nodes:** The end nodes are the elements of the LoRa network where the control or sensing is undertaken. They are normally battery-powered and remotely located. End nodes send data to every gateway in their vicinity and they transmit data in periodic not 24×7.

- **Network Server:** The network server manages the network. It filters duplicate packets caused by multiple gateways receiving the same data, performs security checks, manages gateway traffic and routing, control adaptive rate, and forwards messages to the application server.



Network Architecture

- **Application Server:** The application server processes data from the network server, analyzes sensor data, supports functions like status display and real-time alerts, and can optionally send responses back to the end node.

- **LoRa gateway:** The gateway receives the data from the LoRa end nodes and then channels it to a network server. A LoRa gateway usually consists of a LoRa radio module, a microprocessor, and an Internet connectivity medium. The gateway converts the data received from the LoRa nodes into TCP/IP format via the backhaul network (Ethernet, 3G, 4G, WiFi, etc.) and sends it to the network server. LoRa gateway supports multi-channel, multi-modulation transceivers, and even simultaneous demodulation of signals on the same channel. They do not store any data and act only as packet forwarders to the network server. A gateway can connect many terminal devices. An SX1301 with 8 channels can handle about 1.5 million packets per day, supporting around 62,500 devices sending one packet per hour.

Advantages

- **Long range:** Connects devices up to 15-20 km in rural settings and 2-5 km in urban areas. Permits city-scale coverage, and good penetration of buildings is achieved.
- **Low power and long lifespan:** Designed for low power use with prolonged battery life up to 10 years. For example, MOKOSmart LW009 LoRaWAN Parking Sensor can operate up to 5 years.
- **High capacity:** A single LoRa gateway can handle millions of messages from thousands of end nodes.
- **Low cost:** Low initial infrastructure investment, free ISM frequency band, and inexpensive end node sensors.
- **Open standard:** LoRaWAN is maintained by the LoRa Alliance. Drives speedy deployment and device interoperability.

Disadvantages

- **Low transmission speed:** LoRa has a relatively narrow bandwidth and its ability to transmit over long distances comes at the cost of lower data rates, making it suitable for sensor networks not high-data applications.
- **Limited payload:** LoRa supports only small data packets, with a maximum data capacity of about 242 bytes per transmission. This makes it less suitable for use cases that need large data transfers.

Application

- **Smart cities:** Smart metering, environmental monitoring, smart parking, street lighting, waste management and more.
- **Supply chain and logistics:** Asset tracking and monitoring, cold chain monitoring, fleet management.
- **Agriculture:** Soil monitoring, irrigation control, livestock tracking.
- **Industrial IoT:** Equipment monitoring, predictive maintenance, automation.
- **Infrastructure monitoring:** Monitor railway tracks, bridges, and tunnels for any physical changes.
- **Utilities:** Smart grid, gas/water metering, leak detection, distributed power generation.
- **Smart homes and buildings:** HVAC and lighting control, energy management, room occupancy monitoring.

Data Compression

Data compression is the process of encoding information using fewer bits than an un-encoded representation would use, through specific encoding schemes. It reduces consumption of expensive resources such as hard drive and transmission bandwidth. There is a trade-off between compression speed, compressed data size and quality (loss).

Lossy	Lossless
For the case if loss of fidelity is acceptable. E.g. 6.666666 = 7	Exploit statistical redundancy in such a way to represent data without error. E.g. 6.666666 = 6[6]6
Examples: Pictures (PEG), Video (MPEG), Audio (MP3), etc.	Examples: zip, ra, Picture (PNG, TIFF), Video (Huff,YUV, AVI), etc.

Raid 0 Striping

Features

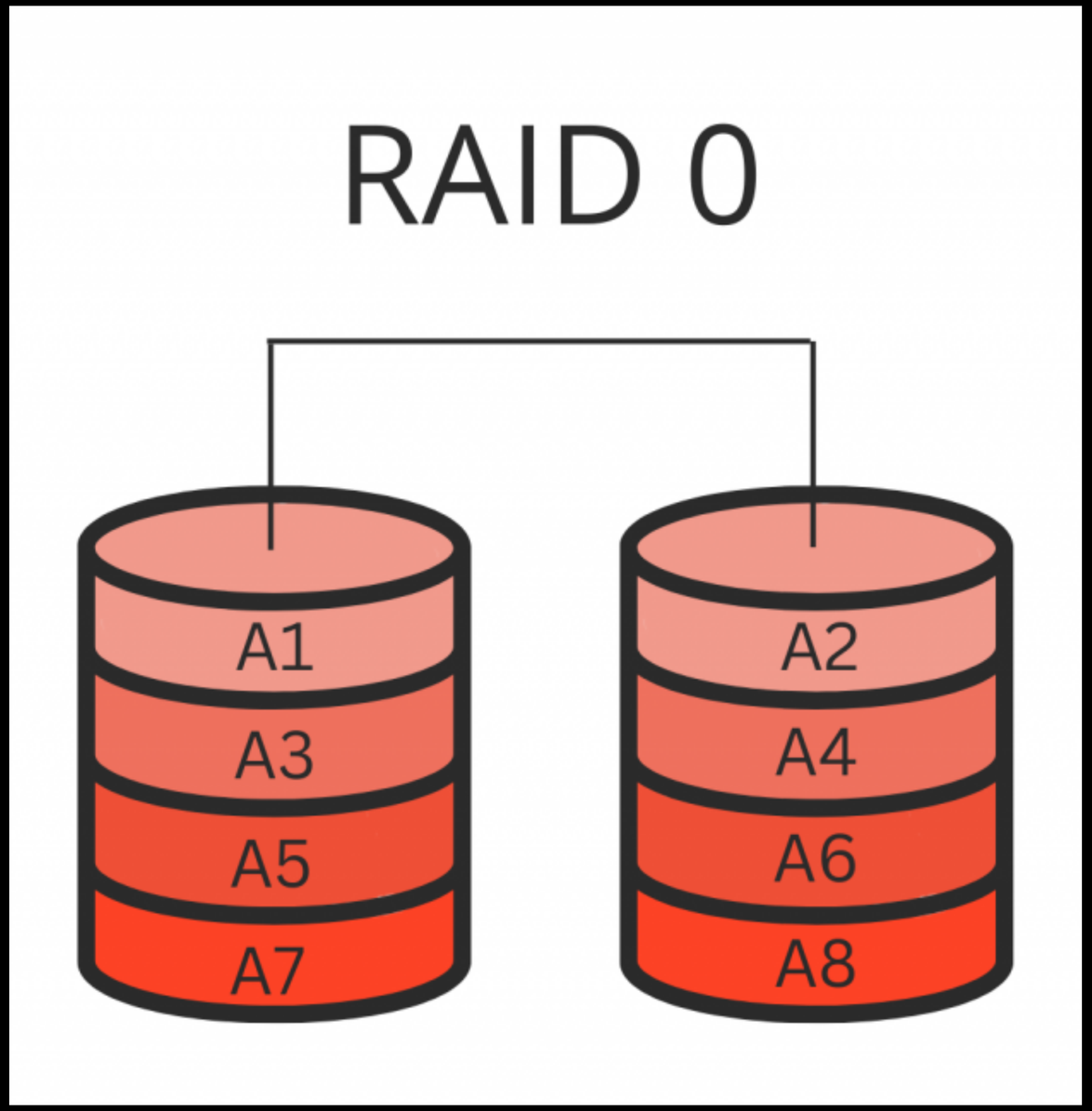
- Data is split evenly (striped) across two or more disks.
- No redundancy.
- Minimum 2 disks required.

Advantages

- High read and write performance.
- Full disk capacity is usable.

Disadvantages

- No fault tolerance—if one disk fails, all data is lost.
- Not suitable for critical data storage.



Raid 1 Mirroring

Features

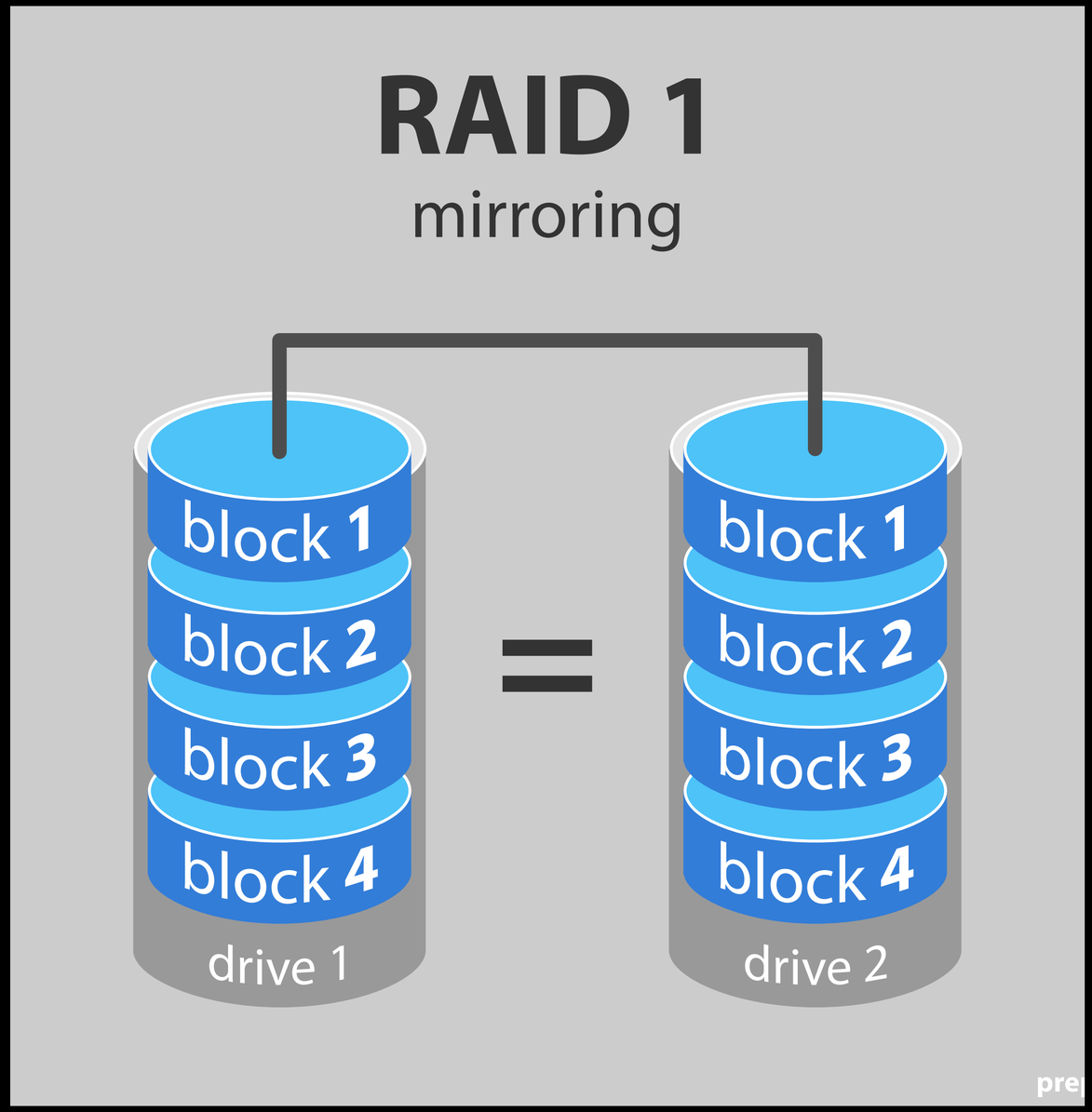
- Exact copy (mirror) of data on two or more disks.
- Minimum 2 disks required.

Advantages

- High data reliability.
- Simple recovery in case of disk failure.

Disadvantages

- Storage capacity is halved.
- Higher cost per GB (since data is duplicated).



Raid 5 Striping with Distributed Parity

Features

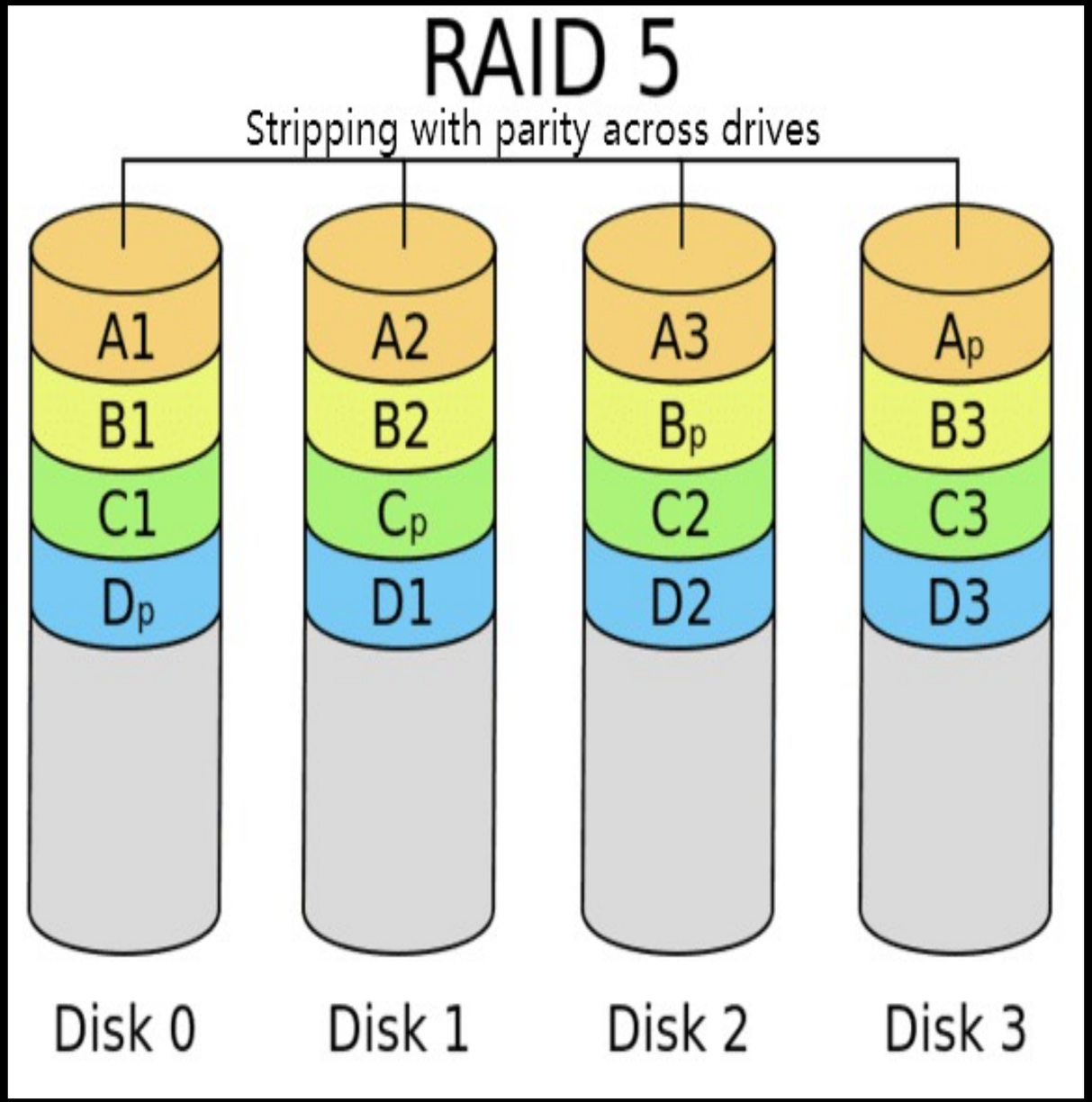
- Data and parity (error correction) are striped across all disks.
- Can tolerate failure of 1 disk.
- Minimum 3 disks required.

Advantages

- Efficient storage with redundancy.
- Good read performance.
- Can recover from single disk failure.

Disadvantages

- Slower write performance due to parity calculations.
- Rebuilding after disk failure is slow and risky.



Raid 6 Striping with Double Parity

Features

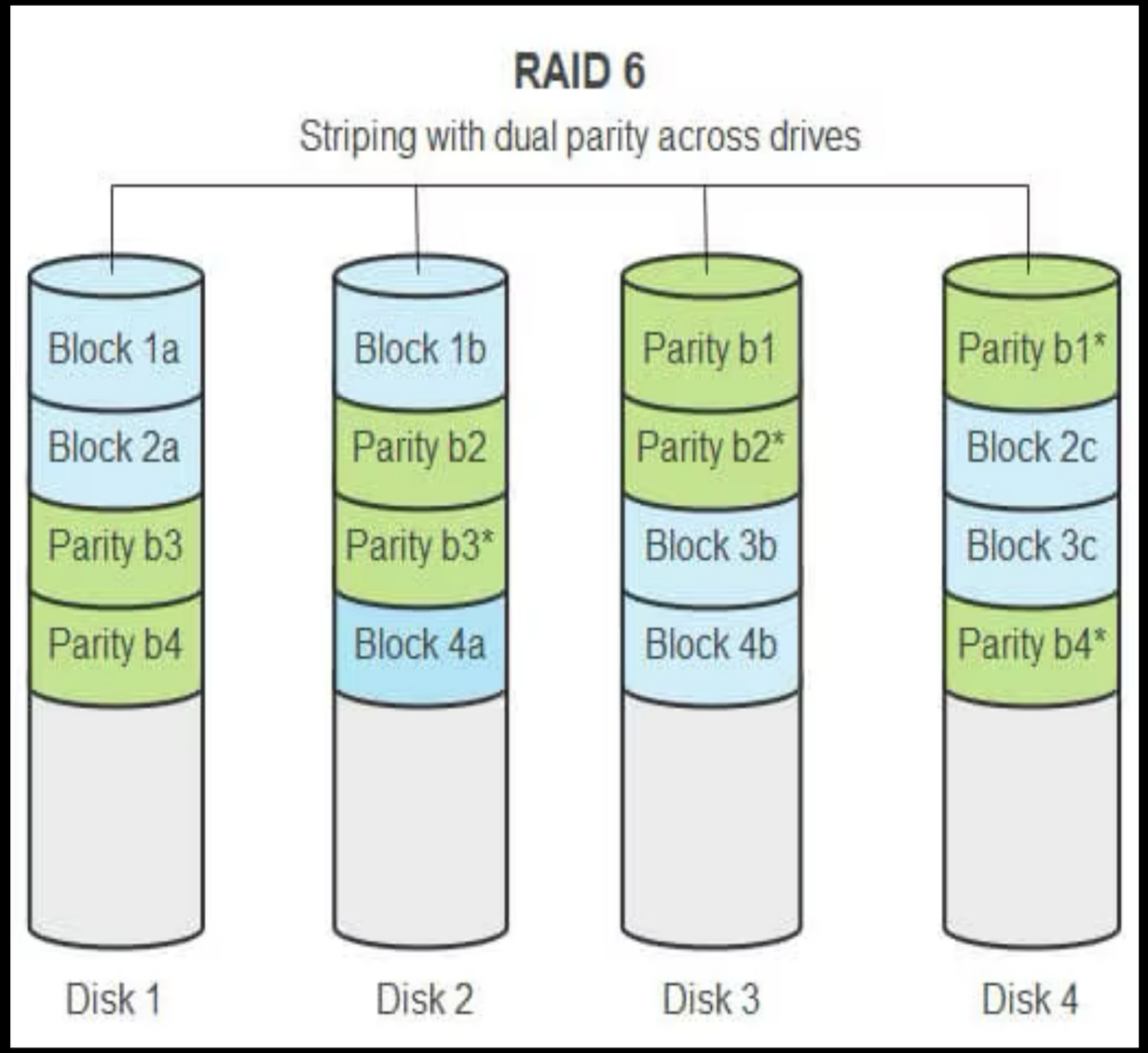
- Similar to RAID 5 but with two parity blocks.
- Can tolerate failure of two disks.
- Minimum 4 disks required.

Advantages

- Higher fault tolerance than RAID 5.
- Good read performance.

Disadvantages

- Slower write speed than RAID 5 (due to double parity).
- Rebuild times can be very long.



Raid 10 Mirroring + Striping

Features

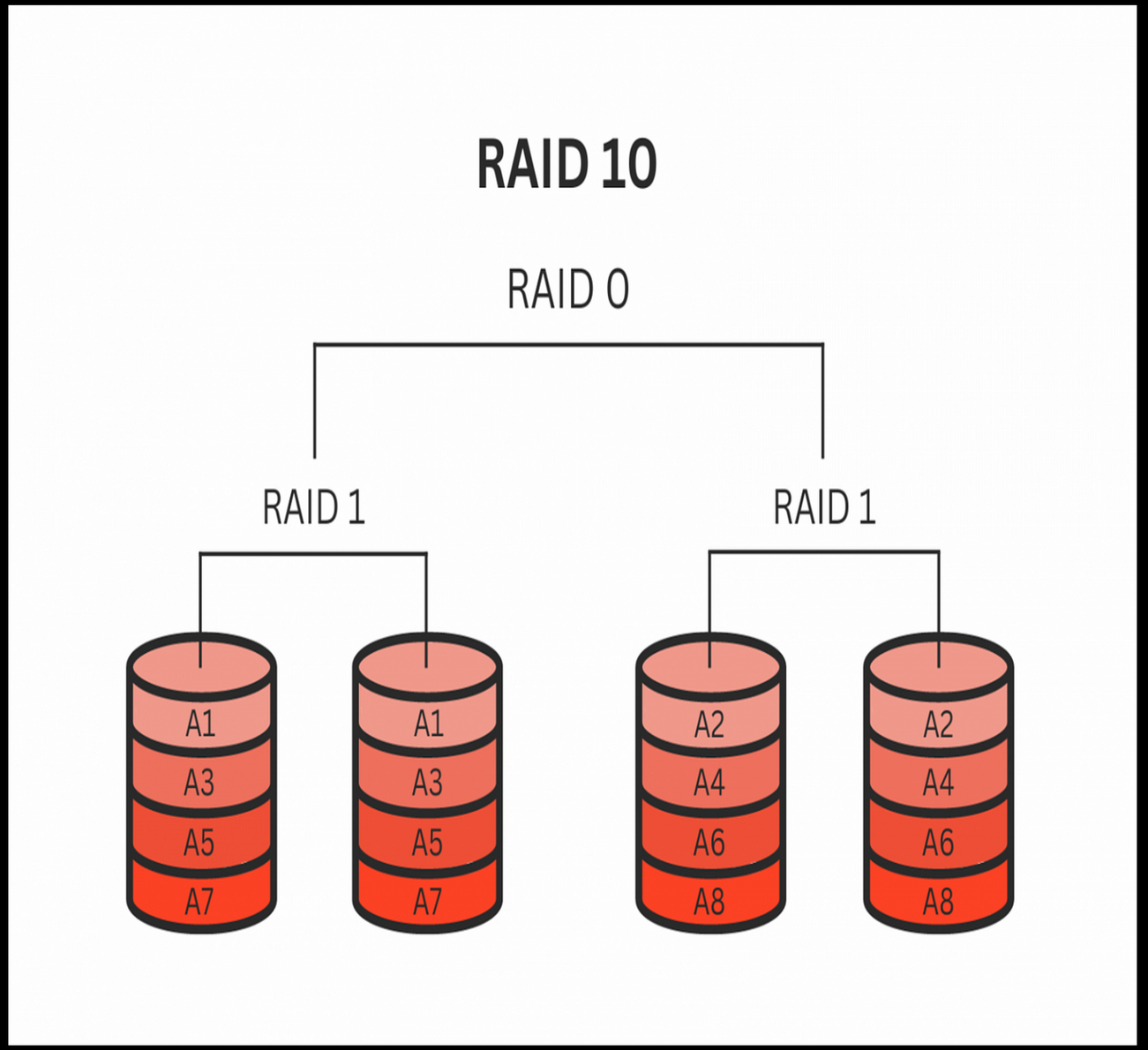
- Combines RAID 1 (mirroring) and RAID 0 (striping).
- Requires minimum 4 disks.
- Data is mirrored in pairs and then striped.

Advantages

- High performance and high redundancy.
- Can survive multiple disk failures (depending on which disks fail).

Disadvantages

- Expensive—only 50% of total storage is usable.
- Requires more disks than other RAID levels.



Raid	Min Disks	Redundancy	Performance	Storage Efficiency	Tolerates Failure
0	2	No	Very High	100%	None
1	2	Yes	High	50%	1 disk
5	3	Yes	Good	67-94%	1 disk
6	4	Yes	Good	50-88%	2 disks
10	4	Yes	Very High	50%	Upto 2 (depends)