VIT®
BHOPAL

Embedded Networking Technologies

Instructor: Dr. Ankur Beohar
School of Electrical and Electronics Engineering
VIT Bhopal University

Embedded Systems

- Suggested Textbooks:
  - Raj Kamal, “Embedded systems Architecture, Programming and Design”, Third Edition, Tata McGraw Hill, 2017.
  - Rob Toulson and Tim Wilmshurst, “Fast and Effective Embedded Systems Design – Applying the ARM mbed”, Elsevier, 2017.
  - Arnold S. Berger, “Embedded Systems Design: An Introduction to Processes, Tools, and Techniques”, CRC Press, 2002.
- Other sources
  - Lecture notes
  - Handouts
  - Blogs
  - MOOC courses

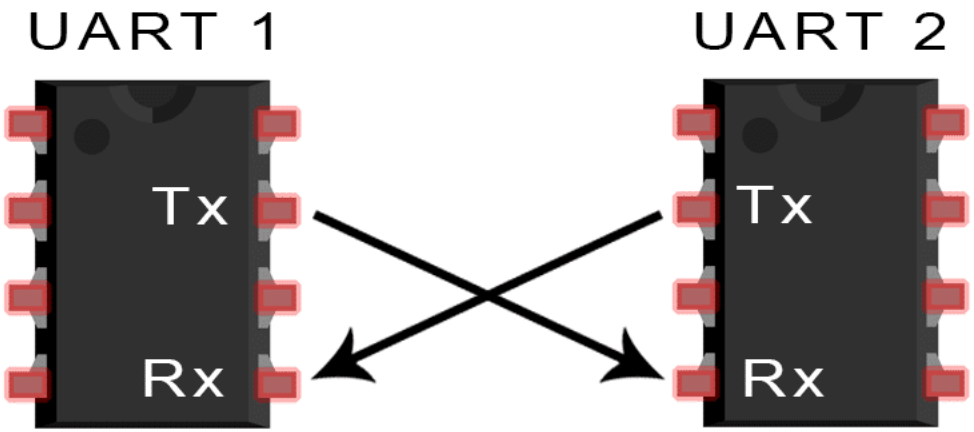
UART

UART

- **Universal Asynchronous Receiver and Transmitter**
- It is a single LSI (large scale integration) chip designed to perform asynchronous communication.
- The function of UART is to convert the incoming and outgoing data into the serial binary stream.
- An 8-bit serial data received from the peripheral device is converted into the parallel form using serial to parallel conversion and parallel data received from the CPU is converted using parallel to serial conversion.
- When high-speed data transfer is not required UART is used

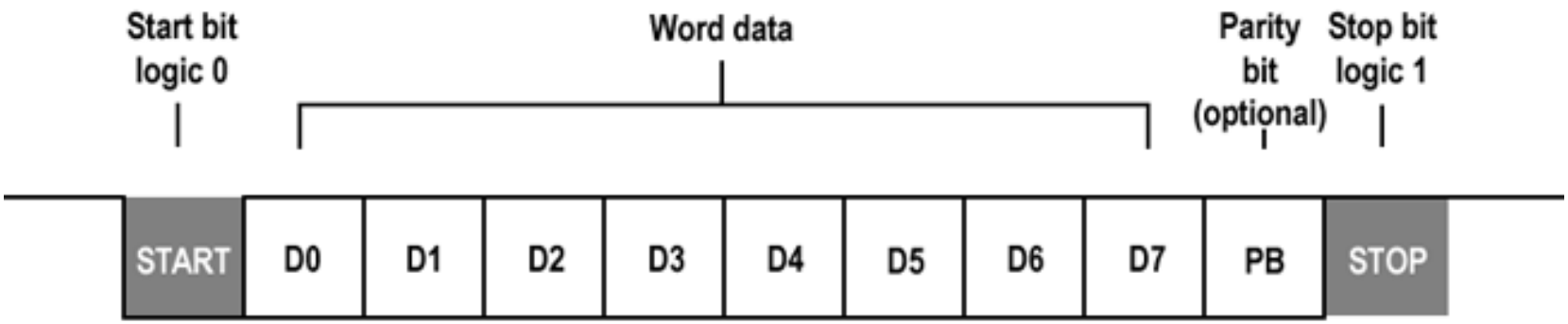
UART

- UART is a simple half-duplex, asynchronous, serial protocol
- Simple communication between two equivalent nodes
- Any node can initiate communication



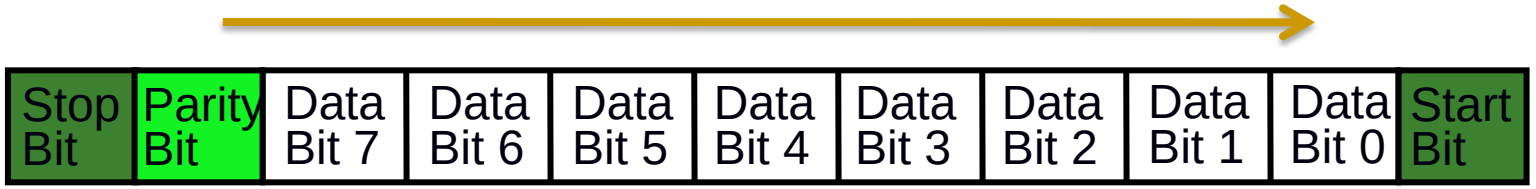
UART

- What makes it ‘universal’ ?
  - Its parameters (format, speed ..) are configurable
- Why ‘asynchronous’ ?
  - It doesn’t have a clock
- Format of Communication



UART

- Baud Rate
  - In telecommunication and electronics, baud is a common measure of the speed of communication over a data channel. Technically speaking, it is the unit for symbol rate or modulation rate in symbols per second or pulses per second.
  - If the baud rate is 4800 and there are 2 bits per symbol, then bit rate R = 4800 * 2 = 9600 bits/sec
- Sequence of Transmission



UART Advantages

- Only uses two wires
- No clock signal is necessary
- Has a parity bit to allow for error checking
- The structure of the data packet can be changed as long as both sides are set up for it
- Well documented and widely used method

UART Disadvantages

- The size of the data frame is limited to a maximum of 9 bits
- Doesn't support multiple slave or multiple master systems
- The baud rates of each UART must be within 10% of each other

SPI

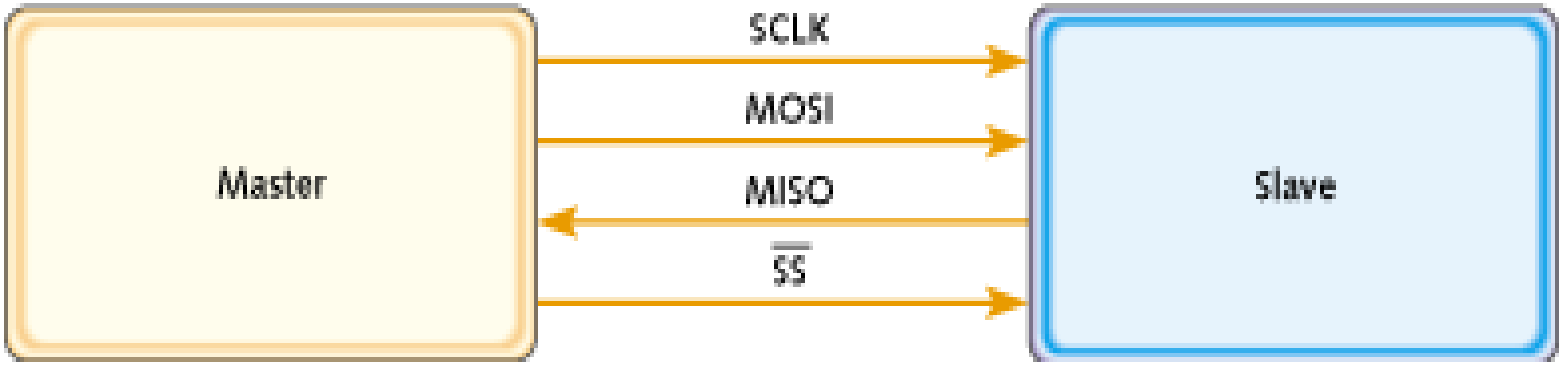
SPI

- SPI stands for '**S**erial **P**eripheral **I**nterface'.
- The SPI standard was developed by Motorola.
- It is a serial data transfer protocol, which is synchronous and full duplex.
- Full duplex – data can be sent in both directions simultaneously between the controller unit and a peripheral.
- It is a single master and multi-slave system, in which one of the slaves to be enabled at a time.
- It is a master – slave protocol, where the master is the unit that generates clock signal and initiates data transfer.
- When the master does this, data transfer occurs in both direction.

SPI Signals

- The SPI bus specifies four logic signals.
  - SCLK - Serial Clock (output from master)
  - MOSI - Master Output, Slave Input (output from master)
  - MISO - Master Input, Slave Output (output from slave)
  - SS - Slave Select (active low; output from master)
- Alternative naming conventions
  - SCK, CLK - Serial Clock (output from master)
  - SDI, DI, SI - Serial Data In
  - SDO, DO, SO - Serial Data Out
  - SSEL - Slave Select

TYPICAL SPI CONFIGURATION



1. The master pulls the slave select low and then issues clock cycles.
2. The clock frequency is not specified in the SPI protocol and can be anything from 0 up to 70MHz depending on the characteristics of the slave device.
3. The data transfer then takes place.
4. The master then de-selects the slave.

SPI Protocol

- The transfer of data using a SPI interface can be thought of as a large shift register shared between the master and the slave devices.
- Data is clocked IN at the same time as it is clocked OUT of the device.
- This is only possible if these devices share common clock.
- In addition to this, there should be a transmit buffer register at the transmitter side and a receive buffer register at the receiver side.
- The SPI protocol behaves like a ring buffer, so that whenever the master sends a byte to the slave, the slave sends a byte back to the master.
- Essentially two action takes place in a SPI clock cycle

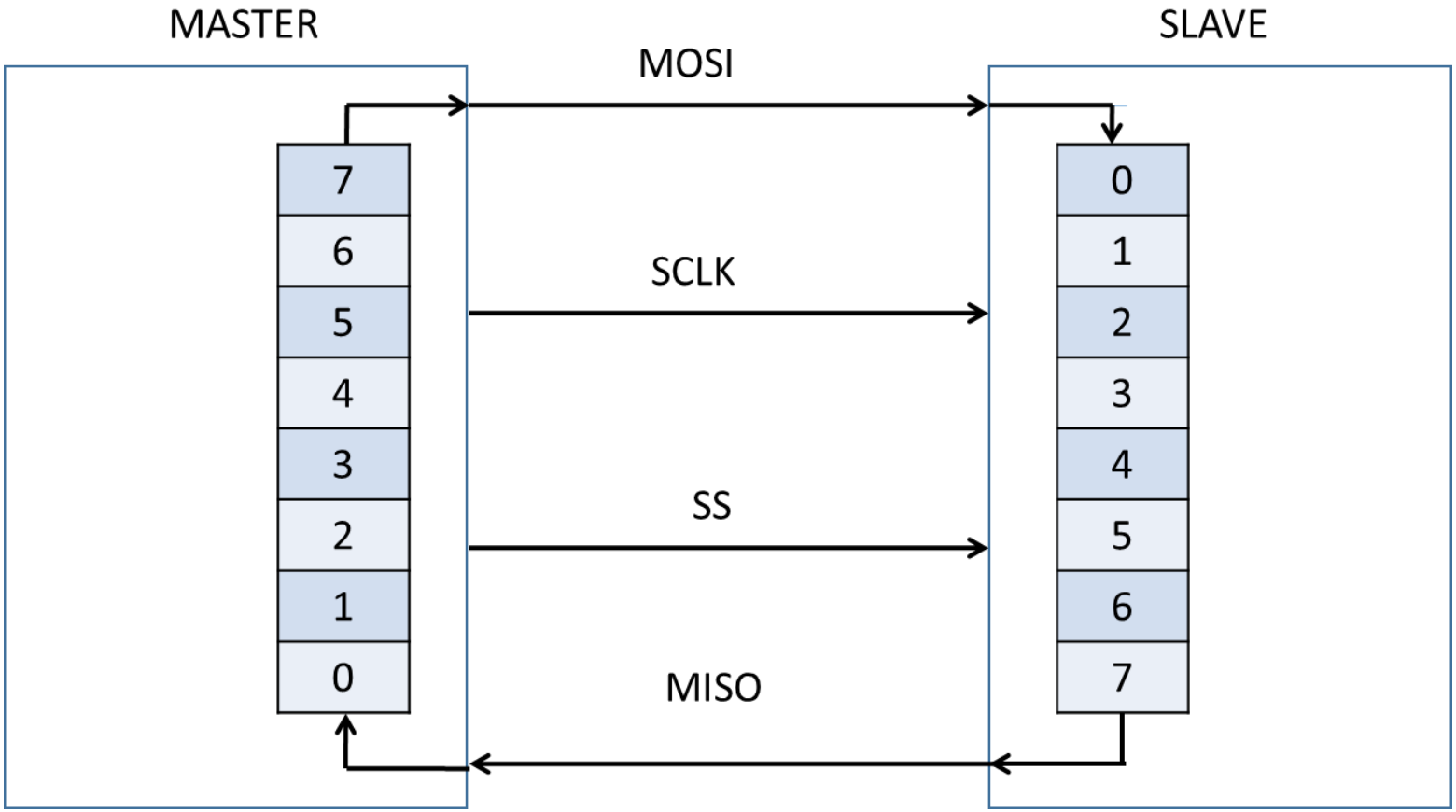
  1) Master sends a bit on the MOSI line which the slave reads from the same line.

  2) Slave sends a bit on the MISO line and the master reads it from the same line.

SPI Protocol

- There are shift registers in the master and slave which are serially connected using MISO and MOSI pins.
- In this interconnection, a bit is shifted from master to slave and slave to master simultaneously (full duplex).
- If individual shift registers are 8 bit long, after 8 clock cycles data is transferred from master to slave.
- The length of the shift register is decided by the manufacturer of SPI controller.

Basic Serial Data Transfer



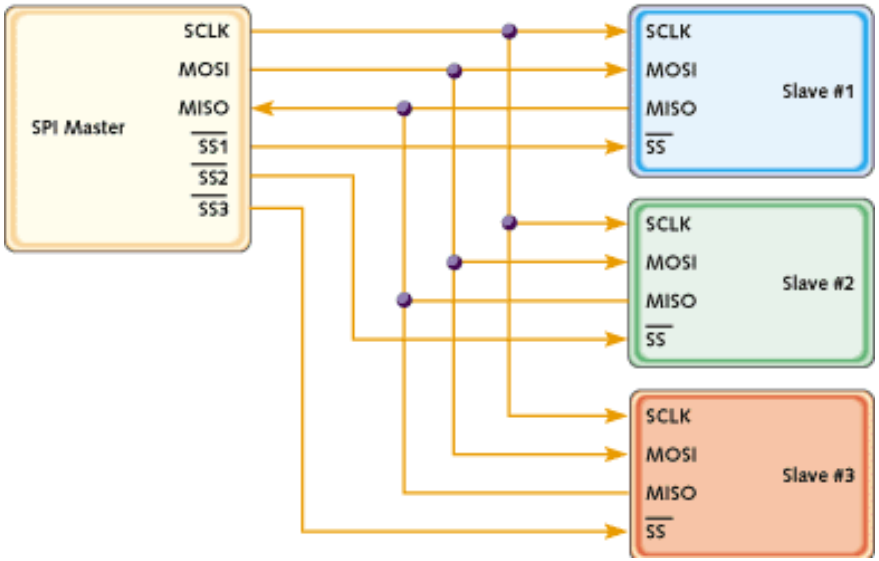
- The registers within the master and slave act like shift registers shifting one bit on every cycle of the SCLK.

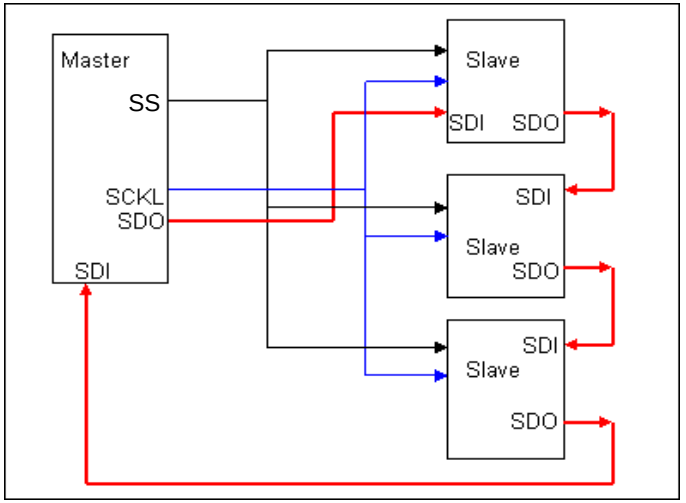
Basic Serial Data Transfer

- Once a set of data has been transmitted, the buffer at the transmitter side should get a fresh data to be sent.
- Similarly the receiver data should be copied and saved at the receiver side.
- This process continues till the required block of data is transferred.

Multiple Slaves

- If multiple slave devices exist, the master normally generates a separate slave select signal for each slave. - Star connection.





Alternative daisy chain connection -requires only one slave select signal

Multiple Slaves

- The master is usually a controller which has an SPI controller with the specified pins.
- The SPI controller in the master has three SS pins, but one slave is selected at a time.
- Slaves that are currently not selected should have their MOSI and MISO tri stated and thus isolated from the system.

SPI Bus Characteristics

- It is up to the master and slave devices to know whether a received byte is meaningful or not.
- No Acknowledgement
- Master doesn't even know if slave is present!
- Slaves can be thought of as IO devices of the master.

SPI Advantages & Limitations

Advantages

- Full duplex communication
- Higher throughput than I2C
- Not limited to 8-bit word in case of bit transfer
- Slaves use masters clock
- Low power requirement than I2C circuit

Limitations

- Require more pins in the IC package
- No slave acknowledge
- Multi master buses are rare and awkward. Normally limited to single slave.

I2C Protocol

I2C

- I2C : **Inter - Integrated Circuit**
- Bus Developed and patented by Philips for connecting low speed peripherals
- On – board Bus protocol
- Has become a worldwide industry standard and used by all major IC manufacturer
- I2C is a serial protocol for two wire interface to connect low speed devices
- I2C combines best features from SPI and UART.
- Today, a variety of devices are available with I2C Interfaces
  - Microcontroller, EEPROM, Real-Timer, interface chips, LCD driver, A/D converter

Terminology

- Transmitter
  - The device that puts data on the bus
- Receiver
  - The device that receives data from the bus
- Master
  - Initiates and terminates a transfer by generating start and stop conditions
  - Generates the clock
  - A master can be either a transmitter or a receiver
- Slave
  - Responds only when addressed
  - A slave can be either receiver or transmitter

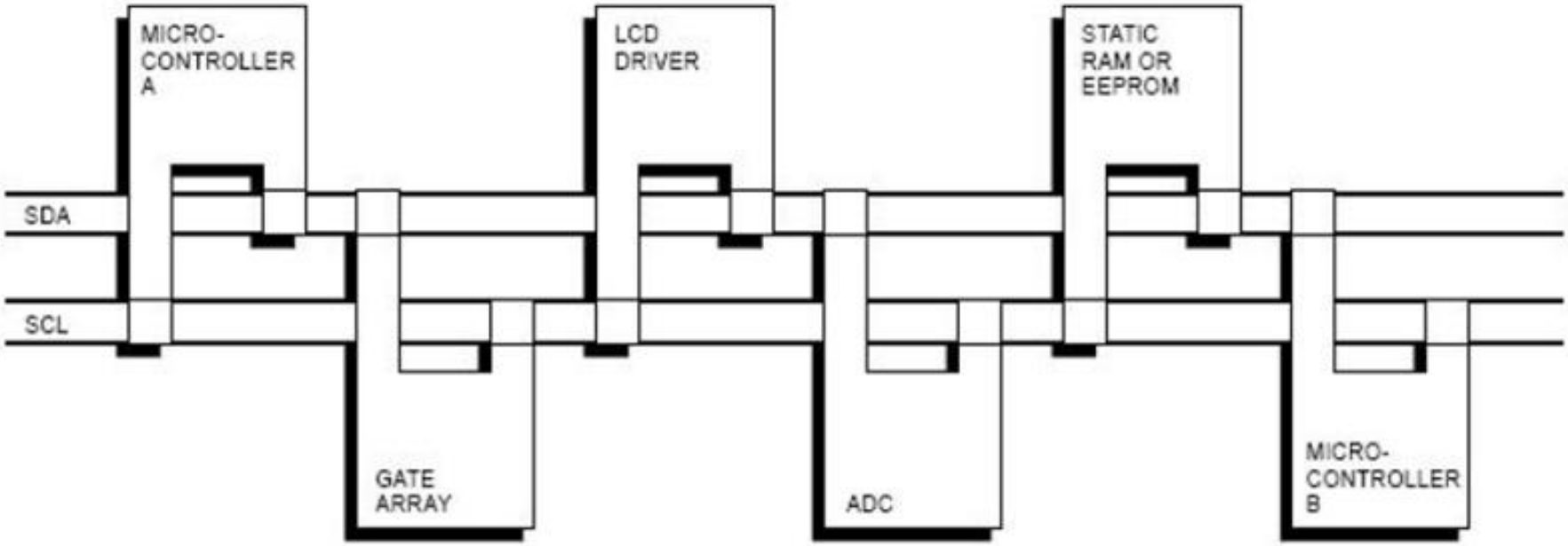
Why I2C?

- Data transfer between ICs and systems at relatively low rates
  - “Classic Mode” - up to 100K bits/second
  - “Fast Mode” - up to 400K bits/second
  - “High Speed Mode - up to 3.4M bits/second
- Reduces Board Space and Cost By
  - Allowing use of ICs with fewer pins and smaller packages
  - Greatly reducing interconnect complexity
  - Allowing digitally controlled components to be located close to their point of use

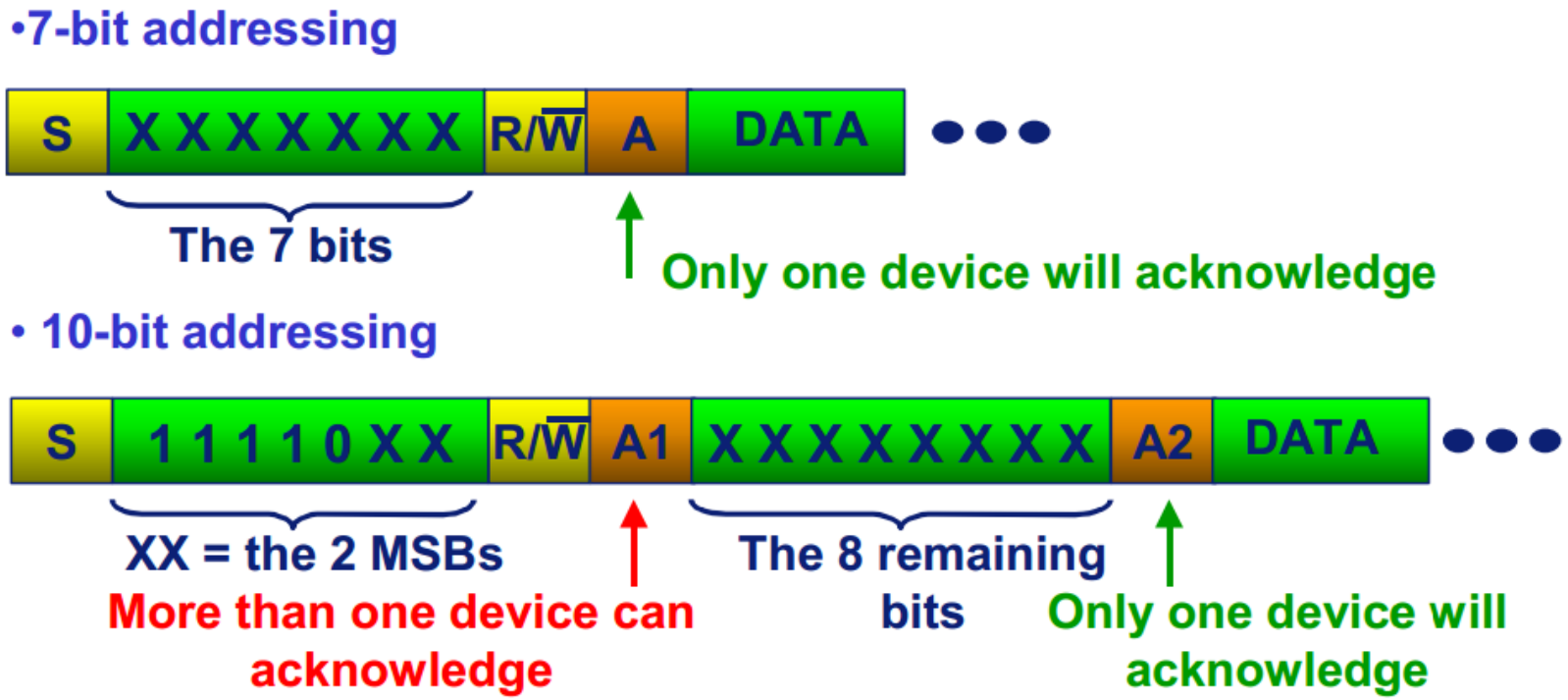
I2C Characteristics

- Includes electrical and timing specifications, and an associated bus protocol
- Simple bi-directional 2-wire bus hence also called TWI
  - serial data (SDA) line
  - serial clock (SCL) line
- It is synchronous, half duplex, serial protocol
- Unique start and stop condition
- Slave selection protocol uses a 7/10 - Bit slave address
- Acknowledgement after each transferred byte
- No fixed length of transfer

I2C Configuration Example

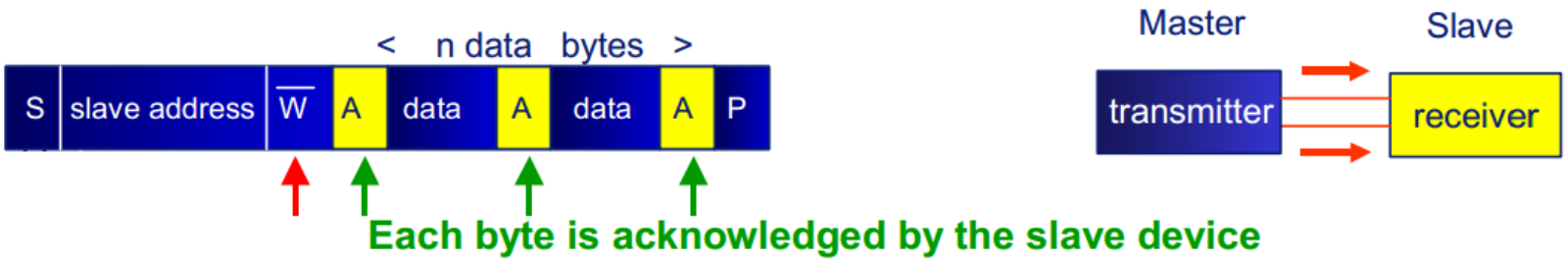


Addressing, 7-bit and 10 bit format

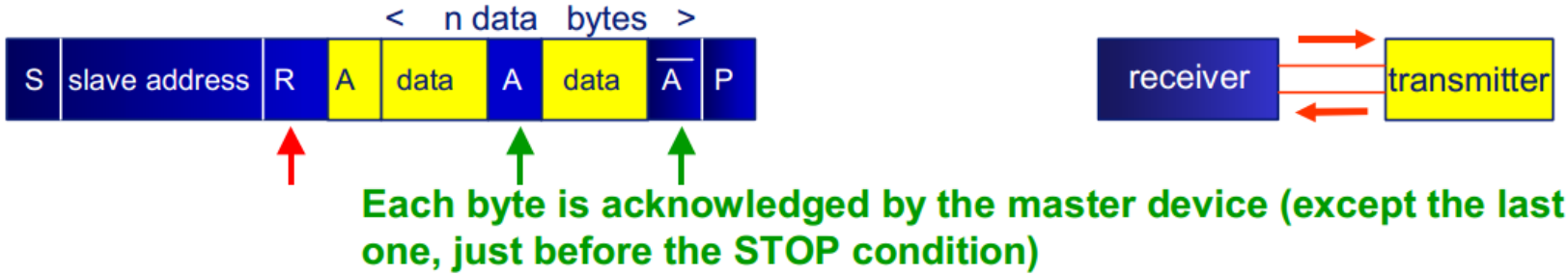


Data Formats

- Master writing to a Slave

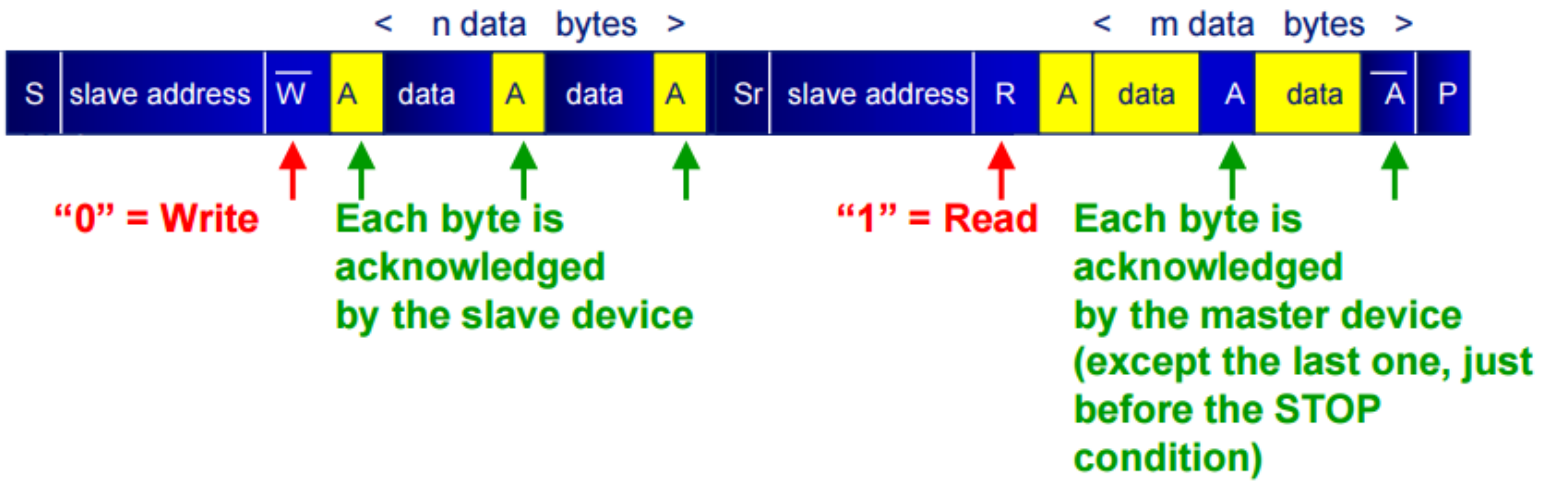


- Master reading from a Slave



Data Formats

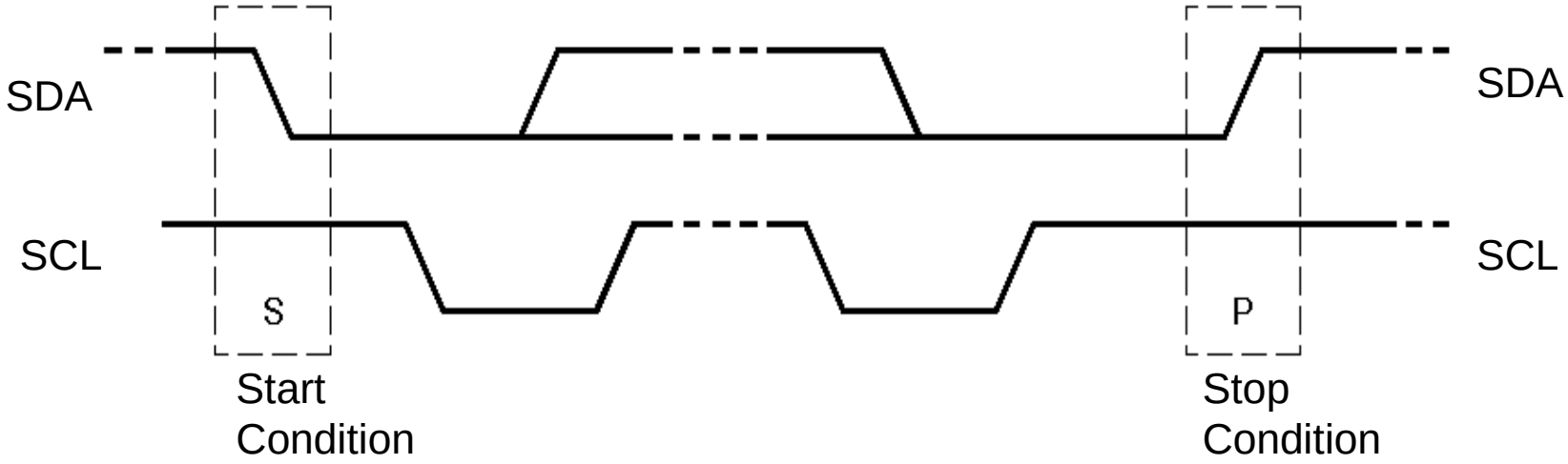
- Combined Write and Read Format



- A repeated start avoids releasing the bus and therefore prevents another master from taking over the bus

Start and Stop Conditions

- A transition of the data line while the clock line is high is defined as either a start or a stop condition.
- Both start and stop conditions are generated by the bus master
- The bus is considered busy after a start condition, until a stop condition occurs



How I2C Works?

Start Condition: The SDA line switches from a high voltage level to a low voltage level *before* the SCL line switches from high to low.

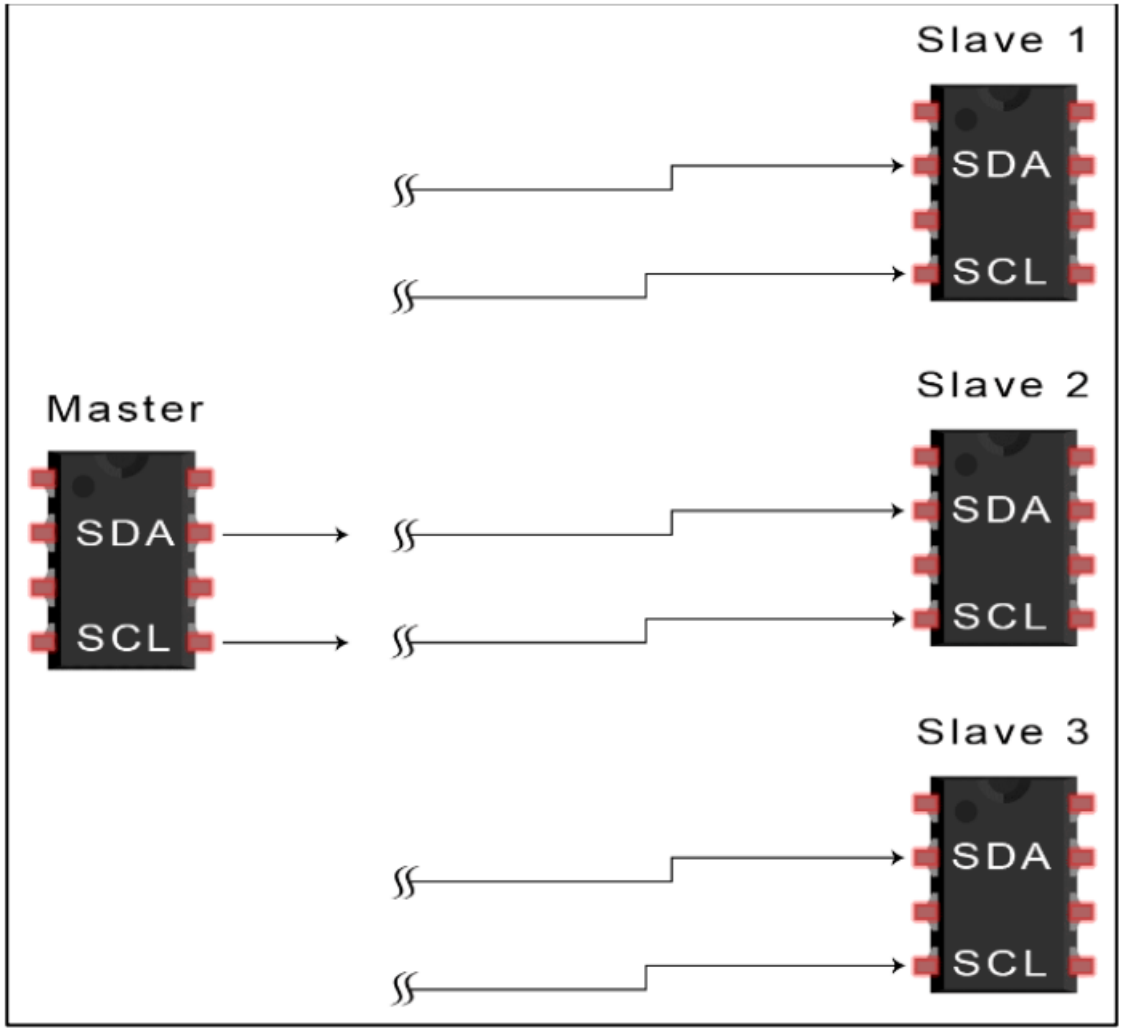
Stop Condition: The SDA line switches from a low voltage level to a high voltage level *after* the SCL line switches from low to high.

Address Frame: A 7 or 10 bit sequence unique to each slave that identifies the slave when the master wants to talk to it.

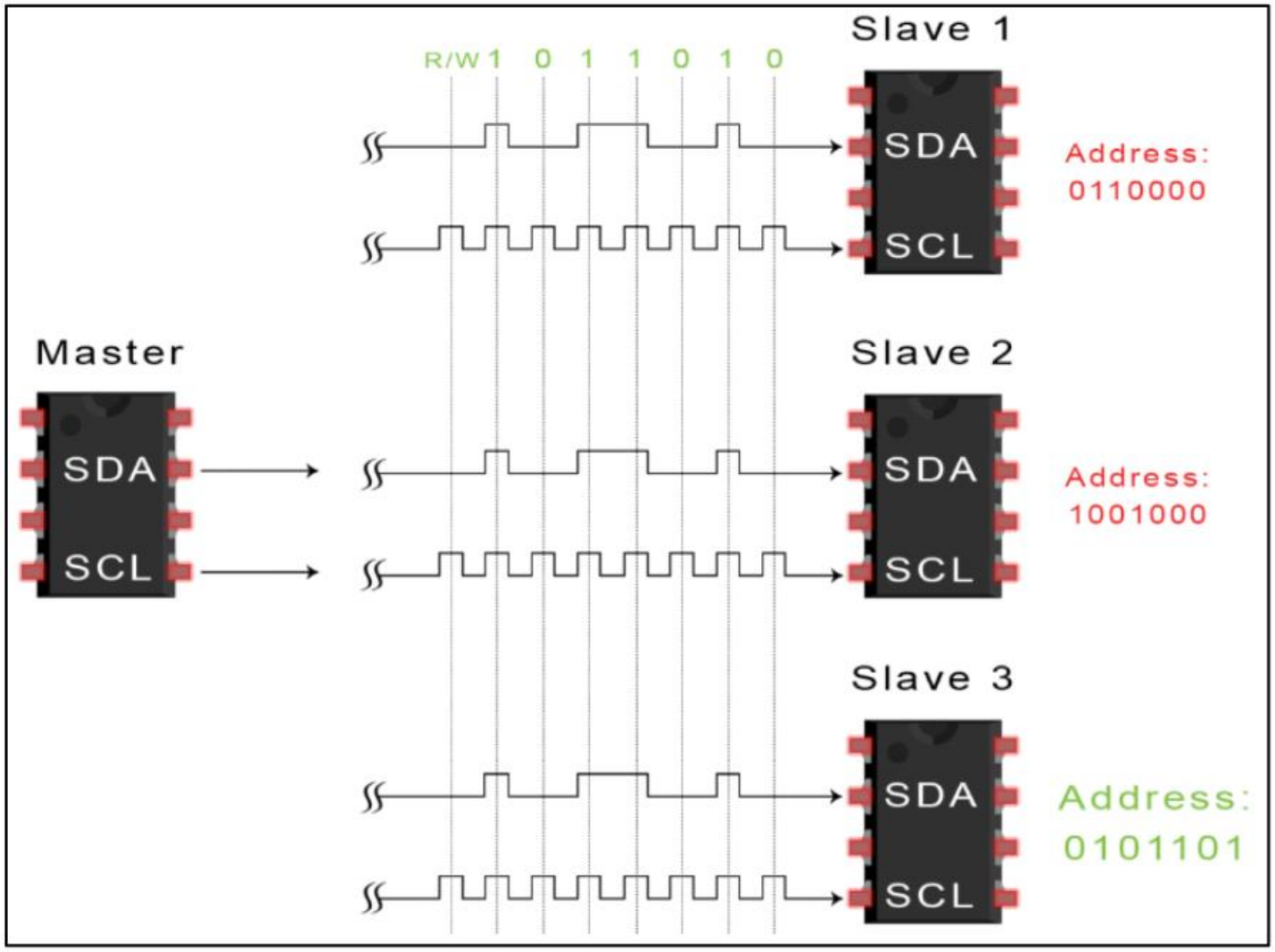
Read/Write Bit: A single bit specifying whether the master is sending data to the slave (low voltage level) or requesting data from it (high voltage level).

ACK/NACK Bit: Each frame in a message is followed by an acknowledge/no-acknowledge bit. If an address frame or data frame was successfully received, an ACK bit is returned to the sender from the receiving device.

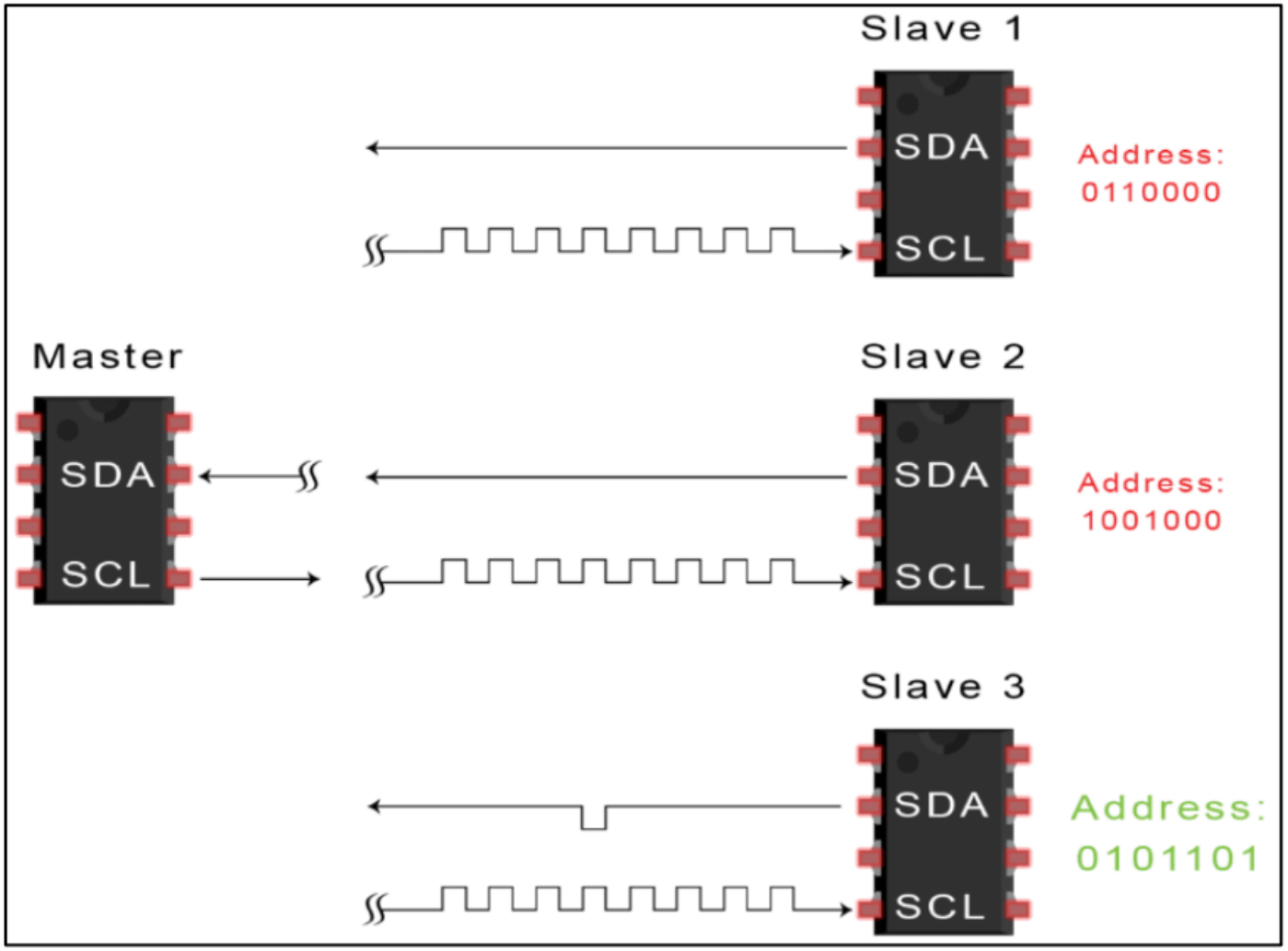
Steps of I2C Data Transmission



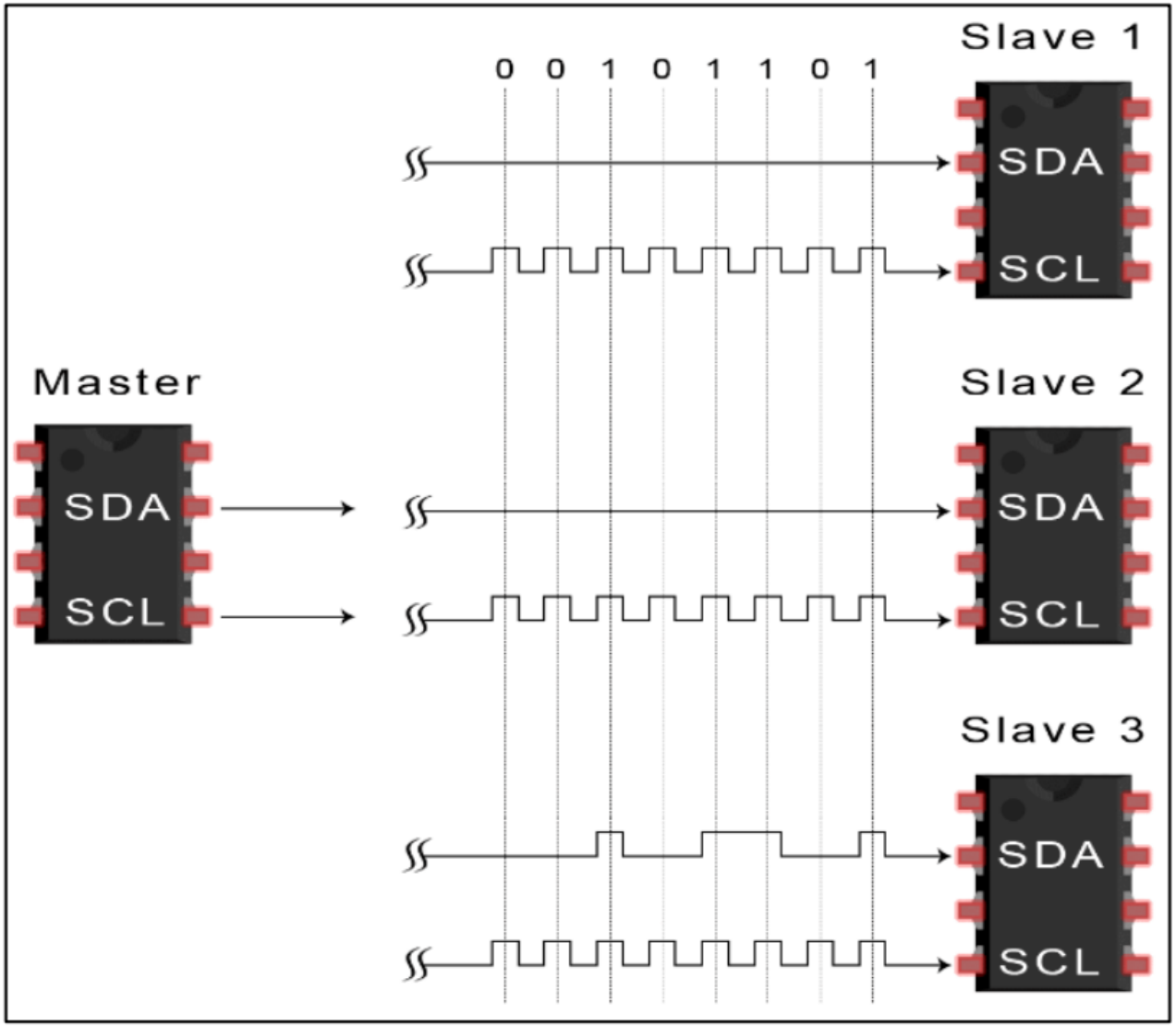
Steps of I2C Data Transmission



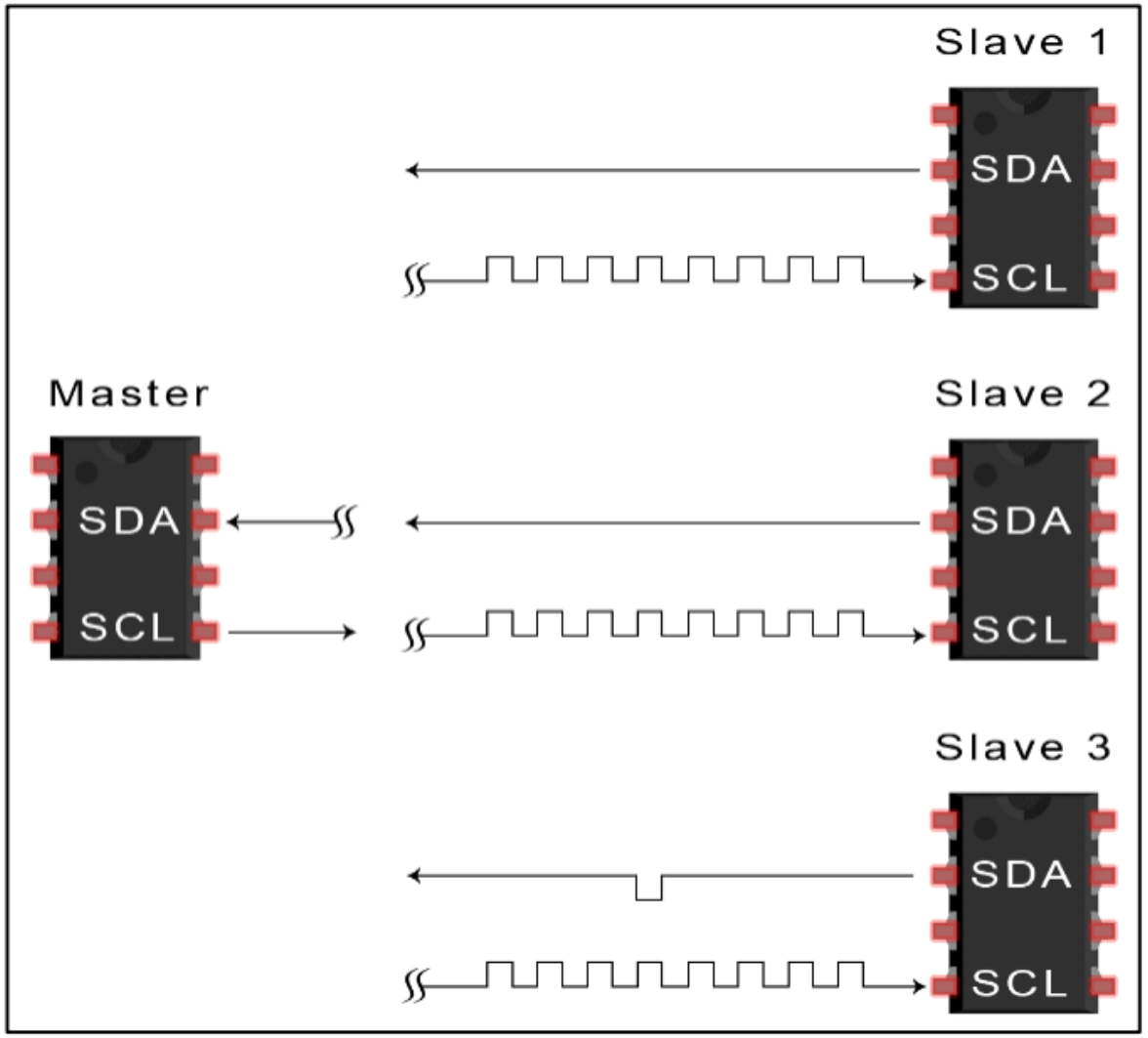
Steps of I2C Data Transmission



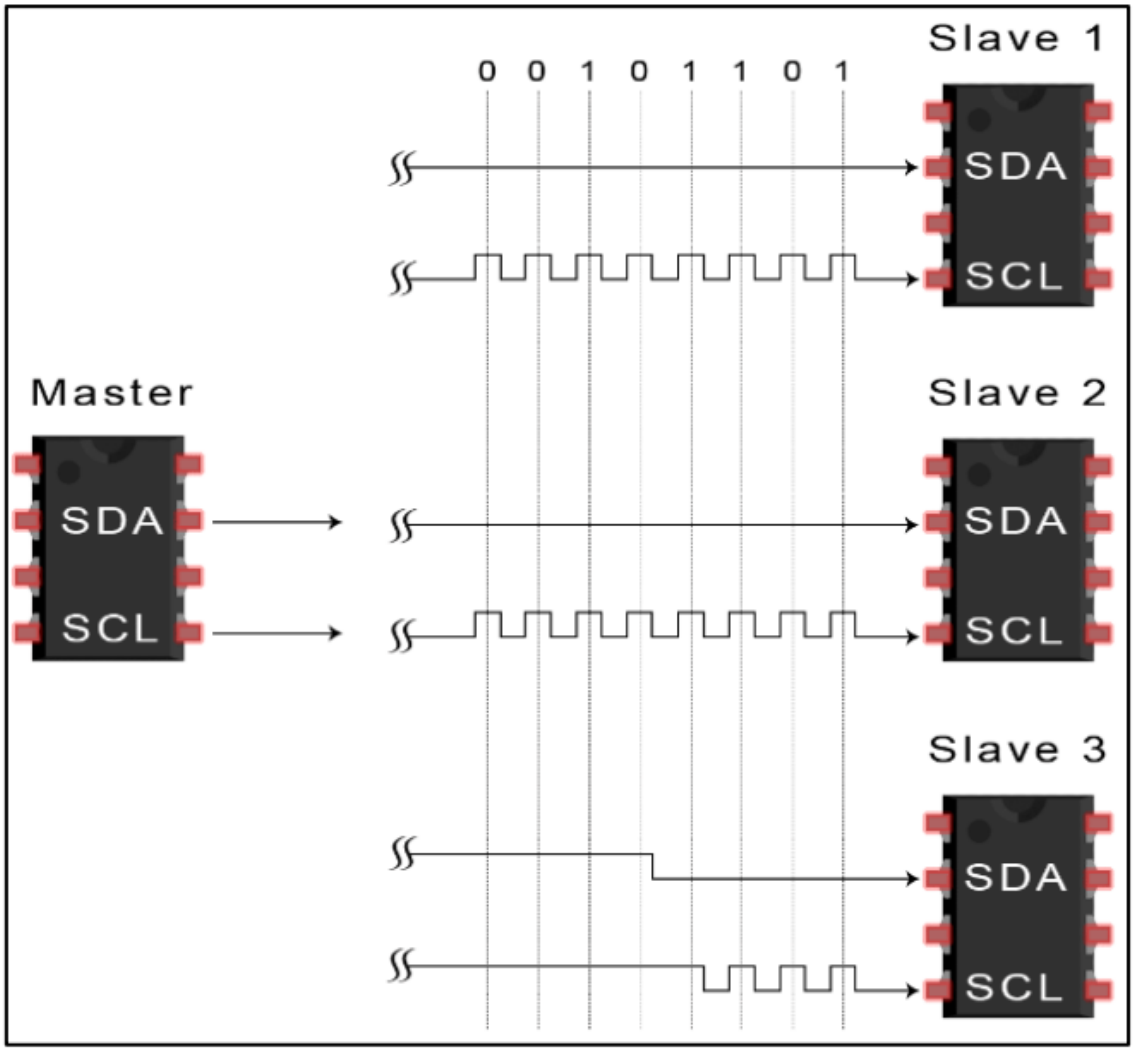
Steps of I2C Data Transmission



Steps of I2C Data Transmission



Steps of I2C Data Transmission



I2C Advantages & Disadvantages

Advantages

- Simple Hardware standard
- Supports multiple masters and multiple slaves
- Only uses two wires
- Acknowledgement bit confirms the data transmission
- Well known and widely used protocol

Disadvantages

- Slower data transfer rate than SPI
- The size of the data frame is limited to 8 bits

Assignment

- Write down different functions in Arduino program along with its use?

Activity

- Use Arduino UNO for blinking LED
- Interface temperature sensor with Arduino UNO

CAN

Controller Area Network

- CAN is a protocol developed to reduce the wiring inside vehicles.
- It was developed by Bosch during 1984.
- There are different standard versions for CAN

  1) Low Speed CAN – 125kbps – 11 bit identifier.

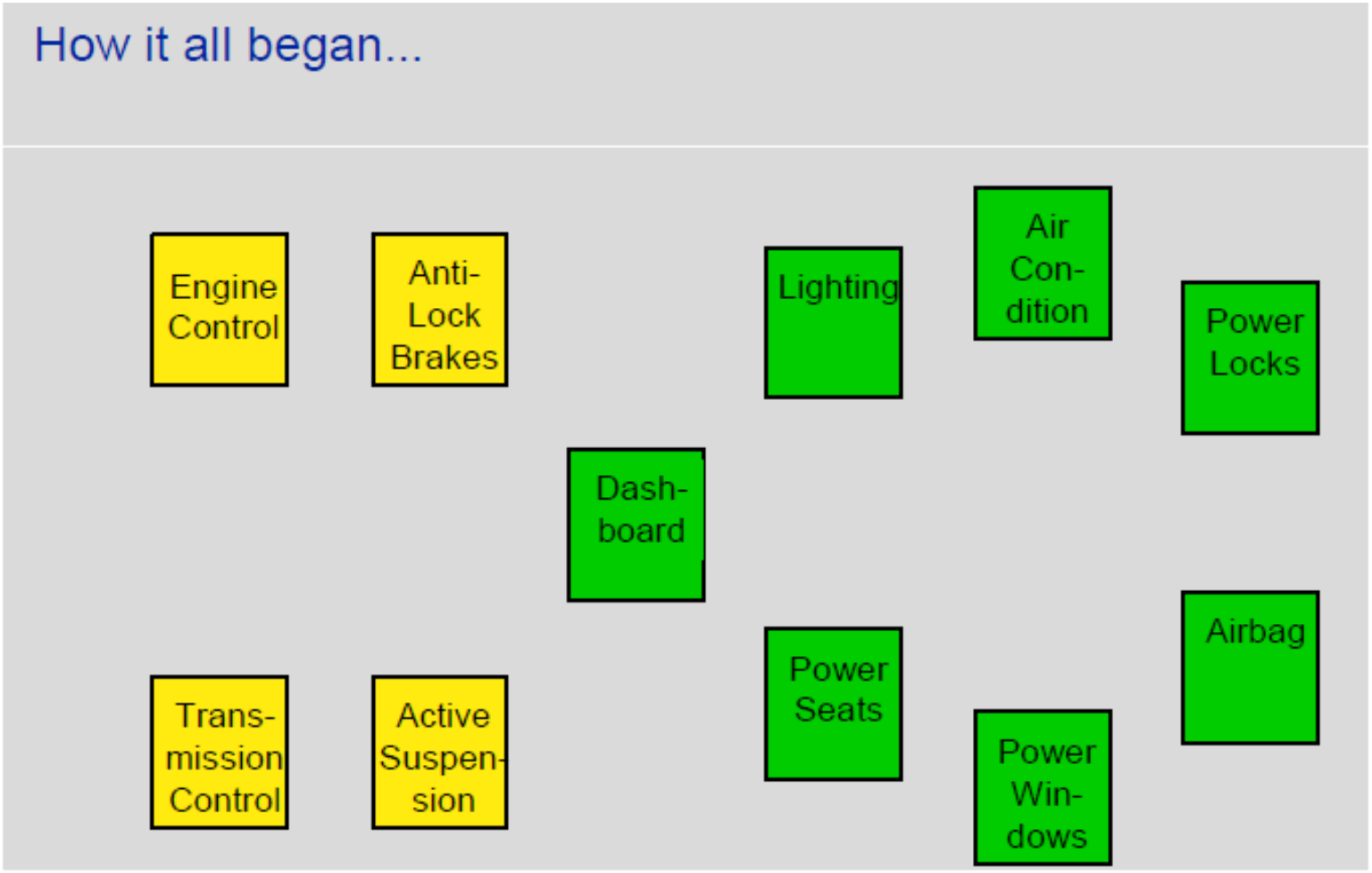
  2) Standard CAN 2.0 A – 1 Mbps – 11 bit identifier

  3) Extended CAN 2.0 B – 1 Mbps – 29 bit identifier.

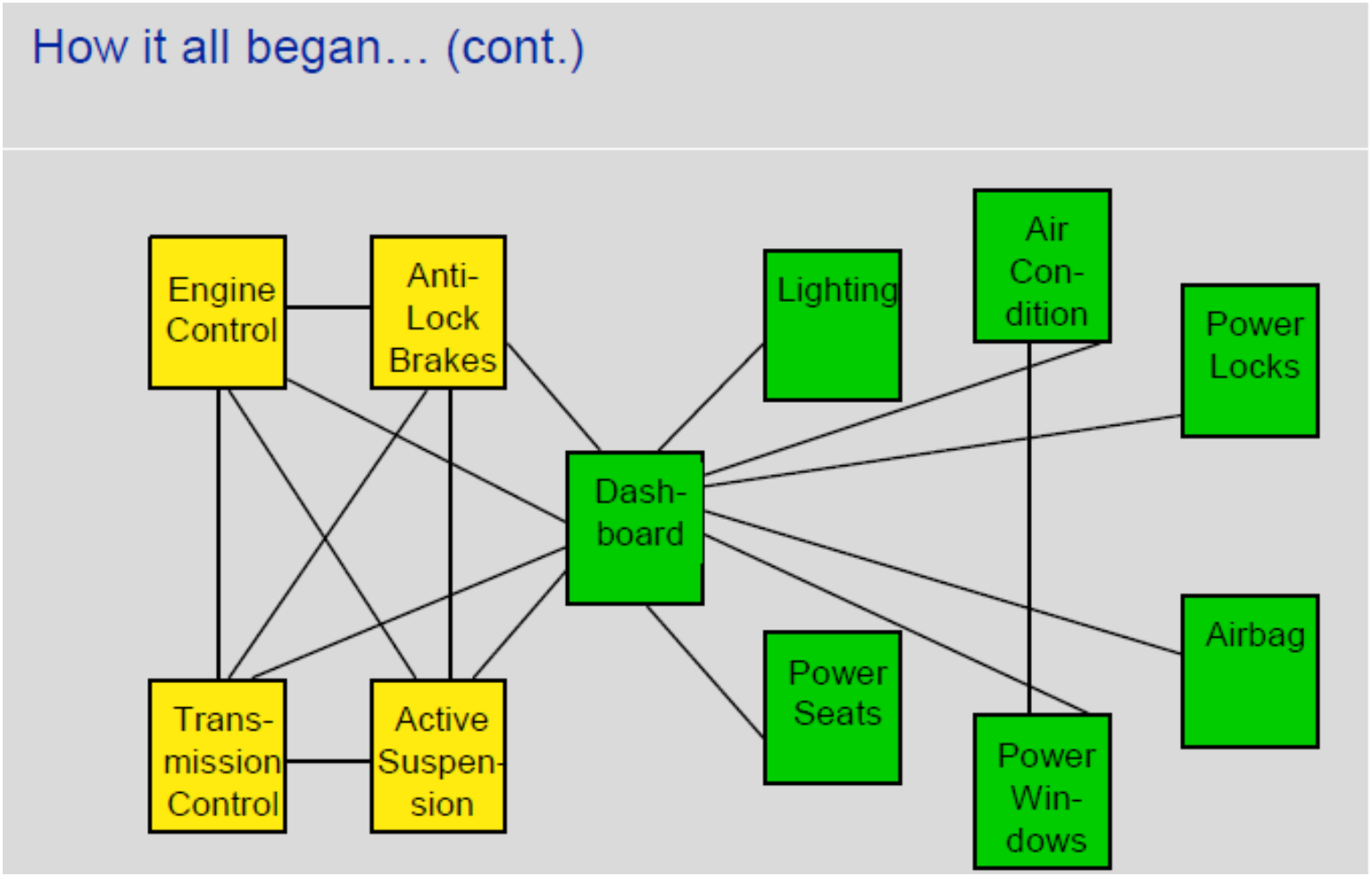
CAN

- CAN uses a differential signal with two logic states, called recessive and dominant.
- Recessive indicates that the differential voltage is less than a minimum threshold voltage.
- Dominant indicates that the differential voltage is greater than this minimum threshold.
- Interestingly, the dominant state is achieved by driving a logic '0' onto the bus, while the recessive state is achieved by a logic '1'.
- This is inverted from the traditional high and low used in most systems.

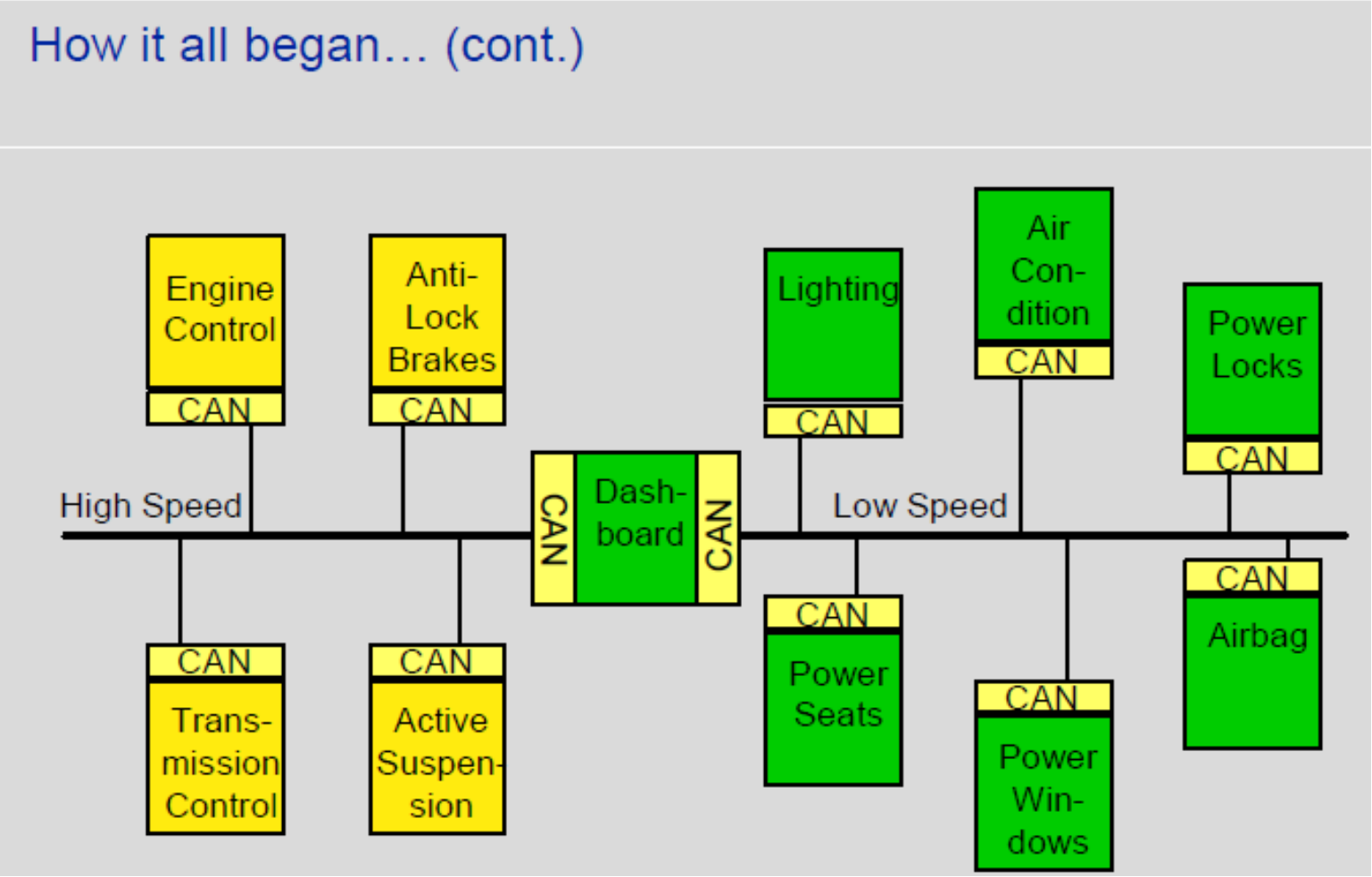
CAN


How it all began...
Engine Control
Anti-Lock Brakes
Lighting
Air Con-dition
Power Locks
Dash-board
Airbag
Power Seats
Trans-mission Control
Active Suspen-sion
Power Win-dows

CAN


How it all began… (cont.)
Engine Control
Anti-Lock Brakes
Lighting
Air Con-dition
Power Locks
Dash-board
Airbag
Power Seats
Power Win-dows
Trans-mission Control
Active Suspen-sion

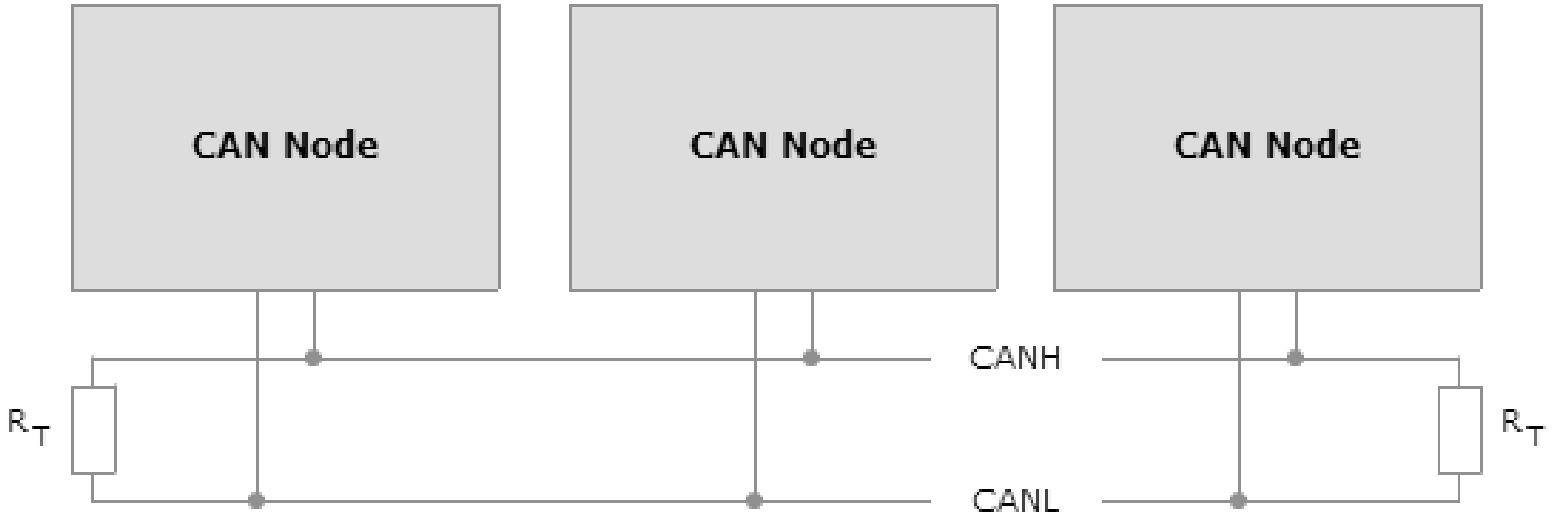
CAN


How it all began… (cont.)
Engine Control
CAN
Anti-Lock Brakes
CAN
Lighting
CAN
Air Con-dition
CAN
Power Locks
CAN
High Speed
CAN
Dash-board
CAN
Low Speed
CAN
Trans-mission Control
CAN
Active Suspen-sion
CAN
Power Seats
CAN
Power Win-dows
CAN
Airbag

CAN in Vehicles

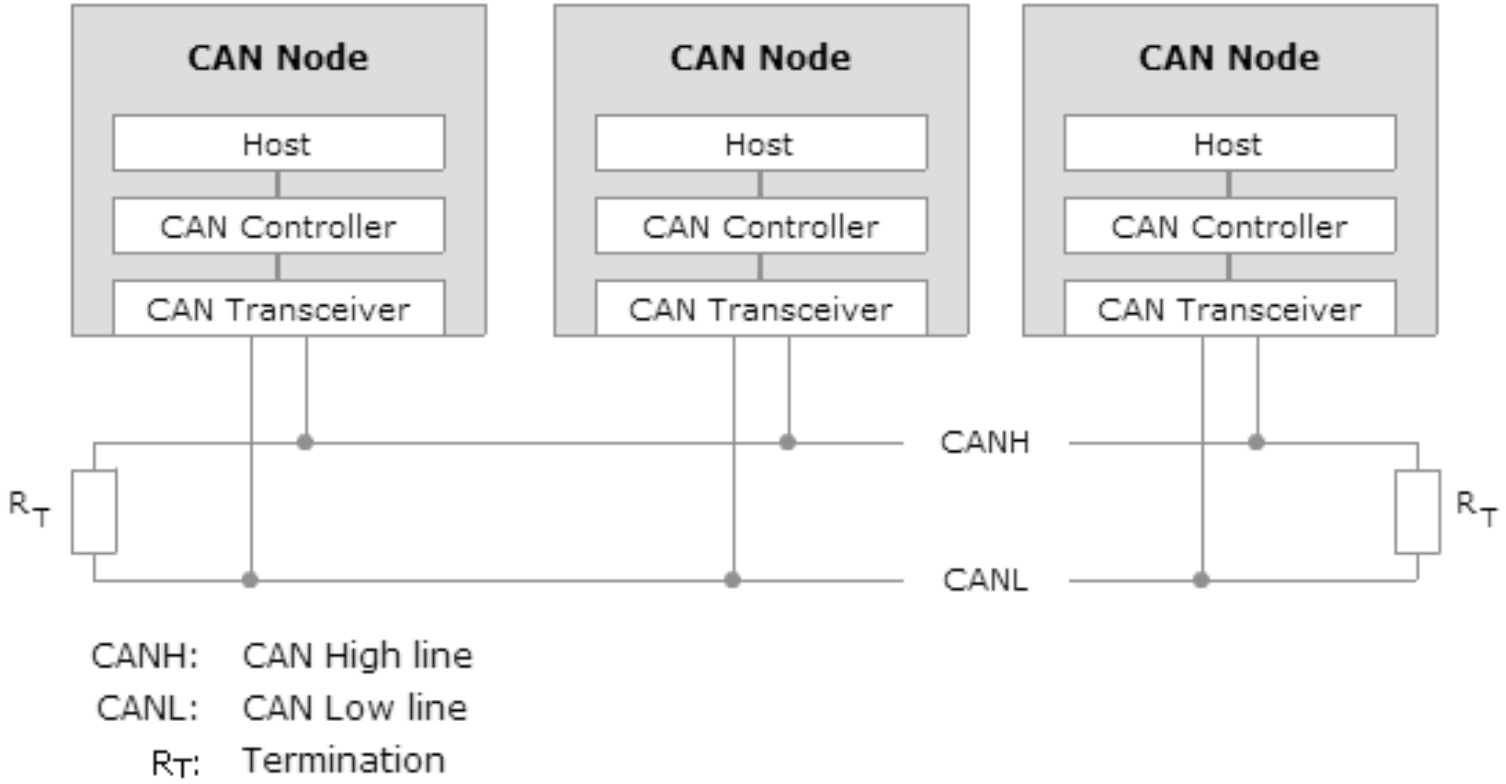
- In one vehicle itself there are different CAN buses of different data rate.
- There can be other kind of buses also in a vehicle.
- To connect between buses of different speed bridges are used.
- CAN bus connects different nodes.
- A CAN node is one which has a MCU, a CAN controller and transceiver connected to a CAN bus.
- To the MCU i/o pins, sensors and actuators are connected.

CAN Network



CANH: CAN High line
CANL: CAN Low line
R_T: Termination

CAN Network


CAN Node
Host
CAN Controller
CAN Transceiver
CAN Node
Host
CAN Controller
CAN Transceiver
CAN Node
Host
CAN Controller
CAN Transceiver
CANH
CANL
R_T
R_T
CANH: CAN High line
CANL: CAN Low line
R_T: Termination

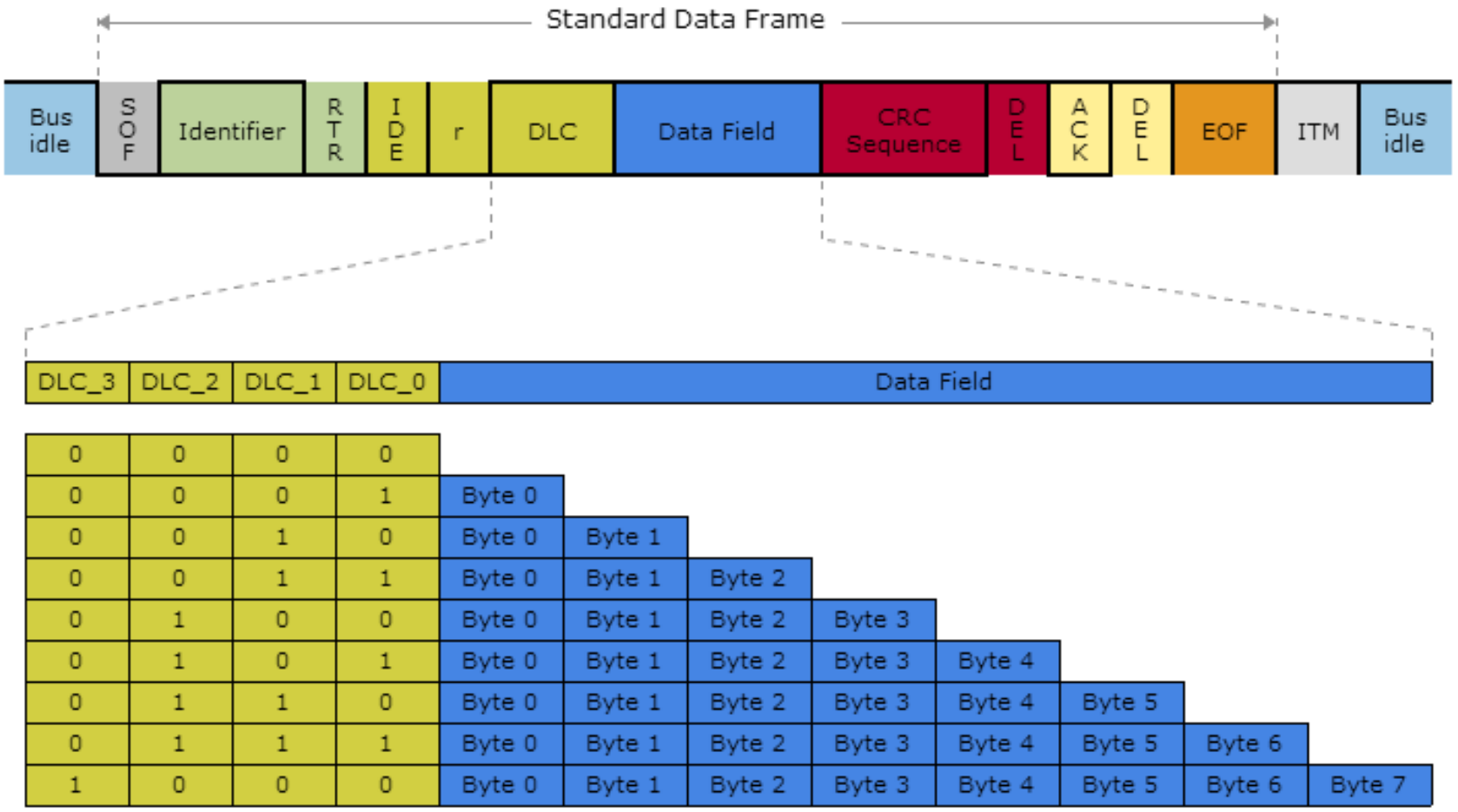
CAN Working

- CAN is a message based protocol.
- One node "broadcasts" the message and every other node uses it. Unlike I2C , none of the nodes have address.
- Which node receives the broadcasted message that depends on the content of the message.
- The message has a field with identifier, which indicates priority. The receiving node do an acceptance test for the identifier of the message to verify if the message is relevant for it.
- If not the message is neglected. This selection procedure is called as **" acceptance filtering"** which is done at each node.

CAN Working

- When many nodes send message simultaneously, it is necessary that only one node is allowed to do a “ valid broadcast”.
- Other transmitters should retreat and try again later. Arbitration is a mechanism that handles bus access conflicts.
- The identifier (11 bit or 29 bit) have a dominant bit (0) and recessive bit (1). The logic is wired AND.

CAN Standard Data Frame



CAN Standard Data Frame

- The first bit is the start of frame (SOF). This dominant bit represents the start of a CAN message.
- Next is the 11-bit identifier, which establishes the priority of the CAN message. The smaller the identifier, the higher the priority of the message.
- The remote transmission request (RTR) bit is normally dominant, but it goes recessive when one node is requesting data from another.
- The identifier extension (IDE) bit is dominant when a standard CAN frame is being sent and not an extended one.
- The r bit is reserved and not currently used.
- The data length code (DLC) nibble signifies how many bytes of data are in this message.

CAN Standard Data Frame

- Next is the data itself, being as many bytes as represented in the DLC bits.
- The cyclic redundancy check (CRC) is a 16-bit checksum for detecting errors in the transmitted data.
- If the message is properly received, the receiving node overwrites the recessive acknowledge bit (ACK) with a dominant bit. The ACK also contains a delimiter bit to keep things synchronized.
- The end of frame (EOF) signifies the end of the CAN message and is 7 bits wide, for detecting bit-stuffing errors.
- The last part of a CAN message is used as a time delay. This time delay is precisely the amount of time needed for a CAN controller to move the received message into a buffer for further processing.

Advantages & Disadvantages

Advantages

- It support multi master and multicast features.
- The CAN bus has maximum length of 40 meters.
- The CAN provides the ability to work in different electrical environment.
- The CAN reduces wiring since it is a distributed control and this ensures enhancing of the system performance.
- It has single serial bidirectional line to achieve half duplex communication.
- It has standard bus in distributed network.

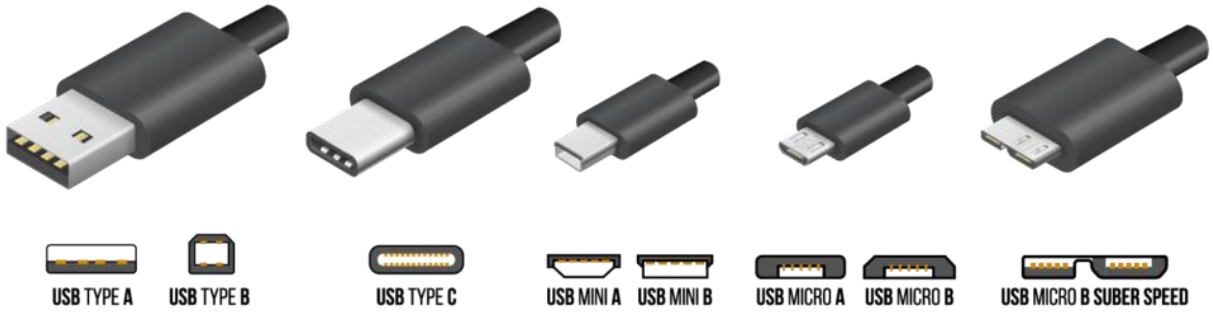
Disadvantages

- It has high software expenditure.
- Undesirable interaction more probable.

USB

Universal Serial Bus (USB)

- Universal Serial Bus (USB) is a set of interface specifications for high speed wired communication between electronics systems peripherals and devices with or without PC/computer.
- The USB was originally developed in 1995 by many of the industry leading companies like Intel, Compaq, Microsoft, Digital and IBM
- USB allows hot swapping which allows devices can be plugged and unplugged without rebooting the computer or turning off the device.
- USB sends data in serial mode i.e. the parallel data is serialized before sends and deserialized after receiving.



Versions of USB

USB1.0

- USB 1.0 is the original release of USB having the capability of transferring 12Mbps, supporting up to 127 devices.
- This USB 1.0 specification model was introduced in January 1996.

USB1.1

- USB 1.1 came out in September 1998. USB 1.1 is also known as full-speed USB.
- This version is similar to the original release of USB; however, there are minor modifications for the hardware and the specifications.
- USB version 1.1 supported two speeds, a full speed mode of 12Mbits/s and a low speed mode of 1.5Mbits/s.

Versions of USB

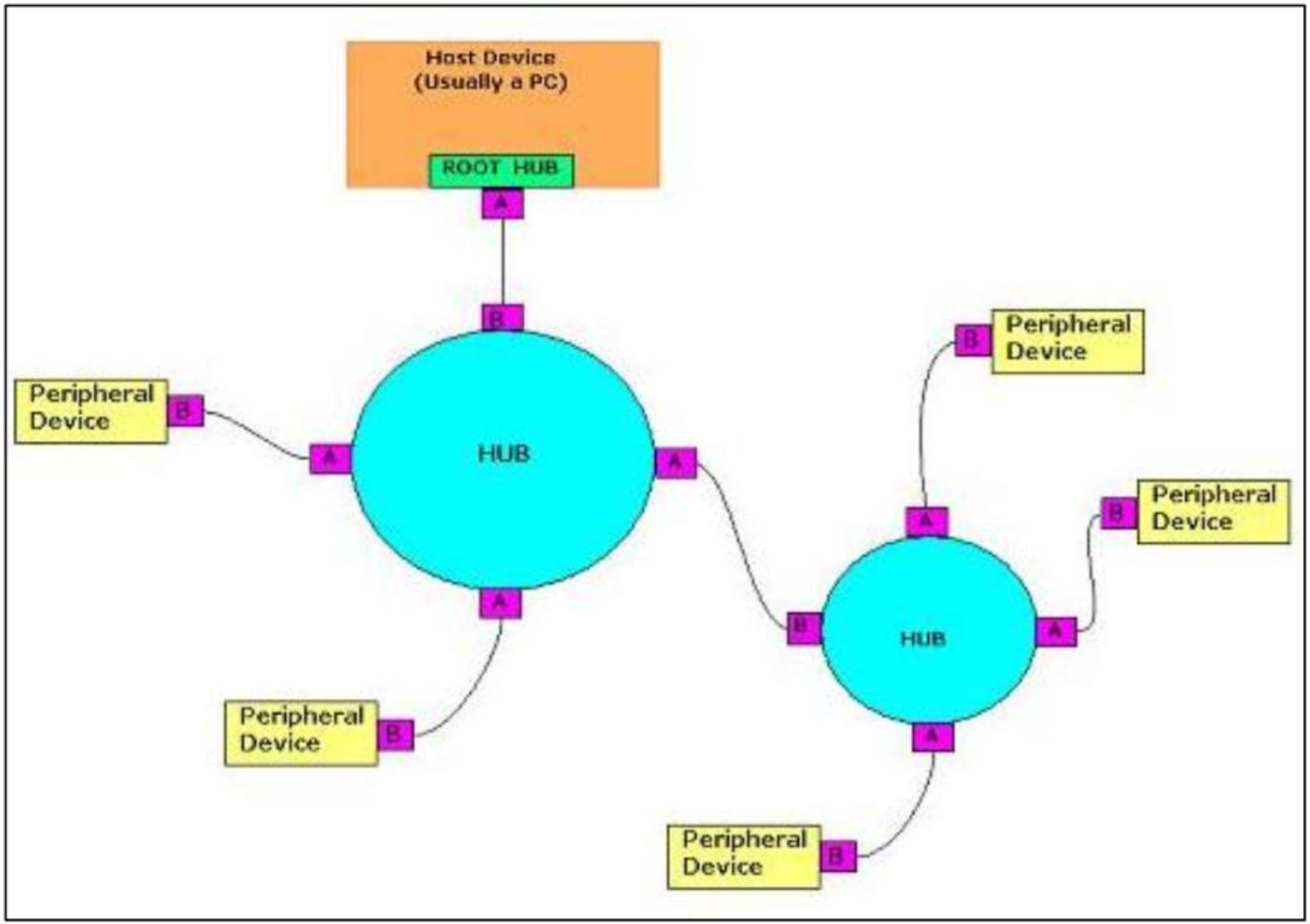
USB2.0

- Hewlett-Packard, Intel, LSI Corporation, Microsoft, NEC, and Philips jointly developed a higher data transfer rate than the 1.1 version.
- Supporting three speed modes (1.5, 12 and 480 Mbps), USB 2.0 supports low-bandwidth devices such as keyboards and mice, as well as high-bandwidth ones like high-resolution Webcams, scanners, printers and high-capacity storage systems.
- USB 2.0, also known as hi-speed USB. This hi-speed USB is capable of supporting a transfer rate of up to 480 Mbps, compared to 12 Mbps of USB 1.1.

USB3.0

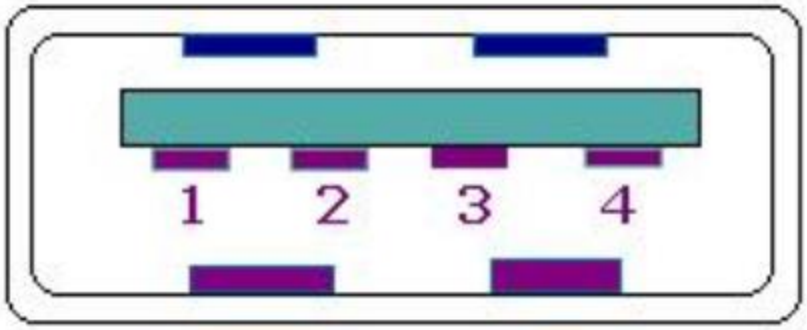
- It is also called as Super-Speed USB having a data transfer rate of 4.8Gbps
- It can deliver over 10x the speed of today's Hi-Speed USB connections.

USB tiered star topology

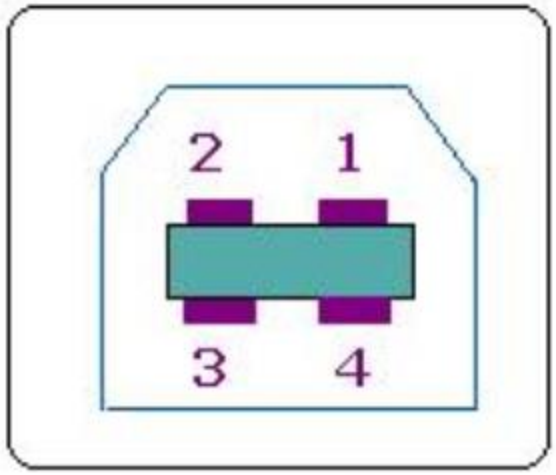


USB Connectors

- The USB standard uses "A" and "B" connectors mainly to avoid confusion:
- "A" connectors head "upstream" toward the computer.
- "B" connectors head "downstream" and connect to individual devices.



Type A socket



Type B socket

Data Transfer

- USB can support 4 data transfer types or transfer modes.
  - Control
  - Isochronous
  - Bulk
  - Interrupt
- **Control transfers** exchange configuration, setup and command information between the device and host. The host can also send commands or query parameters with control packets.
- **Isochronous transfer** is used by time critical, streaming device such as speakers and video cameras. It is time sensitive information so, within limitations, it has guaranteed access to the USB bus.
- **Bulk transfer** is used by devices like printers & scanners, which receives data in one big packet.
- **Interrupt transfer** is used by peripherals exchanging small amounts of data that need immediate attention.

Data Transfer

- All USB data is sent serially.
- USB data transfer is essentially in the form of packets of data, sent back and forth between the host and peripheral devices.
- Initially all packets are sent from the host, via the root hub and possibly more hubs, to devices.

Each USB data transfer consists of a…

1. **Token packet** (Header defining what it expects to follow)
2. **Data Packet** (Containing the payload)
3. **Status Packet** (Used to acknowledge transactions and to provide a means of error correction)

Advantages

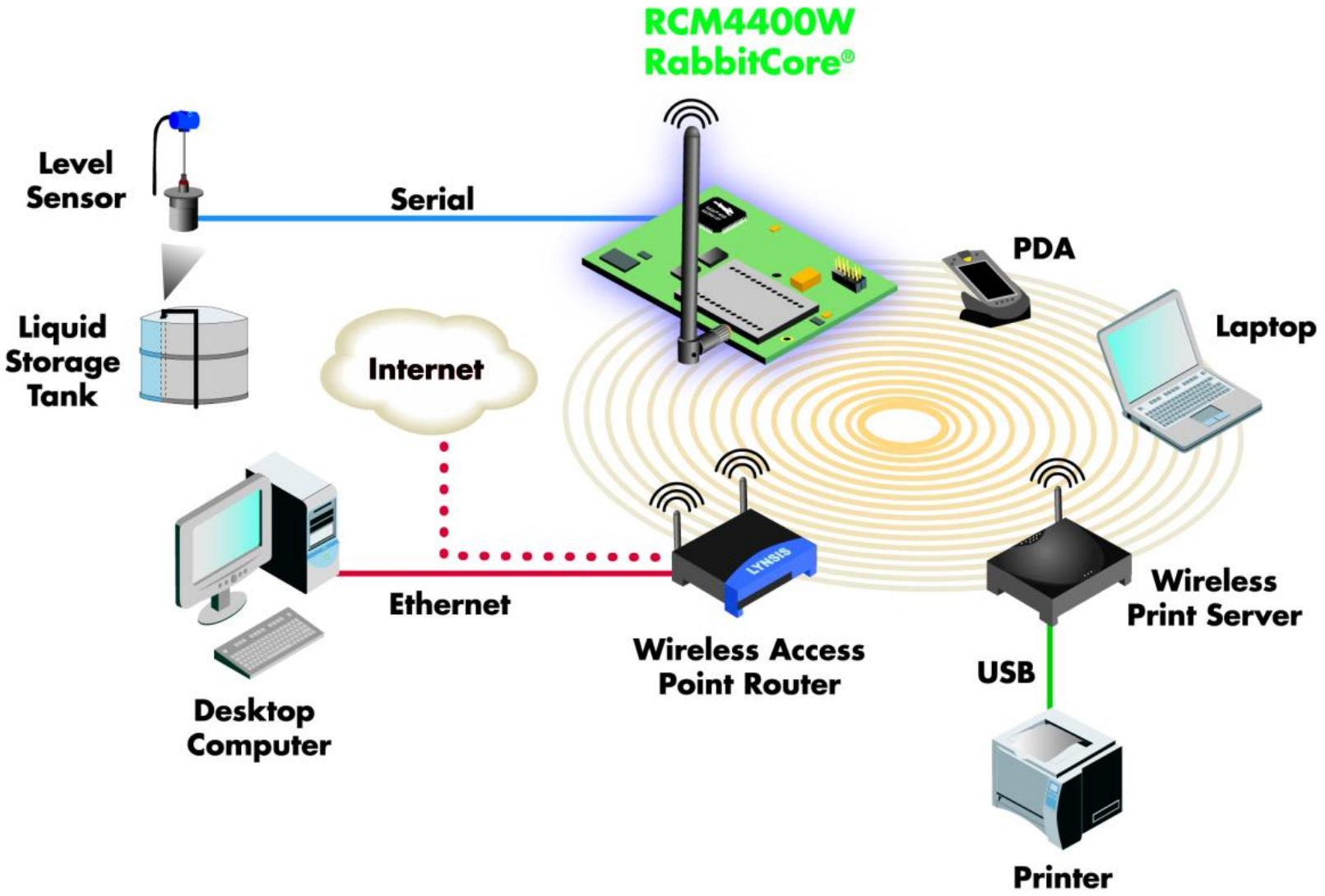
- Low cost
- Expandability
- Auto-configuration
- Hot-plugging
- Outstanding performance
- It also provides power to the bus, enabling many peripherals to operate without the added need for an AC power adapter.

Wi-Fi

Wi-Fi

- Wi-Fi is a wireless local area network (WLAN) technology that allows electronic devices to network using the 2.4 GHz or 5 GHz ISM radio bands.
- It is based on the IEEE 802.11 MAC and physical layer standards for WLAN and is the most pervasive choice for connectivity with the Internet, especially in the home LAN environment.
- Wi-Fi supports very fast data transfer rates, but consumes a lot of power which makes it unviable for low-power applications.
- The embedded networks, wireless sensor network applications and Internet-of-Things implementations explicitly make use of Wi-Fi as a preferred choice for connectivity to the Internet

Wi-Fi


RCM4400W
RabbitCore®
Level Sensor
Serial
Liquid Storage Tank
Internet
PDA
Laptop
Ethernet
Wireless Access Point Router
Wireless Print Server
USB
Desktop Computer
Printer

Benefits of Wi-Fi

- **Wireless Ethernet**. Wi-Fi is an Ethernet replacement. Wi-Fi and Ethernet, both IEEE 802 networks, share some core elements.
- **Extended Access**. The absence of wires and cables extends access to places where wires and cables cannot go or where it is too expensive for them to go.
- **Cost Reduction**. The absence of wires and cables brings down cost. This is accomplished by a combination of factors, the relatively low cost of wireless routers, no need for trenching, drilling and other methods that may be necessary to make physical connections.
- **Mobility**. Wires tie you down to one location. Going wireless means you have the freedom to change your location without losing your connection.
- **Flexibility**. Extended access, cost reductions, and mobility create opportunities for new applications as well as the possibility of creative new solutions for legacy applications.

Wi-Fi Embedded Applications

- Industrial process and control applications where wired connections are too costly or inconvenient, e.g., continuously moving machinery.
- Emergency applications that require immediate and transitory setup, such as battlefield or disaster situations.
- Mobile applications, such as asset tracking.
- Surveillance cameras (maybe you don't want them easily noticed, cables are difficult to hide).
- Vertical markets like medical, education, and manufacturing.
- Communication with other Wi-Fi devices, like a laptop or a PDA.

Elements of WIFI network

- **Access Point (AP)** - The AP is a wireless LAN transceiver or “base station” that can connect one or many wireless devices simultaneously to the Internet.
- **Wi-Fi cards** - They accept the wireless signal and relay information. They can be internal and external.
- **Safeguards** - Firewalls and anti-virus software protect networks from uninvited users and keep information secure.

WIFI Topologies

Peer-to-peer Topology

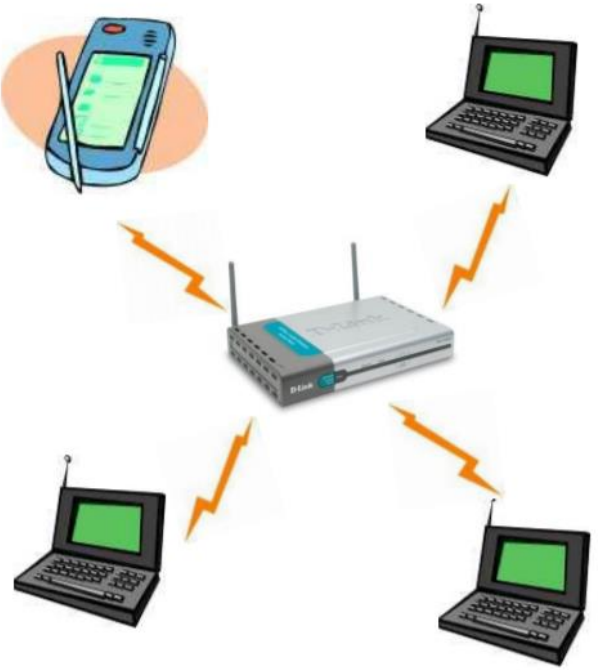
- AP is not required.
- Client devices within a cell can communicate with each other directly.
- It is useful for setting up a wireless network quickly and easily

Infrastructure network

- The client communicate through Access Point.
- Any communication has to go through AP.
- If a Mobile Station (MS), like a computer, a PDA, or a phone, wants to communicate with another MS, it needs to send the information to AP first, then AP sends it to the destination MS.

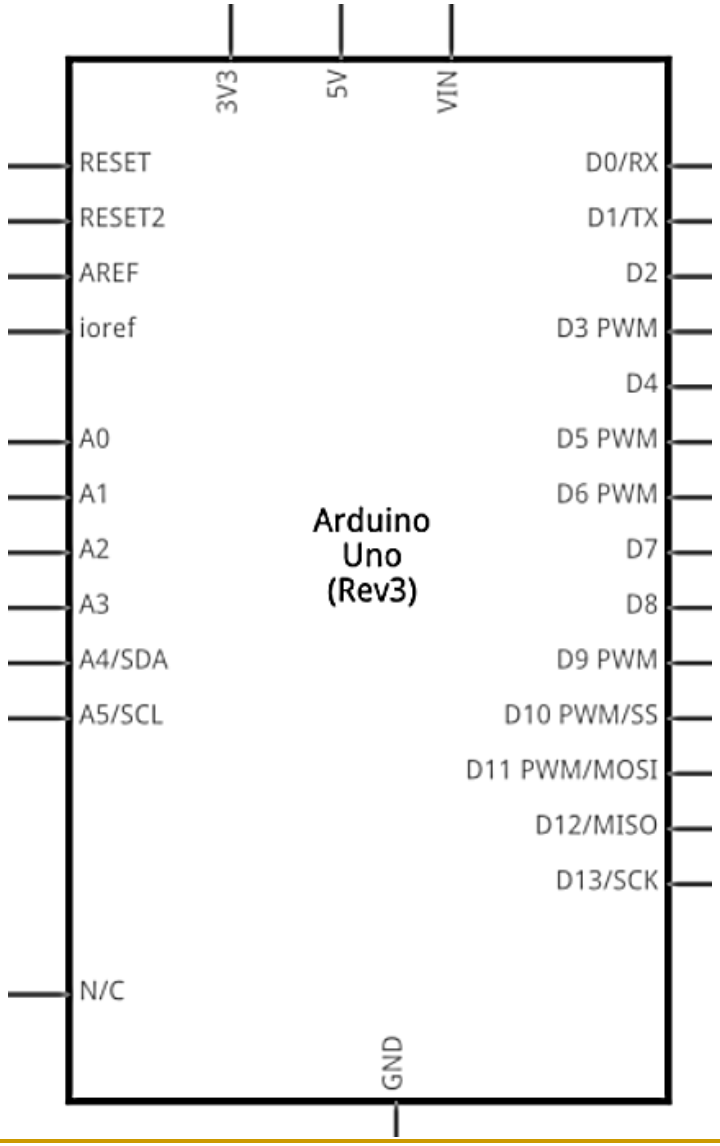
WIFI Topologies

Peer-to-peer Topology



Infrastructure network Topology

Arduino Schematics



Bluetooth

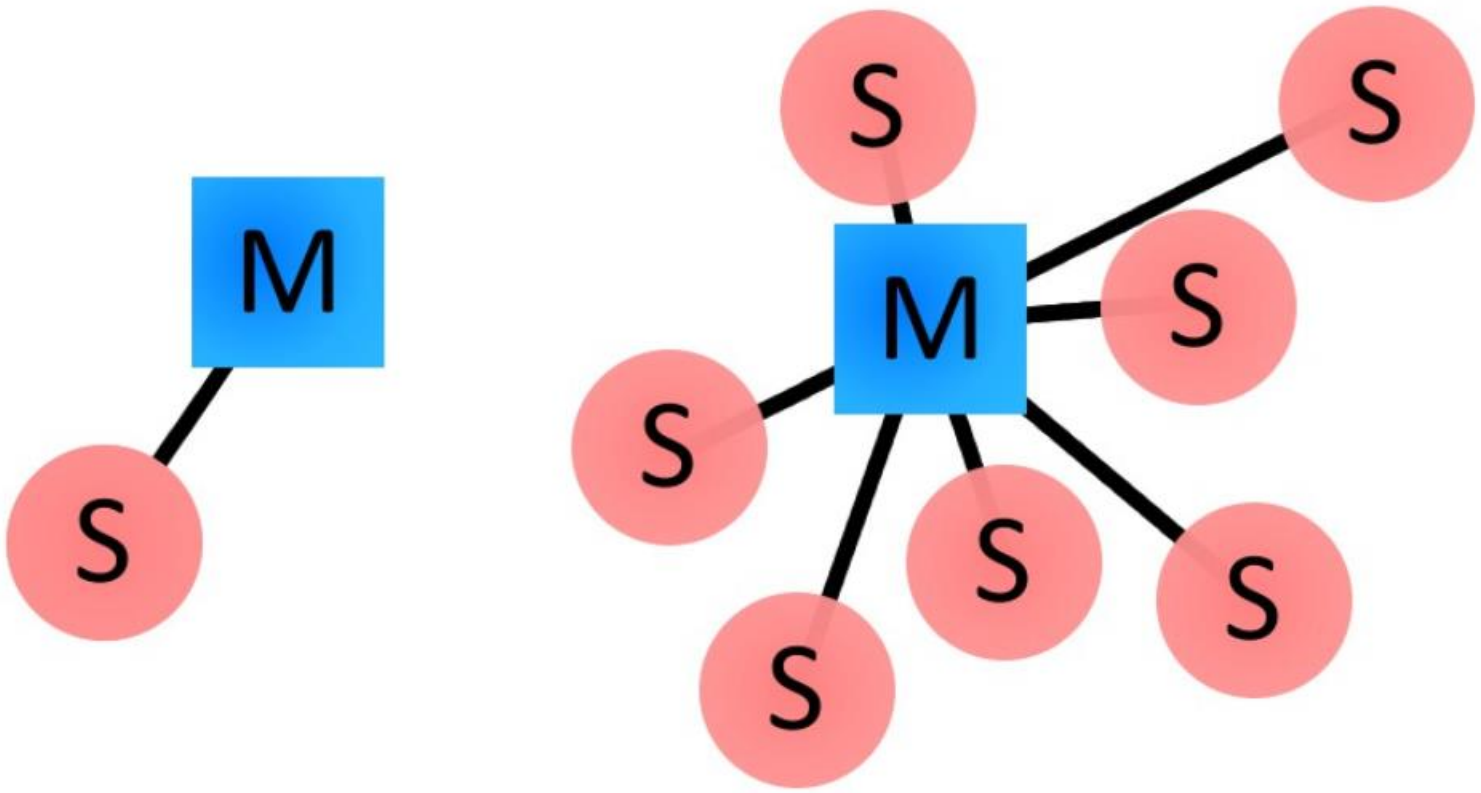
Bluetooth

- Bluetooth is a standardized protocol for sending and receiving data via a 2.4GHz wireless link.
- It's a secure protocol, and it's perfect for short-range, lowpower, low-cost, wireless transmissions between electronic devices.
- Bluetooth serves as an excellent protocol for wirelessly transmitting relatively small amounts of data over a short range (<100 m)
- The Bluetooth protocol operates at 2.4GHz in the same unlicensed ISM frequency band where RF protocols like ZigBee and WiFi also exist.

Bluetooth Working

- Bluetooth networks (commonly referred to as piconets) use a master/slave model to control when and where devices can send data.
- A single master device can be connected to up to seven different slave devices.
- Any slave device in the piconet can only be connected to a single master.
- The master coordinates communication throughout the piconet.
- It can send data to any of its slaves and request data from them as well.
- Slaves are only allowed to transmit to and receive from their master. They can’t talk to other slaves in the piconet.

Bluetooth Piconets



Bluetooth Connection Process

- **Inquiry** – If two Bluetooth devices know absolutely nothing about each other, one must run an inquiry to try to discover the other. One device sends out the inquiry request, and any device listening for such a request will respond with its address, and possibly its name and other information.
- **Paging (Connecting)** – Paging is the process of forming a connection between two Bluetooth devices. Before this connection can be initiated, each device needs to know the address of the other (found in the inquiry process).
- **Connection** – After a device has completed the paging process, it enters the connection state. While connected, a device can either be actively participating or it can be put into a low power sleep mode.

Bluetooth Modes

- **Active Mode** – This is the regular connected mode, where the device is actively transmitting or receiving data.
- **Sniff Mode** – This is a power-saving mode, where the device is less active. It'll sleep and only listen for transmissions at a set interval (e.g. every 100ms).
- **Hold Mode** – Hold mode is a temporary, power-saving mode where a device sleeps for a defined period and then returns back to active mode when that interval has passed. The master can command a slave device to hold.
- **Park Mode** – Park is the deepest of sleep modes. A master can command a slave to "park", and that slave will become inactive until the master tells it to wake back up.

Bonding and Pairing

- When two Bluetooth devices share a special affinity for each other, they can be bonded together.
- Bonded devices automatically establish a connection whenever they're close enough.
- Bonds are created through one-time a process called pairing. When devices pair up, they share their addresses, names, and profiles, and usually store them in memory.
- The also share a common secret key, which allows them to bond whenever they're together in the future.
- Pairing usually requires an authentication process where a user must validate the connection between devices.

Comparison

Name	Bluetooth Classic	Bluetooth 4.0 Low Energy	ZigBee	WiFi
IEEE Standard	802.15.1	802.15.1	802.15.4	802.11 (a, b, g, n)
Frequency (GHz)	2.4	2.4	0.868, 0.915, 2.4	2.4 and 5
Maximum raw bit rate (Mbps)	01/03/17	1	0.25	11 (b), 54 (g), 600 (n)
Typical data throughput (Mbps)	0.7-2.1	0.27	0.2	7 (b), 25 (g), 150 (n)
Maximum (Outdoor) Range (m)	10 (class 2), 100 (class 1)	50	10/01/00	100-250
Relative Power Consumption	Medium	Very low	Very low	High
Example Battery Life	Days	Months to years	Months to years	Hours
Network Size	7	Undefined	64000	255

Advantages

- It avoids interference from other wireless devices.
- It has lower power consumption.
- It is easily upgradeable.
- It has range better than Infrared communication.
- The Bluetooth is used for voice and data transfer.
- Bluetooth devices are available at very cheap cost.
- No line of sight hence can connect through any obstacles.
- Free to use if the device is installed with Bluetooth.
- The technology is adopted in many products such as head set, in car system, printer, web cam, GPS system, keyboard and mouse.

Disadvantages

- It can lose connection in certain conditions.
- It has low bandwidth as compared to Wi-Fi.
- It allows only short range communication between devices.
- Security is a very key aspect as it can be hacked.

NFC

NFC

- Based on the 13.56 MHz wireless communication protocol, Near Field Communication (NFC) uses contactless connectivity to build key enablers that greatly facilitate the adoption of new innovative applications.
- Currently found in contactless payment, e-government (passports), access control, public transport ticketing systems and e-government (passports).
- NFC is a convenient, always-on radio link that is driving the growth for simple pairing, diagnostic readout, parameter programming and much more.
- NFC's unique features will have a positive impact on many of our activities in areas such as smart living, industrial, and mobile devices.

NFC Features

- Fast and intuitive, no training required
- Already widely used in mobile, cards and tags
- Short operating distance guarantees privacy and security
- Perfect for secure transactions, such as payments or access control
- Greatly facilitates Bluetooth pairing and Wi-Fi hotspot registration

What is so special about NFC?

- Triggered by a simple tap; NFC transactions are short, lasting just a fraction of a second, with no need for any preliminary steps. The result is a very intuitive gesture.
- In NFC, only one device needs to be powered (except for Peer-to-peer mod). The possibility to have inexpensive, completely passive tags is a true enabler for IoE (Internet of Everything) scenarios.
- NFC is a proximity technology based on an intentional action that makes obvious the NFC device is present and identifiable by its owner.
- The NFC software stack is fully integrated into Android, iOS and Windows, mobile operating systems that natively provide a number of services, creating the opportunity for many applications to use NFC without the need to install any specific software

NFC Applications

Tag Reader/Writer

Connect the world of apps with the physical world

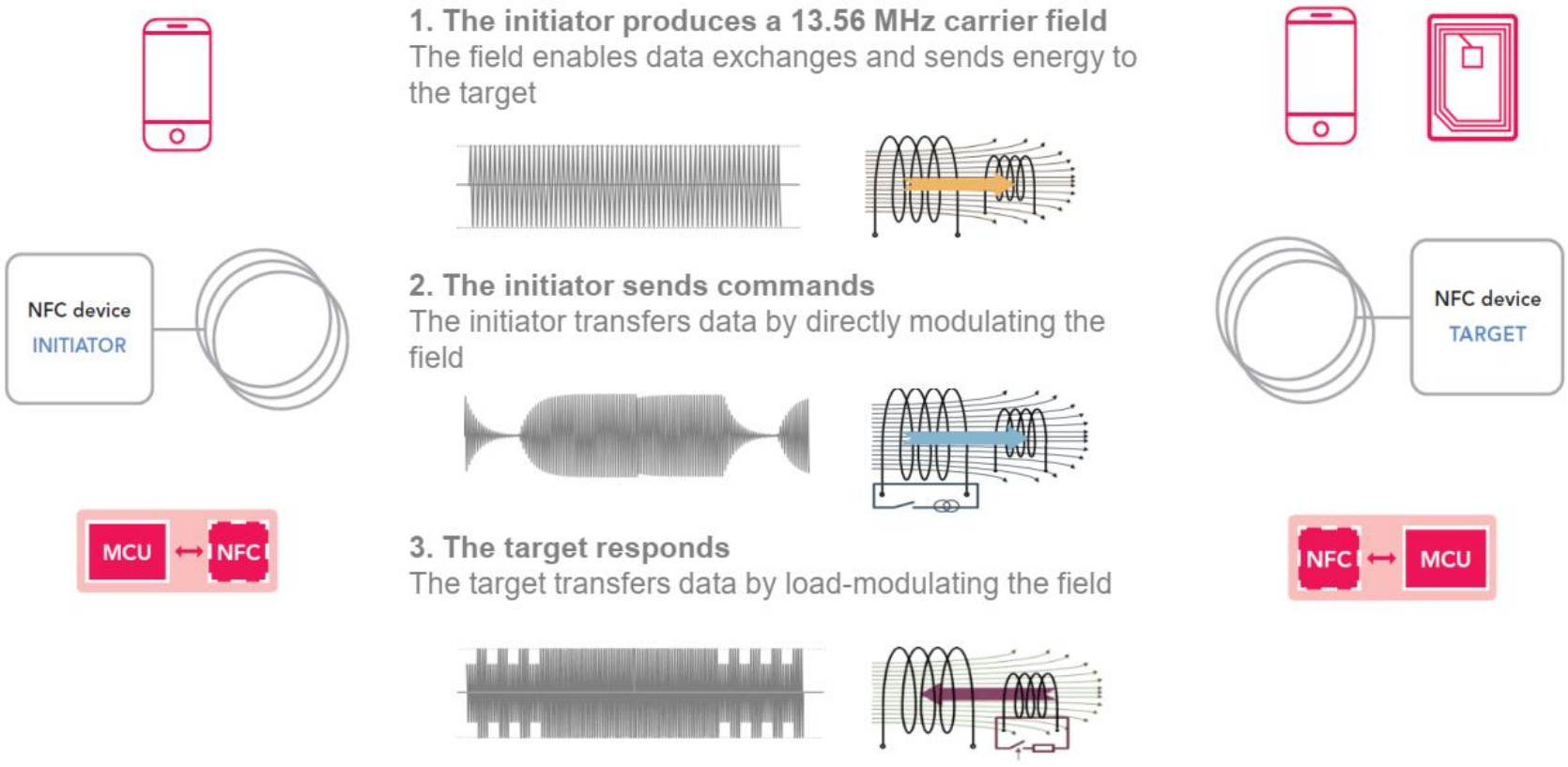
Card Emulation

Use your device as a Card

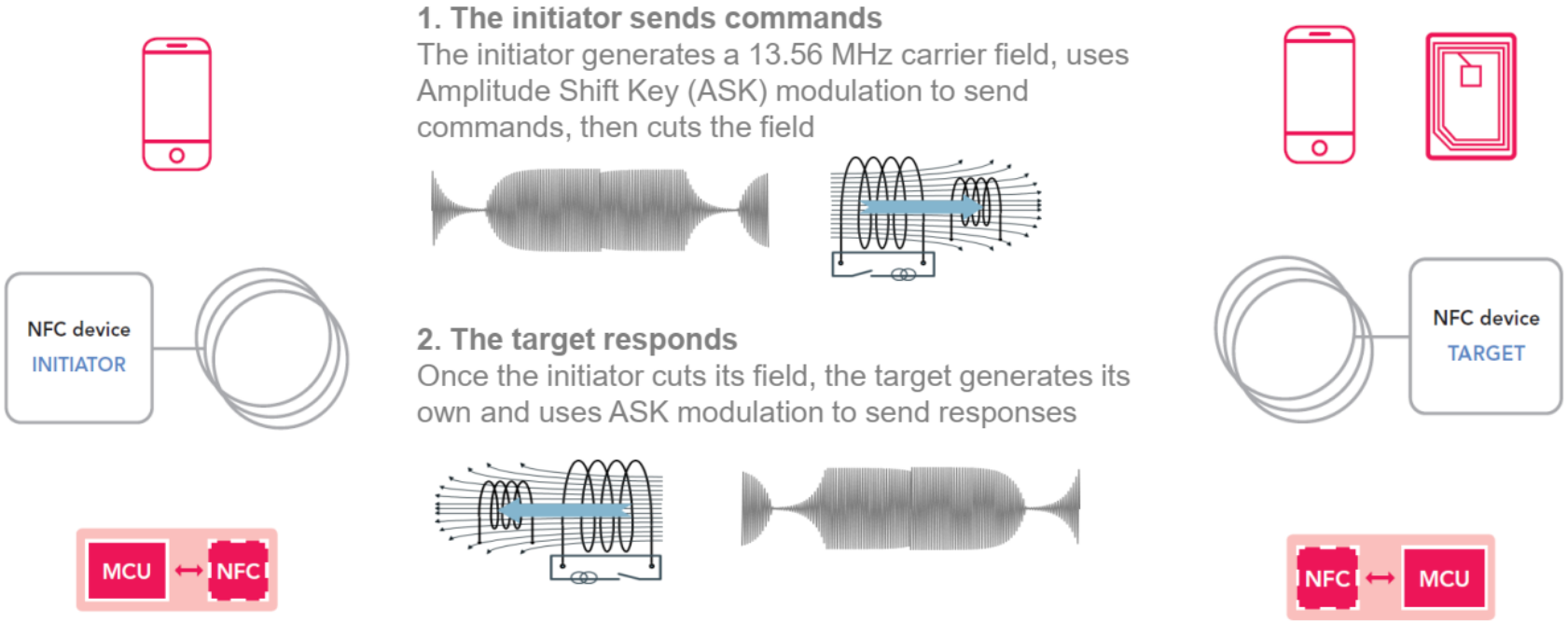
Peer to Peer

Connect devices through physical proximity

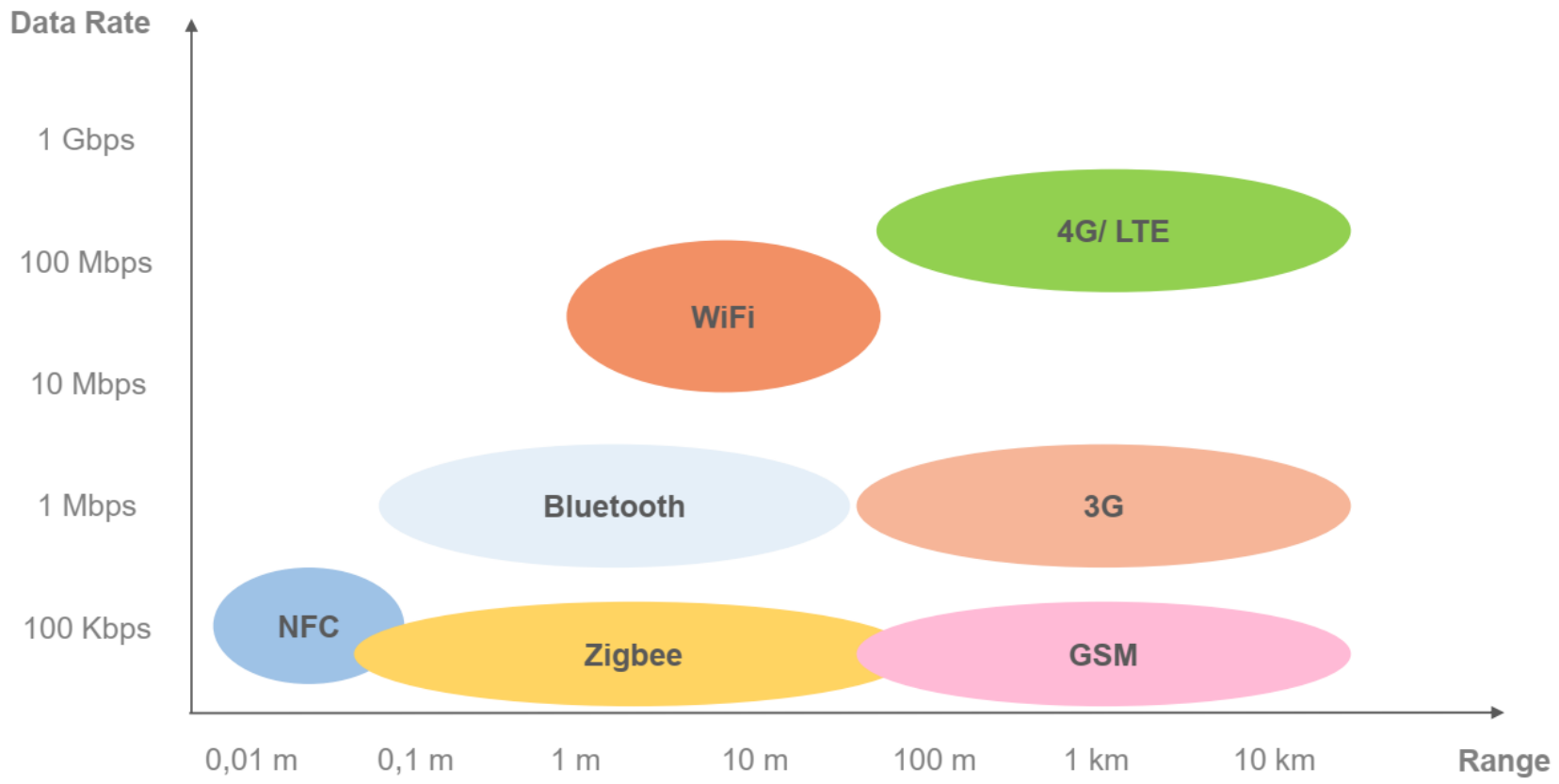
NFC Passive Communication



NFC Active Communication



Range Vs Data rate



Advantages

- **Convenient:** The convenience of payment is one of this system's greatest advantages.
- **Versatile:** NFC is very versatile, in that it covers a range of different industries and services.
- **Better User Experience:** This system is beneficial for enterprises too companies that readily adopt the latest technology are viewed by customers as being dynamic and progressive.
- **Seamless:** The high level of encryption enables institutions to employ it as a sort of a security system, which does an accurate ID on students entering and exiting the premises.

Zigbee

Zigbee

- ZigBee is the most popular industry wireless mesh networking standard for connecting sensors, instrumentation and control systems.
- ZigBee, a specification for communication in a wireless personal area network (WPAN), has been called the "Internet of things."
- ZigBee is an open, global, packet-based protocol designed to provide an easy-to-use architecture for secure, reliable, low power wireless networks.
- ZigBee and IEEE 802.15.4 are low data rate wireless networking standards that can eliminate the costly and damage prone wiring in industrial control applications.
- Flow or process control equipment can be place anywhere and still communicate with the rest of the system.
- It can also be moved, since the network doesn't care about the physical location of a sensor, pump or valve

How Zigbee Works?

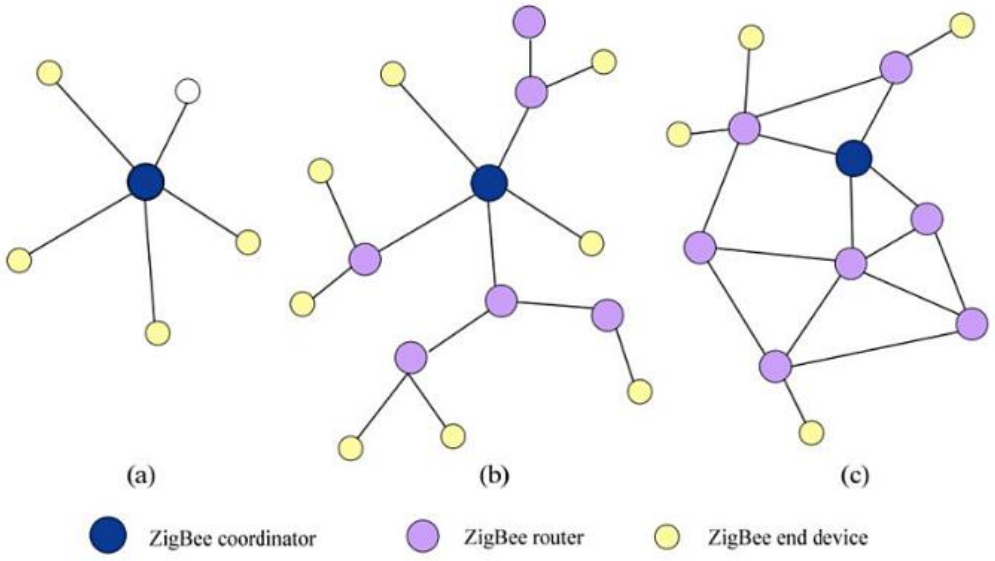
- ZigBee basically uses digital radios to allow devices to communicate with one another.
- Every ZigBee network must contain a network coordinator. Other Full Function Devices (FFD's) may be found in the network, and these devices support all of the 802.15.4 functions.
- They can serve as network coordinators, network routers, or as devices that interact with the physical world.
- Several topologies are supported by ZigBee, including star, mesh, and cluster tree. Star topology is most useful when several end devices are located close together and they can communicate with a single router node.
- Mesh networking allows for redundancy in node links, so that if one node goes down, devices can find an alternative path to communicate with one another.

Zigbee Features

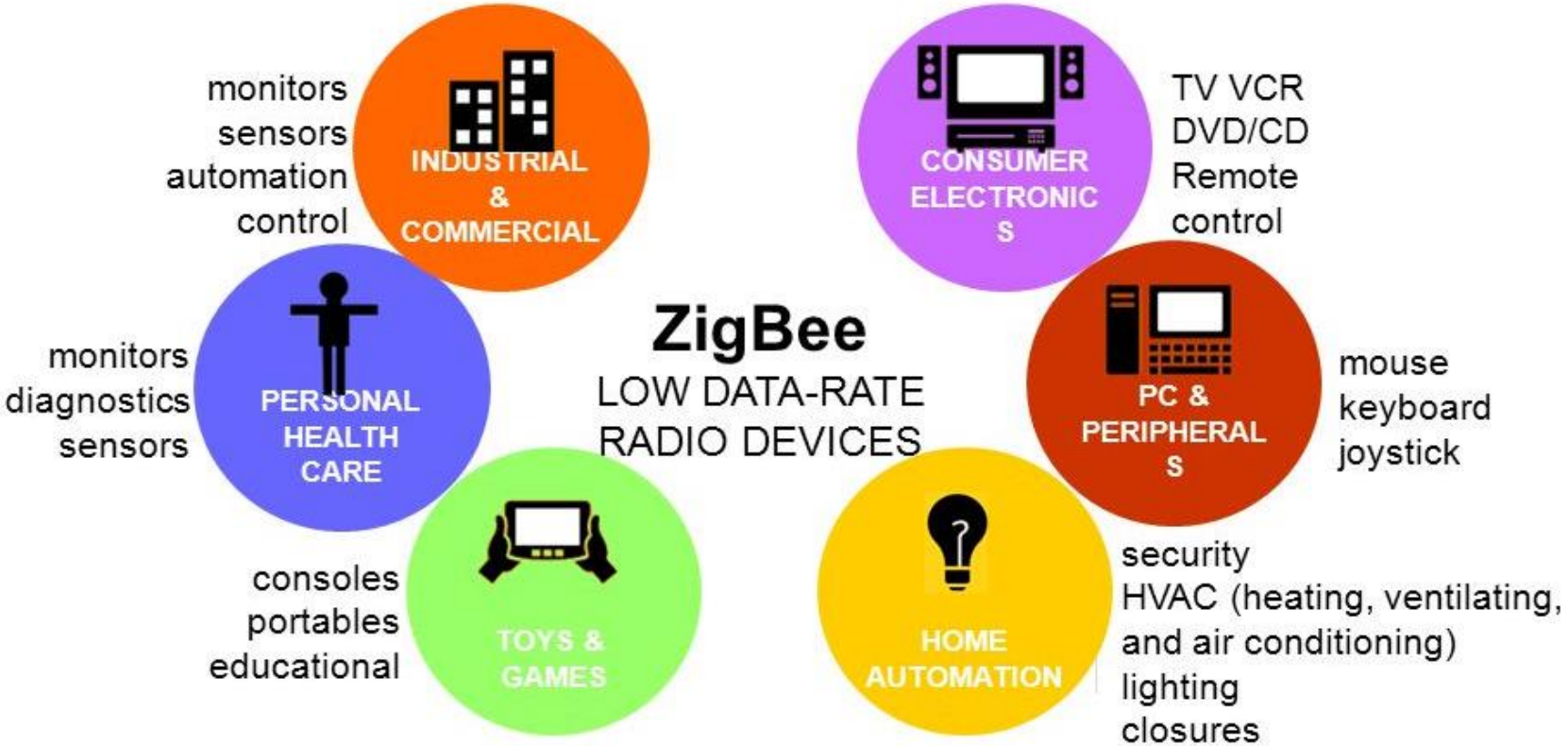
- There are three different states defined for the devices: Transmitting, receiving and sleeping. This allows to the device to save energy when duty cycles are defined and the device sleeps.
- Mainly used for Wireless Sensor Networks
- Users expect batteries to last many months to years
- Even mains powered equipment needs to be conscious of energy.
- ZigBee devices will be more ecological than its predecessors saving megawatts at it full deployment.
- ZigBee provides ultra low consumption and efficiency (thanks to the adaptable duty cycle, the low rate rates and the low coverage radio), and enable large scale networks for the WSN, making it one of the most convenient standards for this purpose.

ZigBee Communication

- ZigBee Coordinator: responsible for initializing, maintaining and controlling the network. There is one and only one per network
- ZigBee Router: connected to the coordinator or other routers. It can have zero or more children nodes. Participate in multi hop routing
- ZigBee End Devices: does not participate in routing



Zigbee Applications



Advantages

- ZigBee is standardized at all layers, this ensures that products from different manufacturers are compatible with each other.
- The power of the mesh, devices tend to connect with every near device, that makes every node of the network reachable from every other node and expanding the network geographically, also providing self healing, if the preferable path to a node fails there are other path to reach the node. The more devices you have the more reliable the network is.
- Low consumption of energy and working in the network even without the necessity of a battery (Green Power). Energy-harvesting devices lack batteries, getting it by extracting the energy they need from the environment.
- High scalability, ZigBee networks can to thousand of devices and they will communicate with each other using the best available path.

Activity

EEPROM Library

- The microcontroller on the Arduino and Genuino AVR based board has EEPROM: memory whose values are kept when the board is turned off (like a tiny hard drive).
- This library enables you to read and write those bytes.
- EEPROM available in UNO – 1024 bytes (1Kb)
- #include <EEPROM.h>

Activity

- EEPROM Clear: Clear the bytes in the EEPROM.
- EEPROM Read: Read the EEPROM and send its values to the computer.
- EEPROM Write: Stores values from an analog input to the EEPROM.
- EEPROM Crc: Calculates the CRC of EEPROM contents as if it was an array.
- EEPROM Get: Get values from EEPROM and prints as float on serial.
- EEPROM Iteration: Understand how to go through the EEPROM memory locations.
- EEPROM Put: Put values in EEPROM using variable semantics.
- EEPROM Update: Stores values read from A0 into EEPROM, writing the value only if different, to increase EEPROM life.

Activity

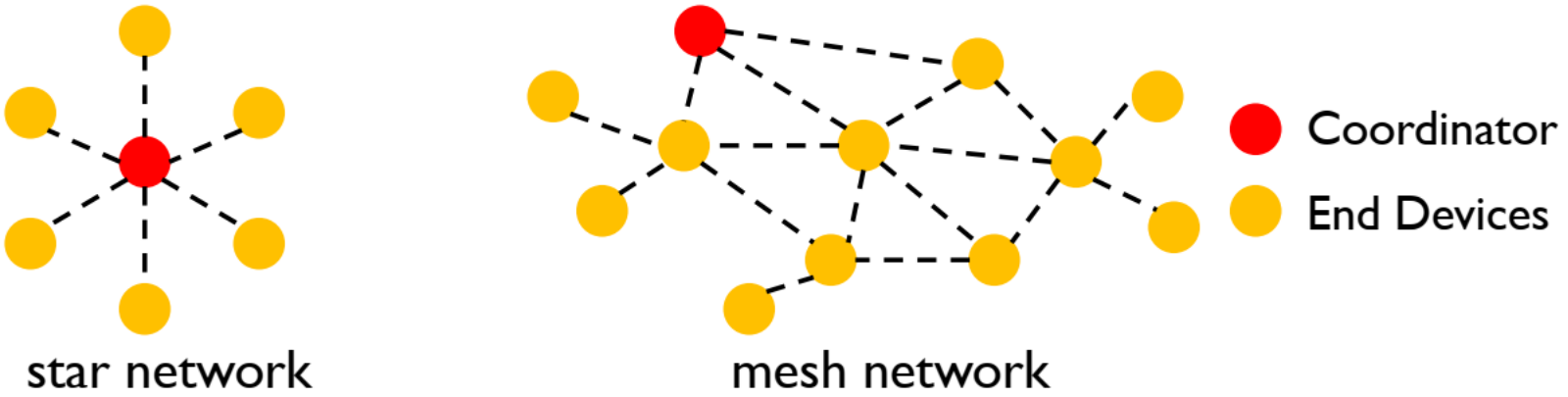
- Write a sketch that allows a user to access data in EEPROM using the serial monitor. In the serial monitor the user should be able to type one of two commands: “read” and “write. "Read" takes one argument, an EEPROM address. "Write" takes two arguments, an EEPROM address and a value.

- For example, if the user types “read 3” then the contents of EEPROM address 3 should be printed to the serial monitor. If the user types “write 3 10” then the value 10 should be written into address 3 of the EEPROM.

Wireless HART

Wireless HART

- For process measurement and control applications
- First open and interoperable wireless standard to address the critical needs of real-world industrial applications
- Existing standards fail in industrial environments
  - ZigBee: static channel
  - Bluetooth: quasi-static star network



Wireless HART

- HART (Highway Addressable Remote Transducer Protocol)
  - Most widely used field communication protocol
  - 30 million devices worldwide
- WirelessHART released in Sep 2007 (as a part of HART 7)
  - Adds wireless capabilities to the HART protocol while maintaining compatibility with existing devices, commands and tools.

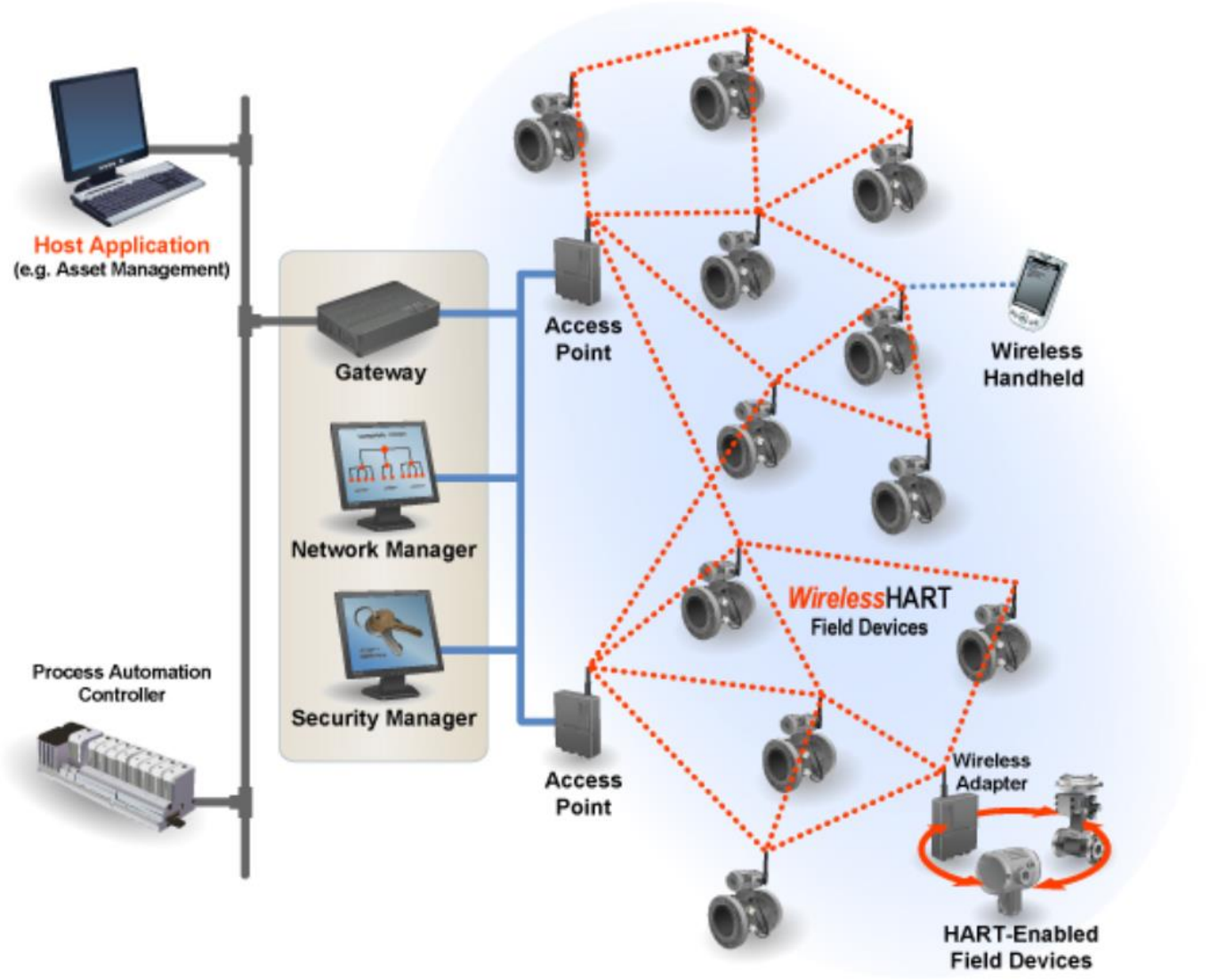
Wireless HART

- Monitor and control pressure and temperature of process fluids and gases
- Improved control of plant steam supply by detecting “cool spots” in cross plant steam lines
- Reducing risk of overfilling tanks by adding redundant level measurements (in oil and petroleum refineries)
- Monitor and control safety valves

Wireless HART

- Reliable: 99.9%
- Secure
- Self-organizing, self-healing
- Interoperable
- Supports both star and mesh topologies
- Built-in time synchronization

Network Architecture



Network Architecture

Network Manager

- Centralized brain
- Manages the network and its devices
  - Collect topology information
  - Routing, scheduling
  - Generates network management packets to devices
  - Change when devices/links break
  - User/administrator interacts with the Network Manager
- Redundant Network Managers supported (only one active)

Field Devices

- Sensor/actuator/both
- Connected to the process or plant equipment
- Combines wireless communication with traditional HART field device capabilities
- May be line or battery-powered

Network Architecture

WirelessHART Adapter

- Enables communication with a non-native device through a WirelessHART Network

Gateway

- One gateway can support up to 80 devices
- A Gateway provides
  - One or more Host Interfaces connecting the Gateway to backbone networks (e.g., the plant automation network)
  - One or more Access Points providing the physical connection into the WirelessHART network
  - A connection to the Network Manager
  - Buffering and local storage for publishing data, event notification, and common commands
  - Time synchronization sourcing

Network Architecture

Handheld devices

- Portable applications used to configure, maintain or control plant assets.
- Typically belong to networks of different standards

Plant Automation Network

- Connects client applications to the gateway

Security Manager

- Industry standard AES-128 ciphers/keys

WiMax

Why WiMax?

- WiMAX stands for wireless interoperatibility for microwave access.
- WiMAX is expected to do more for Metropolitan Area Networks (MANs) similar to Wi-Fi has done for local area networks (LANs)
- WiMAX is not projected to replace Wi-Fi, but to complement it by connecting Wi-Fi networks to each other or the Internet through high-speed wireless links.
- WiMAX technology can be used to extend the power and range of Wi-Fi and cellular networks.
- In developing countries, WiMAX may become the only wireless technology because Wi-Fi and cellular have not penetrated areas that can be reached with WiMAX technology

WiMax

- Worldwide Interoperability for Microwave Access (WiMAX) is currently one of the hottest technologies in wireless.
- WiMAX, is based on an RF technology called Orthogonal Frequency Division Multiplexing (OFDM), which is a very effective means of transferring data with carriers of width of 5MHz or greater.
- Below 5MHz carrier width, current CDMA based 3G systems are comparable to OFDM in terms of performance.
- WiMAX is a standard-based wireless technology that provides high throughput broadband connections over long distance.
- WiMAX can be used for a number of applications, including “last mile” broadband connections, hotspots and high-speed connectivity for business customers.
- It provides wireless metropolitan area network (MAN) connectivity at speeds up to 70 Mbps and the WiMAX base station on the average can cover between 5 to 10 km.

WiMax vs. WLAN

- Unlike WLAN, WiMAX provides a media access control (MAC) layer that uses a grant request mechanism to authorize the exchange of data. This feature allows better exploitation of the radio resources, in particular with smart antennas, and independent management of the traffic of every user.
- One of the inhibitors to widespread deployment of WLAN was the poor security feature of the first releases. WiMAX proposes the full range of security features to ensure secured data exchange:
  - Terminal authentication by exchanging certificates to prevent rogue devices,
  - User authentication using the Extensible Authentication Protocol (EAP),
  - Data encryption using the Data Encryption Standard (DES) or Advanced Encryption Standard (AES), both much more robust than the Wireless Equivalent Privacy (WEP) initially used by WLAN.

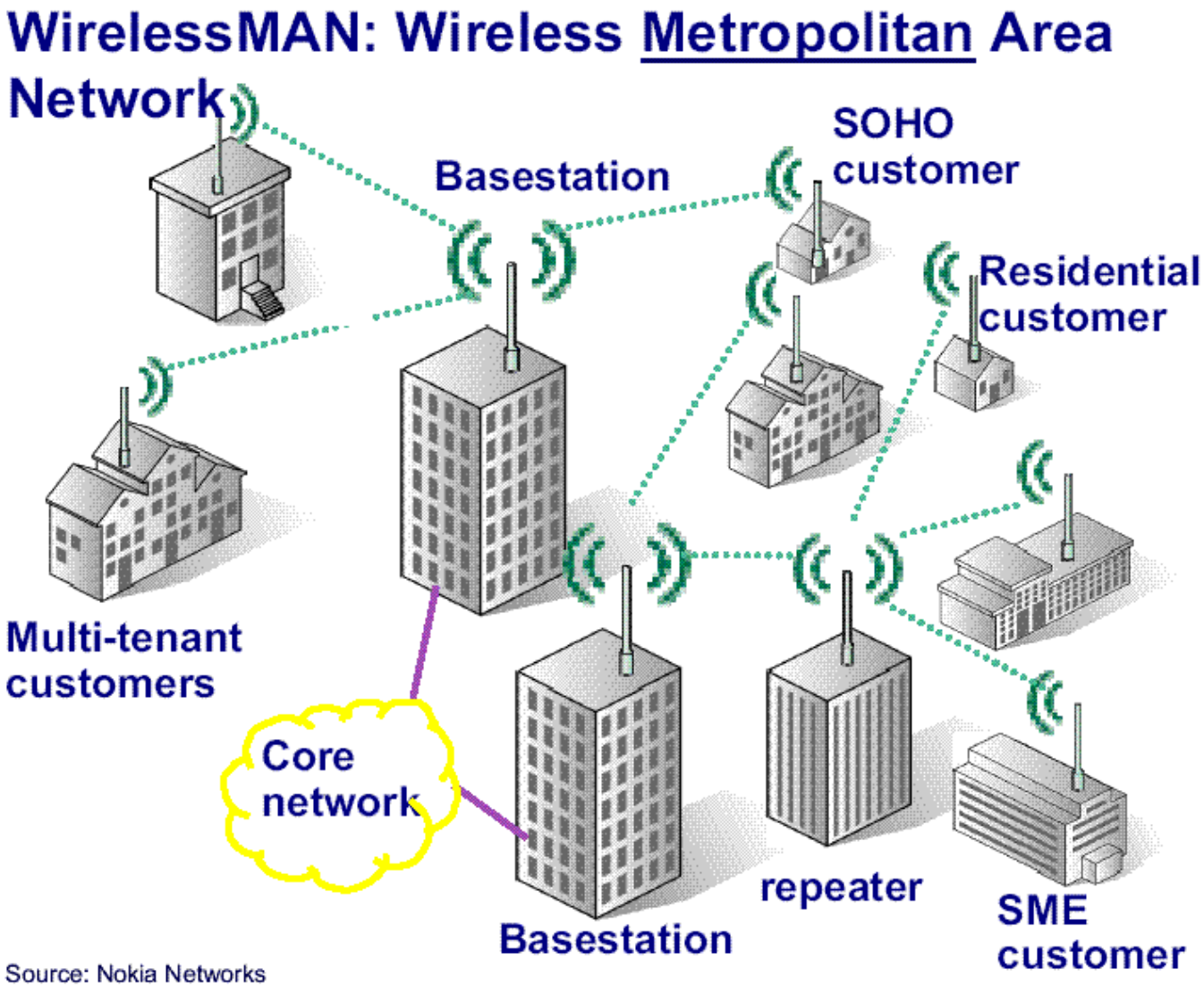
Comparison

Parameters	802.16 (WiMAX)	802.11 (WLAN)	802.15 (Bluetooth)
Frequency Band:	2-11GHz	2.4GHz	Varies
Range	~31 miles	~100 meters	~10meters
Data transfer rate:	70 Mbps	11 Mbps – 55 Mbps	20Kbps – 55 Mbps
Number of users:	Thousands	Dozens	Dozens

WiMax Uses

- The bandwidth and range of WiMAX make it suitable for the following potential applications:
- Connecting Wi-Fi hotspots with other parts of the Int
- Providing a wireless alternative to cable and DSL for "last mile" broadband access.
- Providing data and telecommunications services.
- Providing a source of Internet connectivity as part of a business continuity plan. That is, if a business has a fixed and a wireless Internet connection, especially from unrelated providers, they are unlikely to be affected by the same service outage.

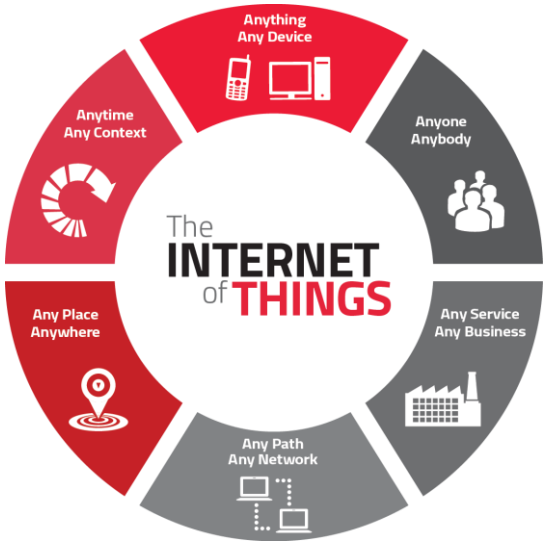
WiMax


WirelessMAN: Wireless Metropolitan Area Network
Basestation
SOHO customer
Residential customer
Multi-tenant customers
Core network
Basestation
repeater
SME customer
Source: Nokia Networks

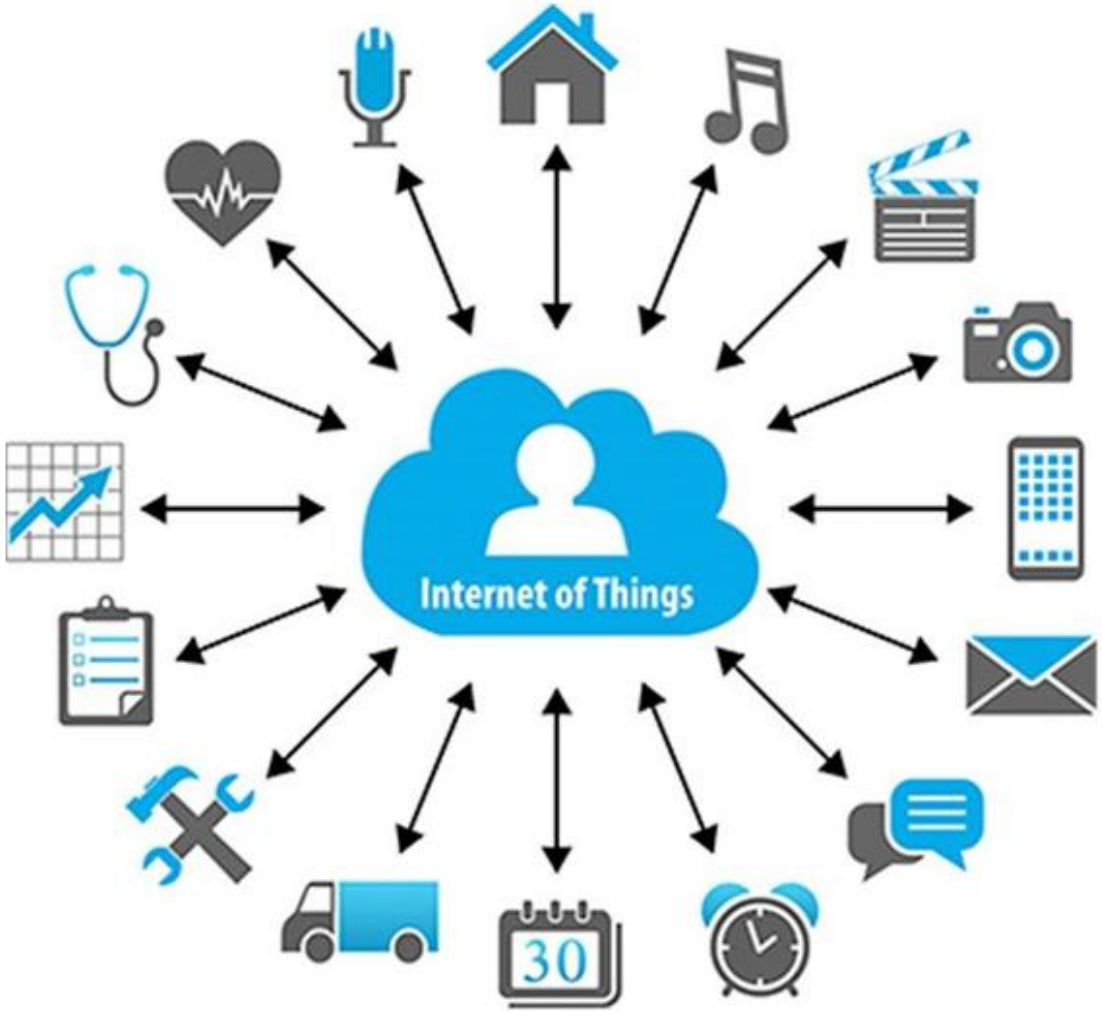
Evolution of IoT

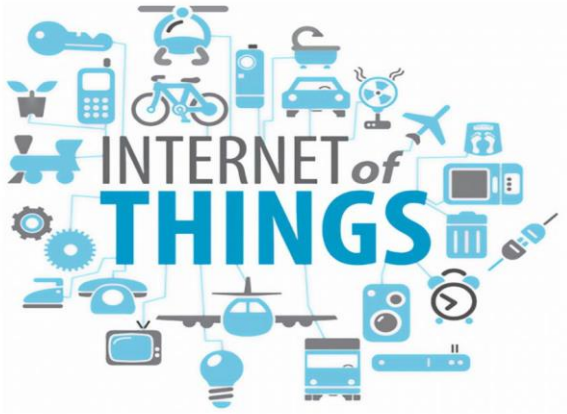
Evolution of IoT

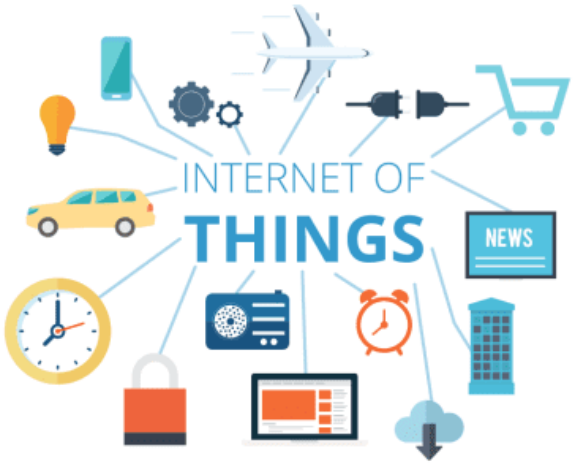
- ***The Internet of Things (IoT) is a system of interrelated computing devices, mechanical and digital machines, objects, animals or people that are provided with unique identifiers and the ability to transfer data over a network without requiring human-to-human or human-to-computer interaction.***
- It involves embedded computing devices interconnected with existing internet infrastructure.



Internet of things



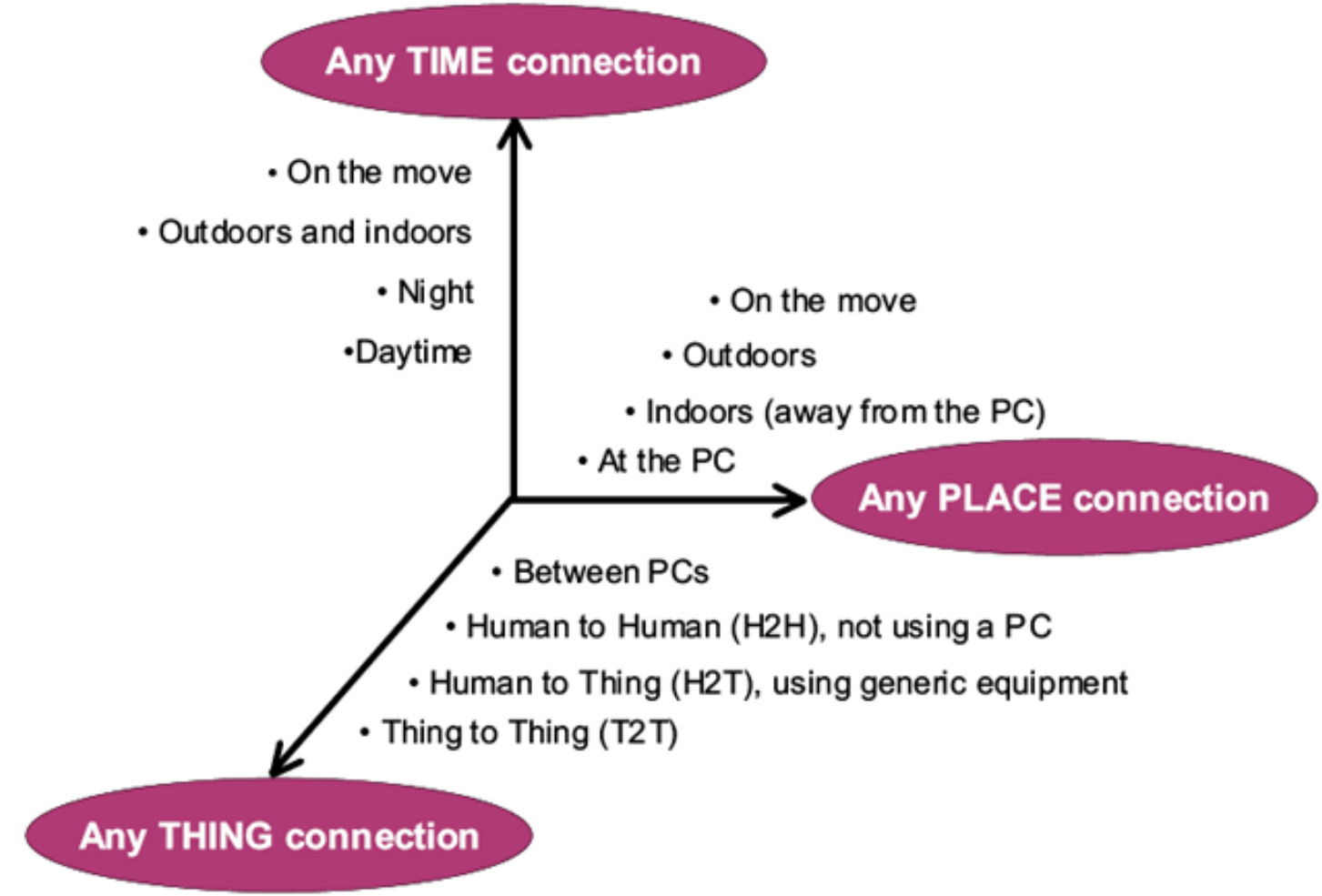




Various Names, One Concept

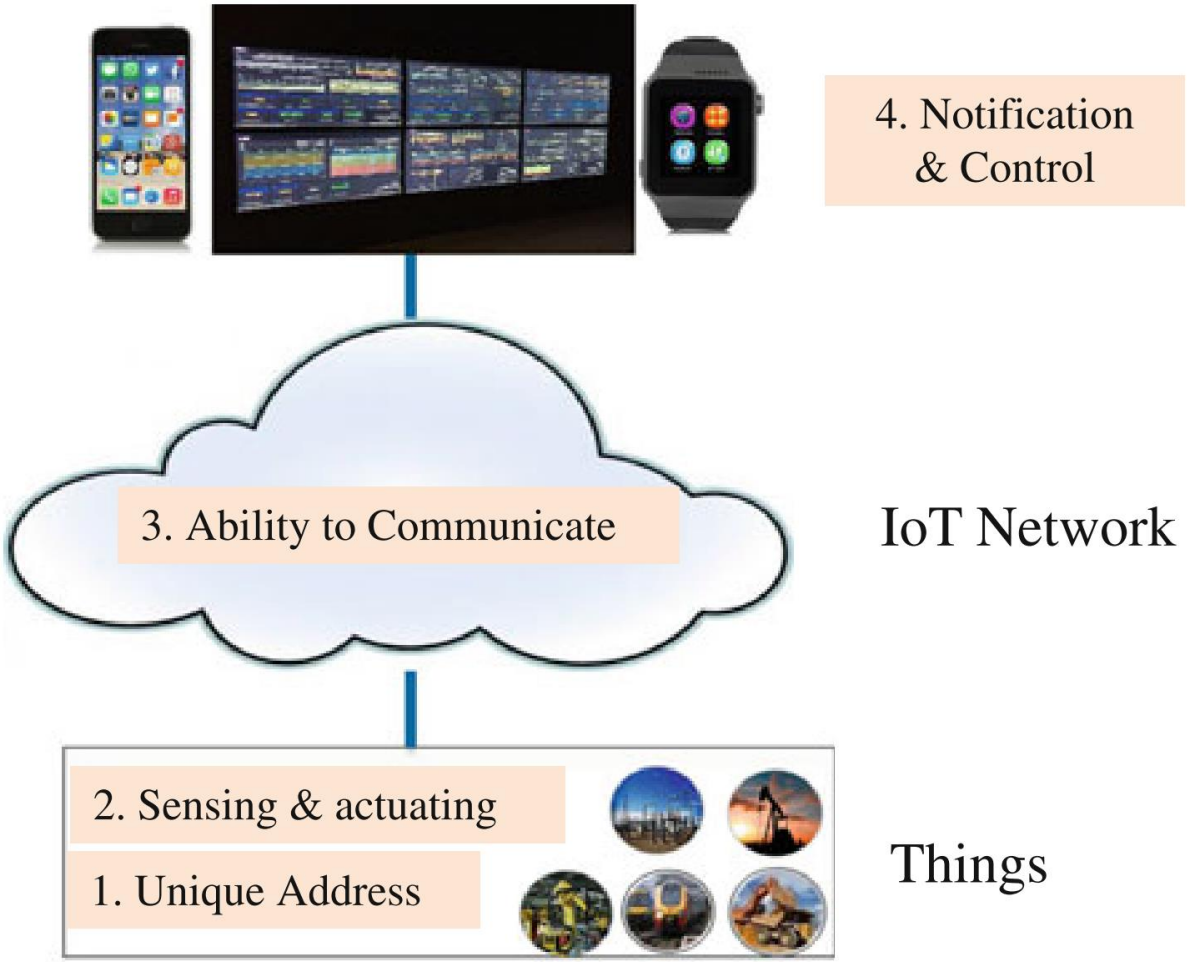
- M2M (Machine to Machine)
- “Internet of Everything” (Cisco Systems)
- “World Size Web” (Bruce Schneier)
- “Skynet” (Terminator movie)

A New Dimension

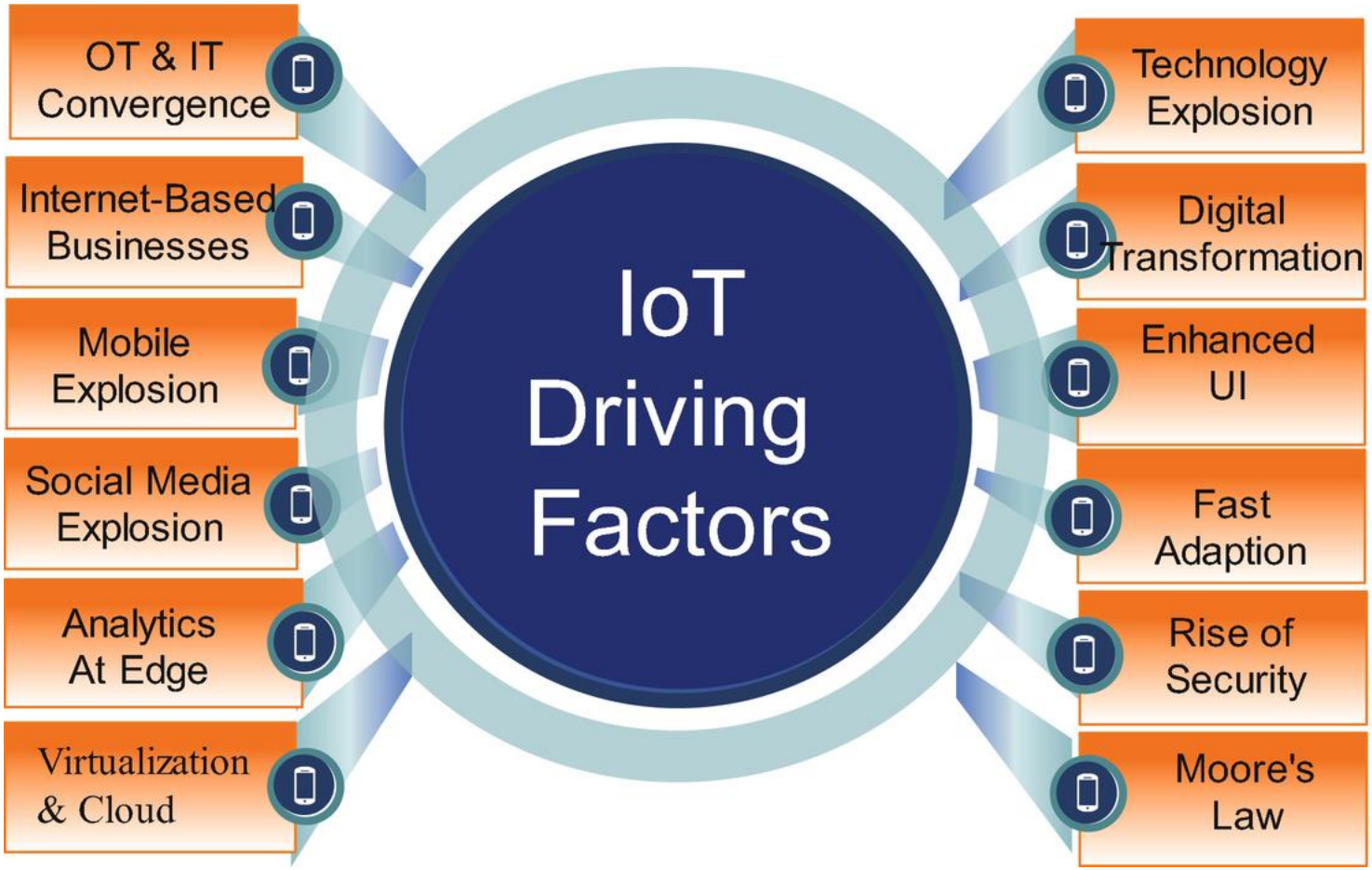


Source: ITU adapted from Nomura Research Institute

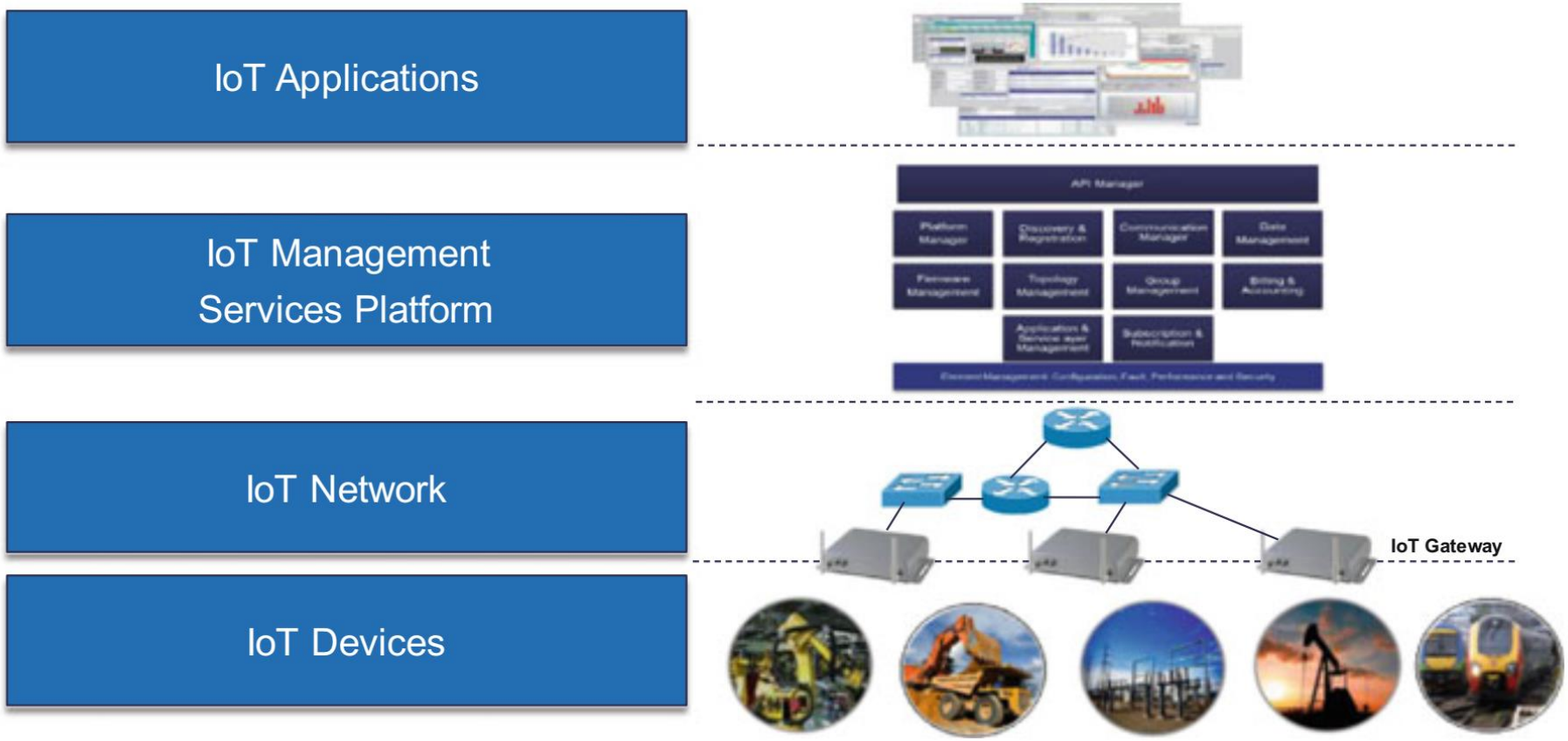
Basic requirements



12 driving factors of IoT



IoT Reference Framework

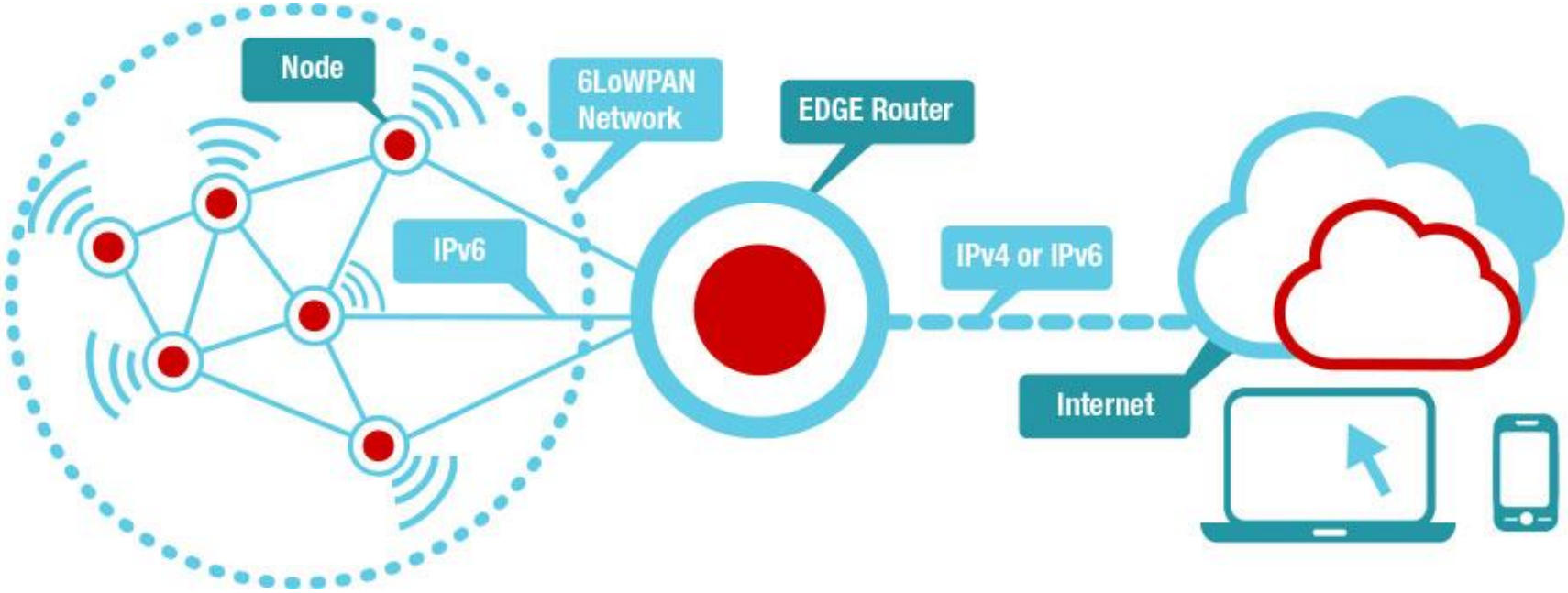


6LoWPAN

What is 6LoWPAN?

- 6LoWPAN is a somewhat contorted acronym that combines the latest version of the Internet Protocol (IPv6) and Low-power Wireless Personal Area Networks (LoWPAN).
- 6LoWPAN, therefore, allows for the smallest devices with limited processing ability to transmit information wirelessly using an internet protocol. It's the newest competitor to ZigBee.
- The concept was created because engineers felt like the smallest devices were being left out from the Internet of Things.
- 6LoWPAN can communicate with 802.15.4 devices as well as other types of devices on an IP network link like WiFi. A bridge device can connect the two.

6LoWPAN


Node
6LoWPAN Network
EDGE Router
IPv6
IPv4 or IPv6
Internet

6LoWPAN Basics

- The 6LoWPAN technology utilises IEEE 802.15.4 to provide the lower layers for this low power wireless network system.
- While this seems a straightforward approach to the development of an packet data wireless network or wireless sensor network, there are incompatibilities between IPv6 format and the formats allowed by IEEE 802.15.4.
- This differences are overcome within 6LoWPAN and this allows the system to be used as a layer over the basic 802.15.4.
- In order to send packet data, IPv6 over 6LowPAN, it is necessary to have a method of converting the packet data into a format that can be handled by the IEEE 802.15.4 lower layer system.

6LoWPAN Basics

- IPv6 requires the maximum transmission unit (MTU) to be at least 1280 bytes in length.
- This is considerably longer than the IEEE802.15.4's standard packet size of 127 octets which was set to keep transmissions short and thereby reduce power consumption.
- To overcome the address resolution issue, IPv6 nodes are given 128 bit addresses in a hierarchical manner.
- The IEEE 802.15.4 devices may use either of IEEE 64 bit extended addresses or 16 bit addresses that are unique within a PAN after devices have associated.
- There is also a PAN-ID for a group of physically co-located IEEE802.15.4 devices.

6LoWPAN Security

- It is anticipated that the Internet of Things, IoT will offer hackers a huge opportunity to take control of poorly secured devices and also use them to help attack other networks and devices.
- Accordingly security is a major issue for any standard like 6LoWPAN, and it uses AES-128 link layer security which is defined in IEEE 802.15.4. This provides link authentication and encryption.
- Further security is provided by the transport layer security mechanisms that are also included. This is defined in RFC 5246 and runs over TCP.
- For systems where UDP is used the transport layer protocol defined under RFC 6347 can be used, although this may require some specific hardware requirements.

6LoWPAN interoperability

- One key issue of any standard is that of interoperability. It is vital that equipment from different manufacturers operates together.
- When testing for interoperability, it is necessary to ensure that all layers of the OSI stack are compatible.
- 6LoWPAN is a wireless / IoT style standard that has quietly gained significant ground.
- Although initially aimed at usage with IEEE 802.15.4, it is equally able to operate with other wireless standards making it an ideal choice for many applications.
- 6LoWPAN uses IPv6 and this alone has to set it aside from the others with a distinct advantage.
- With the world migrating towards IPv6 packet data, a system such 6LoWPAN offers many advantages for low power wireless sensor networks and other forms of low power wireless networks.

6LoWPAN Applications

- General Automation: There are enormous opportunities for 6LoWPAN to be used in many different areas of automation.
- Home automation: There is a large market for home automation. By connecting using IPv6, it is possible to gain distinct advantages over other IoT systems. The Thread initiative has been set up to standardize on a protocol running over 6LoWPAN to enable home automation.
- Smart Grid: Smart grids enable smart meters and other devices to build a micro mesh network and they are able to send the data back to the grid operator's monitoring and billing system using the IPv6 backbone.
- Industrial monitoring: Automated factories and industrial plants provide a great opportunity for 6LoWPAN and using automation, can enable major savings to be made. The ability of 6LoWPAN to connect to the cloud opens up many different areas for data monitoring and analysis.

PCI

PCI

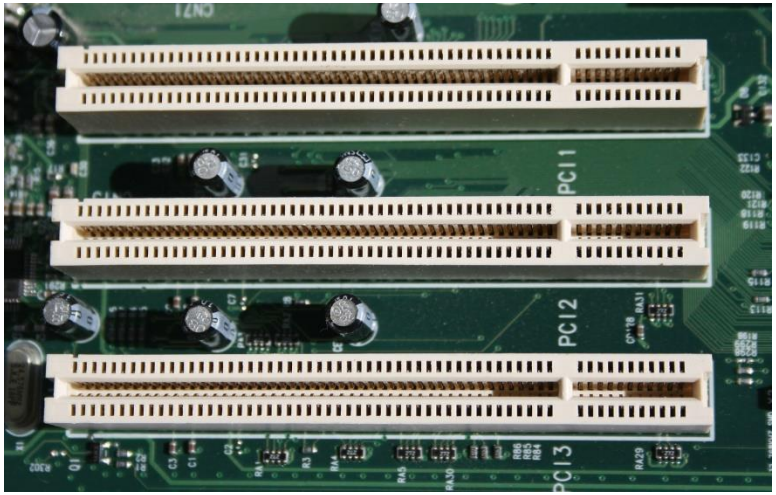
- PCI(Peripheral Component Interconnect) bus is based on ISA (Industry Standard Architecture) Bus and VL (VESA Local) Bus.
- Introduced by Intel in 1992
- Revised twice into version 2.1 which is the 64-bit standard that it is today.
- Great feature of PCI Bus was that it was invented as an industry standard
- PCI provides direct access to system memory for the devices that are connected to the bus which is then connected through a bridge that connects to the front side bus.
- This configuration allowed for higher performance without slowing down the processor

PCI Features

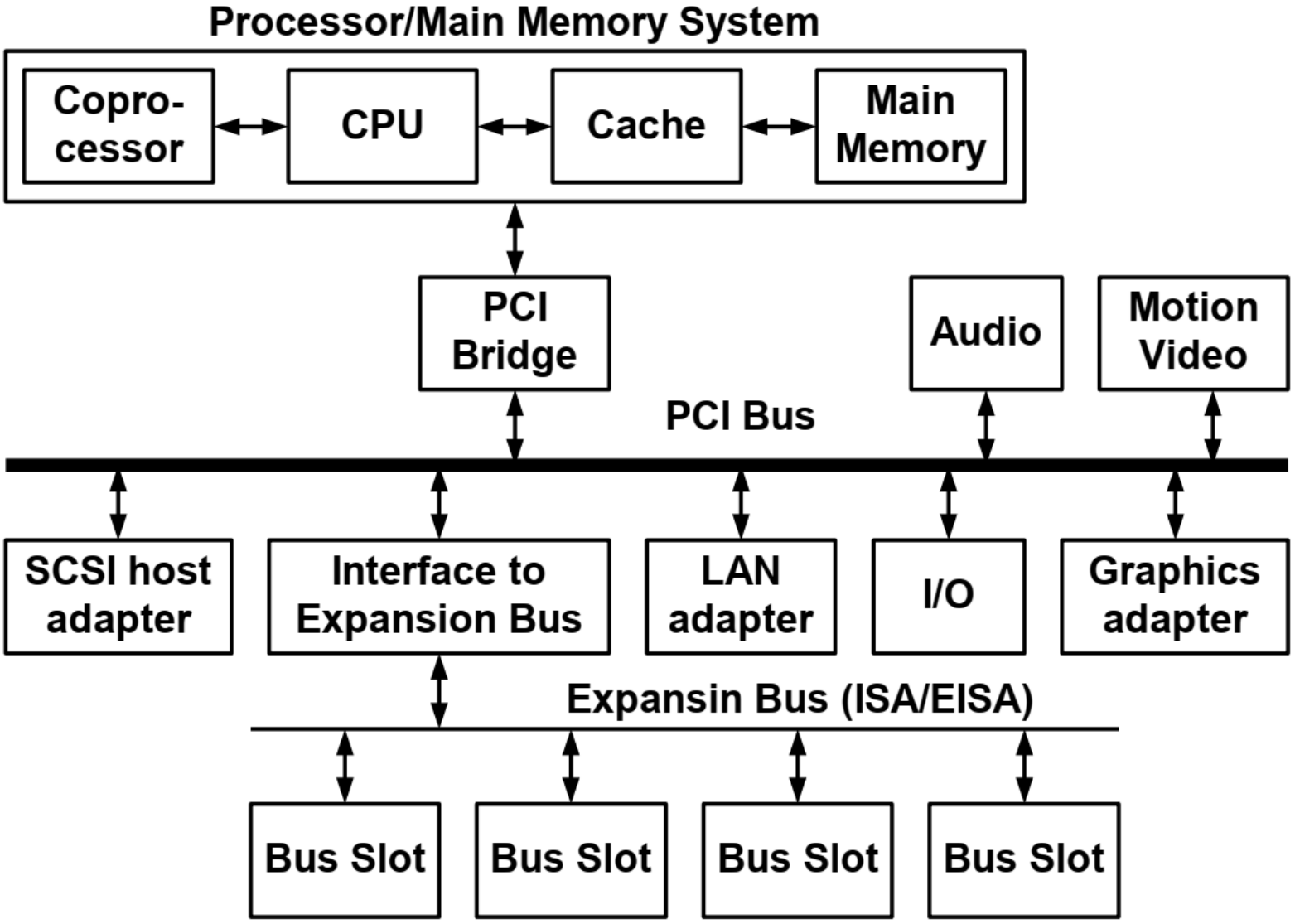
- The maximum theoretical transfer rate of the base configuration is 132 Mbytes/sec.
- Extensions to the base PCI specification can boost this by a factor of four to 528 Mbytes/sec.
- The PCI-X enhancements extend potential bandwidth to over 4 gigabytes per second.
- Any device on the bus can be a bus master and initiate transactions. One consequence of this is that there is no need for the traditional notion of DMA.
- The transfer protocol is optimized around transferring blocks of data. A single transfer is just a block transfer with a length of one.

PCI Features

- Although PCI is officially processor-independent, it inevitably reflects its origins with Intel and its primary application in the PC architecture. Among other things it uses little-endian byte ordering.
- PCI implements Plug-and-Play configurability.
- Every device in a system is automatically configured each time the system is turned on.
- The configuration protocol supports up to 256 devices in a system.
- The electrical specifications emphasize low power use including support for both 3.3 and 5 volt signaling environments.



PCI Bus Block diagram



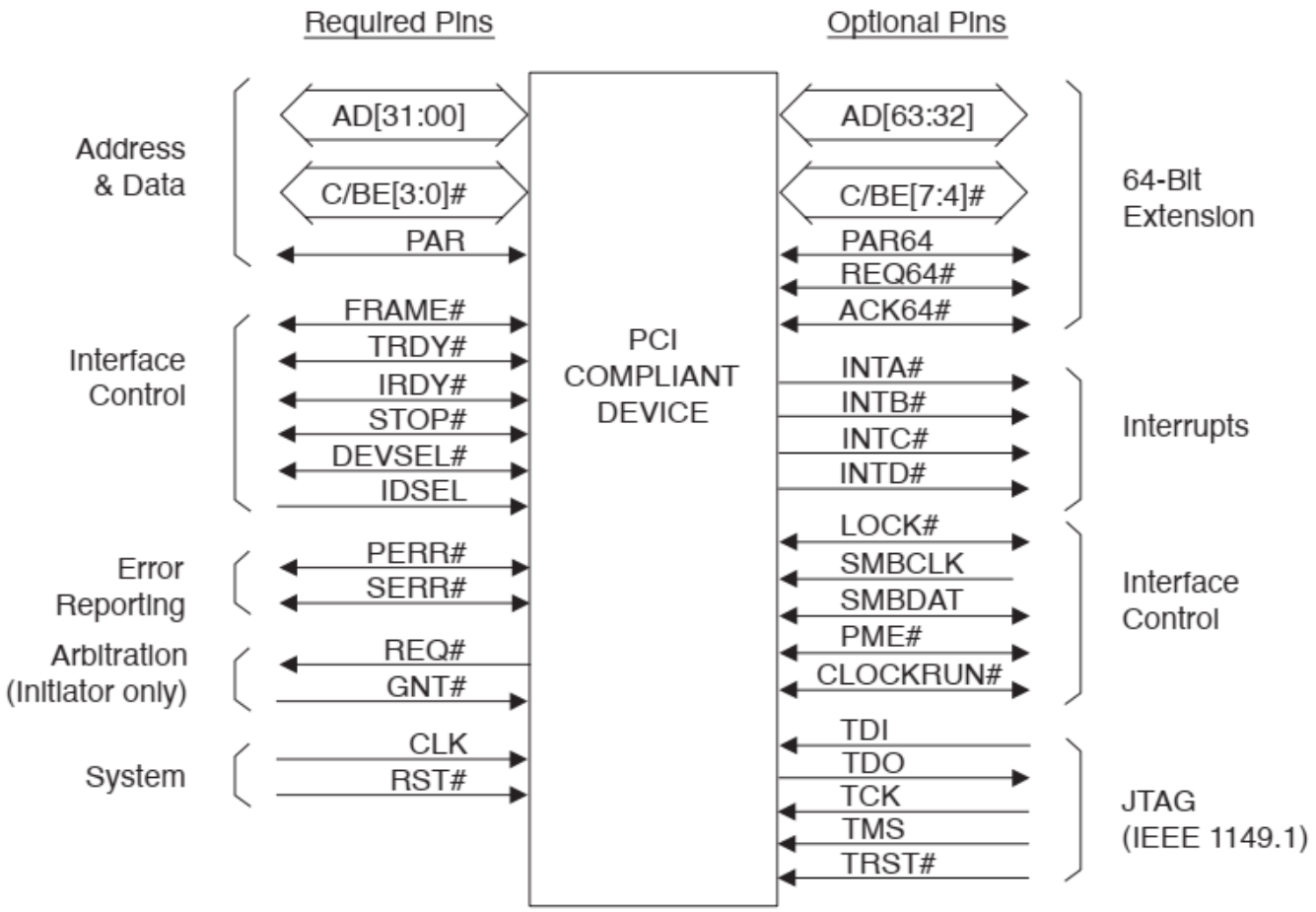
PCI Signals

- A PCI interface requires a minimum of 47 pins for a target-only device and 49 pins for a master.
- This is sufficient for a 32-bit data path running at up to 33 MHz and is mandatory for all devices claiming PCI compatibility.
- An additional 51 pins define optional features such as 64-bit transfers, interrupts and a JTAG interface.

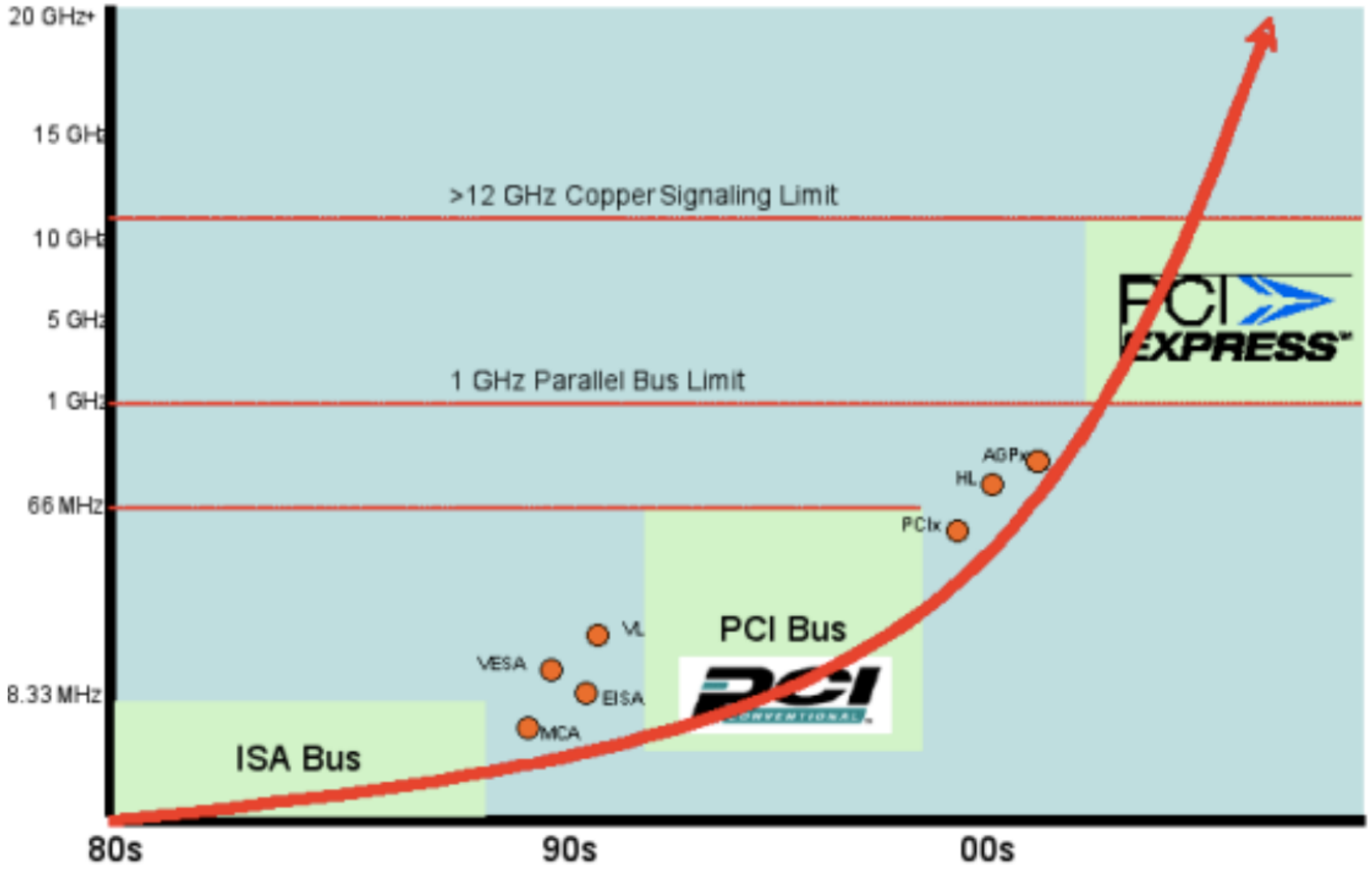
A note about notation:

- A # sign at the end of a signal name, such as FRAME#, indicates that the signal is active or asserted in the low voltage state.
- Signal names without a # are asserted in the high voltage state.
- The notation [n::m], where n and m are integers such that n is greater than m, represents an “array” of signals with n – m + 1 members. Thus, AD[31::0] represents the 32-bit data bus consisting of signal AD[0] to AD[31] with AD[0] being the least significant bit.

PCI Signals


Required Pins
Optional Pins
Address & Data
AD[31:00]
C/BE[3:0]#
PAR
AD[63:32]
C/BE[7:4]#
PAR64
REQ64#
ACK64#
64-Bit Extension
Interface Control
FRAME#
TRDY#
IRDY#
STOP#
DEVSEL#
IDSEL
PCI COMPLIANT DEVICE
INTA#
INTB#
INTC#
INTD#
Interrupts
Error Reporting
PERR#
SERR#
LOCK#
SMBCLK
SMBDAT
PME#
CLOCKRUN#
Interface Control
Arbitration (Initiator only)
REQ#
GNT#
System
CLK
RST#
TDI
TDO
TCK
TMS
TRST#
JTAG (IEEE 1149.1)

Evolution of PCI bus



PCI Read Write Operation

- All signals sampled on rising edge
- Centralized Parallel Arbitration
  - overlapped with previous transaction
- All transfers are (unlimited) bursts
- Address phase starts by asserting FRAME#
- Next cycle “initiator” asserts cmd and address
- Data transfers happen on when
  - IRDY# asserted by master/initiator when ready to transfer data
  - TRDY# asserted by target when ready to transfer data
  - transfer when both asserted on rising edge
- FRAME# deasserted when master intends to complete only one more data transfer

Advantages & Disadvantages

Advantages

- Very high speed
- Plug & Play
- Dominant board-level bus

Disadvantages

- Incompatible with older systems
- Can cost more

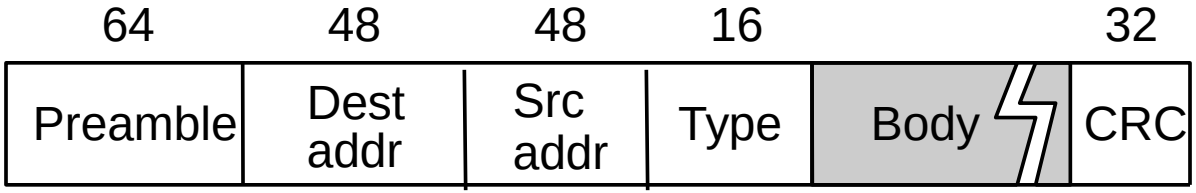
Ethernet

Ethernet

- Most popular packet-switched LAN technology
- Bandwidths: 10Mbps, 100Mbps, 1Gbps
- Max bus length: 2500m
  - 500m segments with 4 repeaters
- Bus and Star topologies are used to connect hosts
  - Hosts attach to network via Ethernet transceiver or hub or switch
    - Detects line state and sends/receives signals
  - Hubs are used to facilitate shared connections
  - All hosts on an Ethernet are competing for access to the medium
    - Switches break this model
- Ethernet operates at the link layer in TCP/IP model architecture.

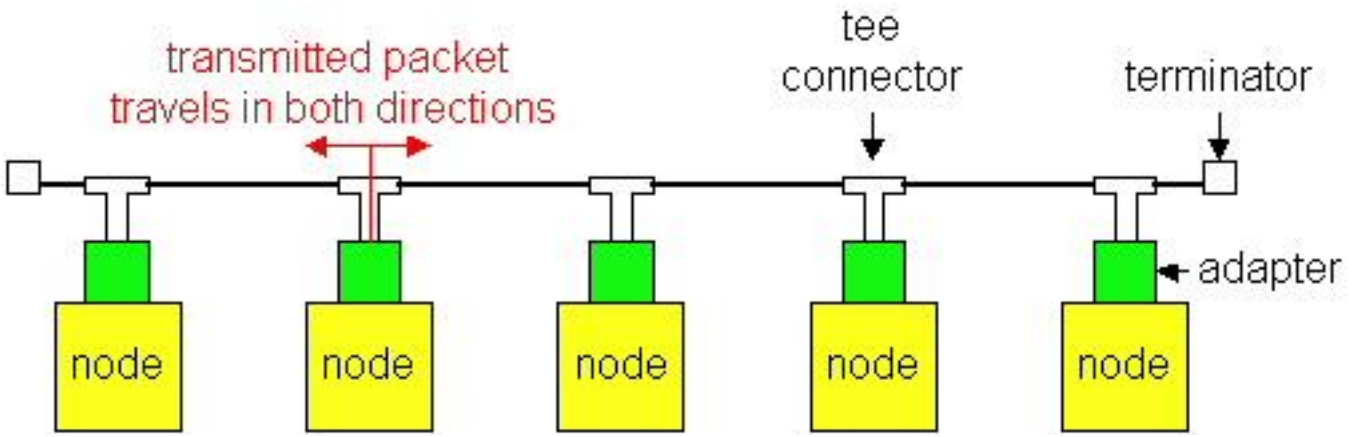
Ethernet

- Ethernet by definition is a broadcast protocol
  - Any signal can be received by all hosts
  - Switching enables individual hosts to communicate
- Network layer packets are transmitted over an Ethernet by encapsulating
- Frame Format



Ethernet

- Ethernet and Wi-Fi are both “multi-access” technologies
  - Broadcast medium, shared by many hosts
  - Simultaneous transmissions will result in collisions
- Media Access Control (MAC) protocol required
  - Rules on how to share medium
- The Data Link Layer is divided into two Parts: MAC (Media Access Control) Sub layer and LLC (Logic Link Control) Sub layer



Ethernet CSMA/CD

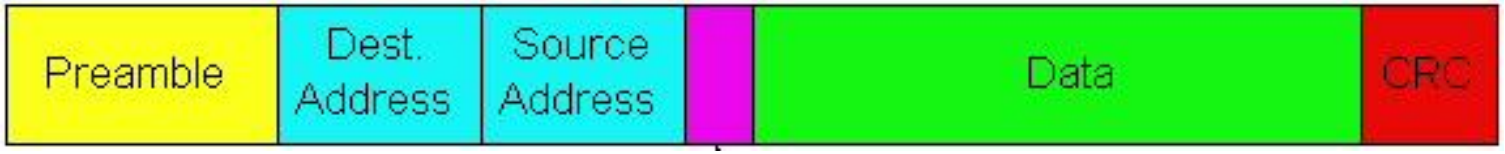
- CSMA/CD (carrier sense multiple access with collision detection) media access protocol is used.
  - Data is transmitted in the form of packets.
  - Sense channel prior to actual packet transmission.
  - Transmit packet only if channel is sensed idle; else, defer the transmission until channel becomes idle.
  - After packet transmission is started, the node monitors its own transmission to see if the packet has experienced a collision.
  - If the packet is observed to be undergoing a collision, the transmission is aborted and the packet is retransmitted after a random interval of time using Binary Exponential Back off algorithm.

Switched Ethernet

- Switches forward and filter frames based on LAN addresses
  - It's not a bus or a router (although simple forwarding tables are maintained)
- Very scalable
  - Options for many interfaces
  - Full duplex operation (send/receive frames simultaneously)
- Connect two or more "segments" by copying data frames between them
  - Switches only copy data when needed
    - key difference from repeaters
- Higher link bandwidth
  - Collisions are completely avoided
- Much greater aggregate bandwidth
  - Separate segments can send at once

Ethernet Frame Structure

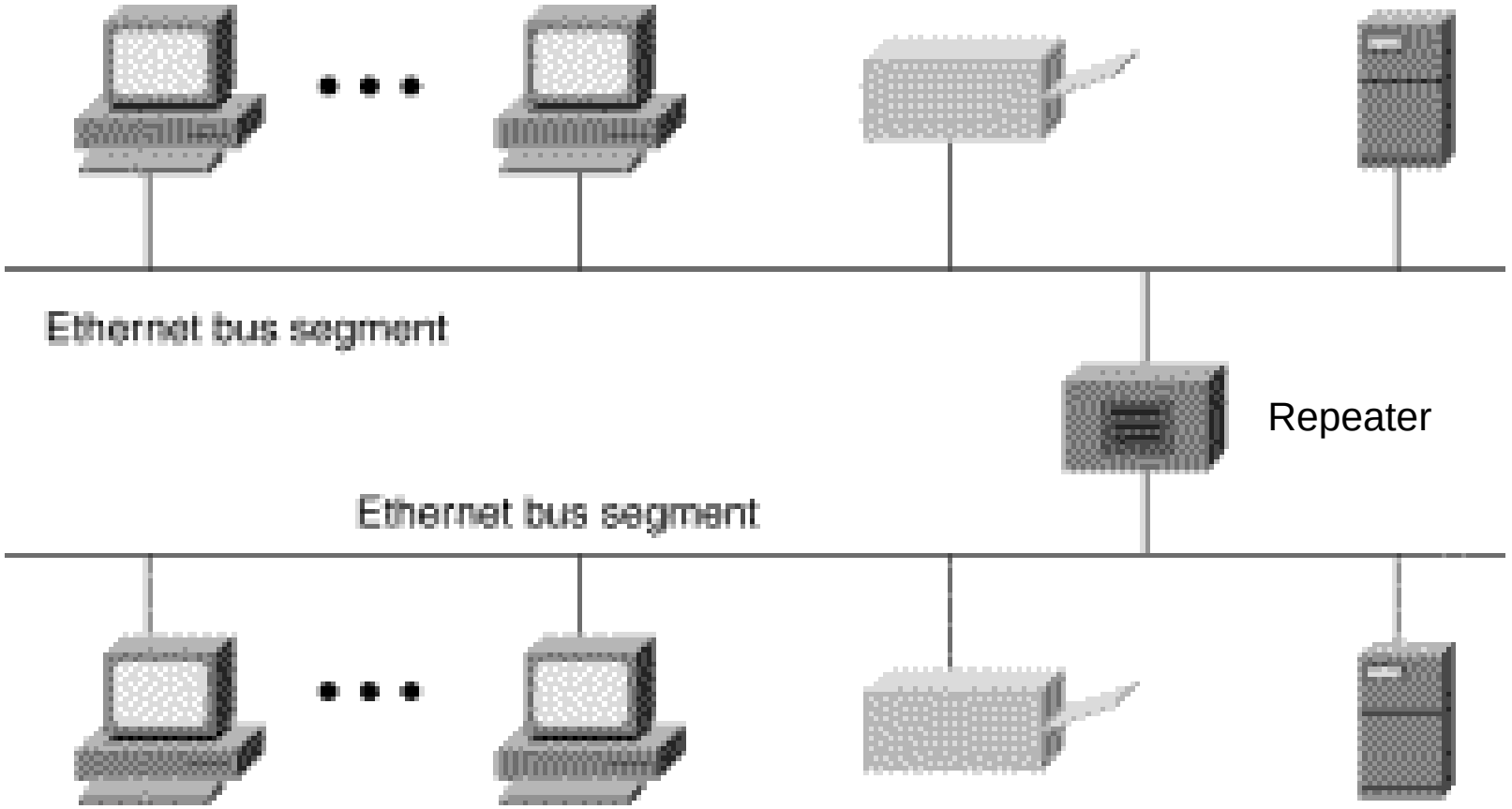
- Preamble:
  - 7 bytes with pattern 10101010 followed by one byte with pattern 10101011
  - Used to synchronize receiver, sender clock rates
- Addresses: 6 bytes, frame is received by all adapters on a LAN and dropped if address does not matched
- CRC: 4 bytes generated using CR-32, checked at receiver, if error is detected, the frame is simply dropped
- Data Payload: Maximum 1500 bytes, minimum 46 bytes
  - If data is less than 46 bytes, pad with zeros to 46 bytes



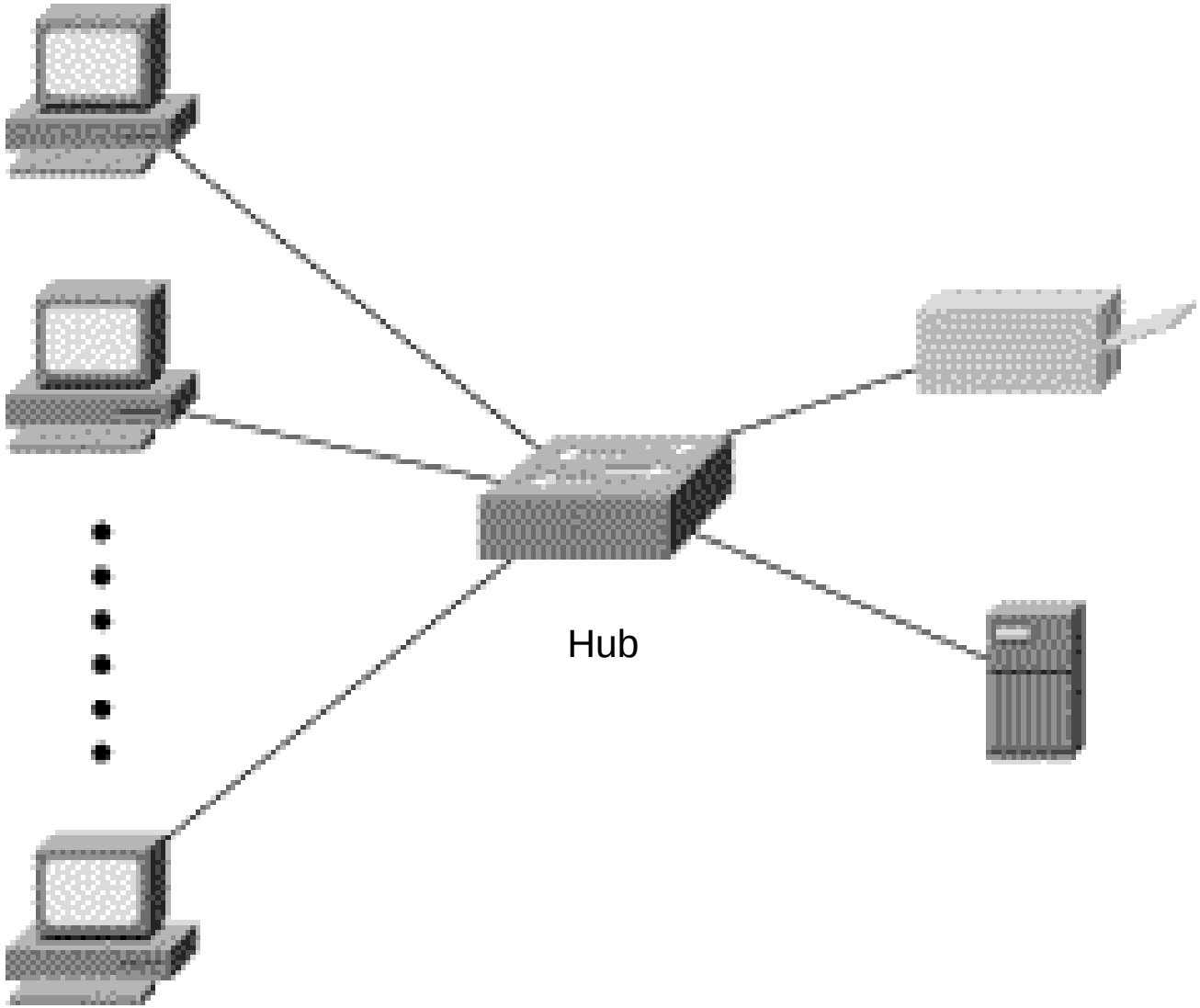
Classifications

- **Basic ethernet** is slowest among all, which provide the s speed of 10Mbps.
- **Fast Ethernet** provides the speed of 100Mbps, which is intermediate between basic and Gigabit network
- **Gigabit Ethernet** has the highest data transfer speed of 1Gbps. This speed is 10 times more than Fast Ethernet.

Ethernet BUS Topology



Ethernet STAR Topology



Advantages

- To form an Ethernet, we do not need much cost. It is **relatively inexpensive**. It is costless as compare to other systems of connecting computers.
- In Ethernet, **all the node have the same privileges**. It does not follow client-server architecture.
- It does not require any switches or hubs
- **Maintenance and administration are simple**.
- The cable used to connect systems in ethernet is **robust to noise**.
- As it is robust to the noise, the quality of the data transfer does not degrade. The **data transfer quality is good**.
- With a Gigabit network, users can transfer data with the **speed of 1-100Gbps**.

Disadvantages

- It does not hold good for real-time applications as it requires deterministic service.
- As the network cannot set priority for the packets, it is not suitable for a client-server architecture.
- In ethernet, there is a limit of the minimum size of the frame to 46B. The result of that, it is not a good choice for interactive applications.
- Not suitable for traffic-intensive applications. If the traffic on the Ethernet increases, the efficiency of the Ethernet goes down.
- After receiving a packet, the receiver doesn't send any acknowledge.
- If there is any problem in ethernet, it is difficult to troubleshoot what cable or node in the network causing an actual problem.

Activity

- About Arduino Shields
- https://learn.sparkfun.com/tutorials/arduino-shields
- Arduino Shield List (Don't memorize, just reference)
- http://playground.arduino.cc/Main/SimilarBoards
- Ethernet Shield
- https://www.arduino.cc/en/Main/ArduinoEthernetShield
- WiFi Shield
- https://www.arduino.cc/en/pmwiki.php?n=Main/ArduinoWiFiShield

Thank You