Started on	Friday, 11 March 2022, 2:40 PM
State	Finished
Completed on	Friday, 11 March 2022, 3:20 PM
Time taken	40 mins 1 sec
Grade	**32.50** out of 40.00 (**81**%)

Question **1**
Correct
Mark 2.00 out of 2.00

Match the following.

Remote Server	Rapid scalability may not be handled by it.	✔
Fog	A decentralized computing infrastructure used to reduce latencies and network bandwidth.	✔
Edge	The data processing is done in a location at or near the source of data generation.	✔
Cloud	Massive scalability of solutions through a shared pool hosted remotely.	✔

The correct answer is:
Remote Server → Rapid scalability may not be handled by it.,

Fog → A decentralized computing infrastructure used to reduce latencies and network bandwidth.,

Edge → The data processing is done in a location at or near the source of data generation.,

Cloud → Massive scalability of solutions through a shared pool hosted remotely.

Question **2**
Correct
Mark 1.00 out of 1.00

Which of the following IEEE standards provides the media layer of Thread?

- a. IEEE 802.15.1
- b. IEEE 802.15.3a
- c. IEEE 802.11a
- d. IEEE 802.15.4 ✔

The correct answer is:
IEEE 802.15.4

Question **3**

Correct

Mark 1.00 out of 1.00

The mapping of host logical address to its hardware address is done by

- a. RARP
- b. ARP ✔
- c. DNS
- d. DHCP

The correct answer is:
ARP

Question **4**

Correct

Mark 1.00 out of 1.00

Which protocol is derived from automatic identification and data capture technology?

Answer: RFID ✔

The correct answer is: RFID

Question **5**

Correct

Mark 0.50 out of 0.50

A network that connects a group of personnel in a home is called personal area network.

Select one:

- True ✔
- False

The correct answer is 'True'.

Question **6**

Correct

Mark 1.00 out of 1.00

Which topology is used to connect the weightless end devices to the base station.

Answer: Star Topology ✔

The correct answer is: Star topology

Question **7**

Partially correct

Mark 0.50 out of 1.00

Which connectivity protocol uses the principle of magnetic induction for data transmission between two devices?

- [ ] a. Sigfox
- [x] b. NFC ✔
- [ ] c. LoRa
- [ ] d. RFID

The correct answers are:
NFC,

RFID

Question **8**

Correct

Mark 1.00 out of 1.00

Which concept is used by ISO 100.11A to achieve immunity over interference over the network?

Answer: Channel black listing ✖

The correct answer is: Channel Blacklisting

Question **9**

Correct

Mark 1.00 out of 1.00

Which layer lacks in Wired HART?

Answer: Network layer ✔

The correct answer is: Network Layer

Question **10**

Correct

Mark 0.50 out of 0.50

IEEE 802.15.4 is widely used secured protocol in various IoT applications as it uses pseudorandom number for modulating the signals before transmission.

Select one:

- True ✔
- False

The correct answer is 'True'.

Question **11**

Not answered

Marked out of 1.00

Duty cycle of a temperature sensor is 20%. Find the sleep time of that sensor.

Answer: ✖

The correct answer is: 80

Question **12**

Correct

Mark 0.50 out of 0.50

The Class '1' IoT nodes may follow mesh topology within a LAN.

Select one:

- True ✔
- False

The correct answer is 'True'.

Question **13**

Correct

Mark 1.00 out of 1.00

Which cellular type communications was developed by Grenoble, France?

- a. WirelessHART
- b. Sigfox
- c. Weightless
- d. LoRa ✔

The correct answer is: LoRa

Question **14**

Incorrect

Mark 0.00 out of 0.50

Direct wireless communication can be achieved when a Zigbee device transmits data to the gateway in a NLOS (Non Line of Sight).

Select one:

- True ✖
- False

The correct answer is 'False'.

Question **15**

Incorrect

Mark 0.00 out of 0.50

The communication link from base station to IoT device is called uplink.

Select one:

- True ✖
- False

The correct answer is 'False'.

Question **16**

Correct

Mark 1.00 out of 1.00

Which device acts as a Trust Center and repository for security keys in ZigBee network?

Answer: ZigBee Coordinator ✔

The correct answer is: ZigBee co-ordinator

Question **17**

Correct

Mark 0.50 out of 0.50

Sensors are called input transducer as it converts various forms of energy into electrical signals.

Select one:

- True ✔
- False

The correct answer is 'True'.

Question **18**

Correct

Mark 2.00 out of 2.00

Match the following

Hybrid sensing	Measuring the scalar and vector property of environments at the same time ✔
Multimedia sensing	Measuring the amplitude of a quantifiable property concerning space and time ✔
Virtual sensing	Deriving the property of one area having no sensors by considering the other area's sensors data ✔
Scalar sensing	Measuring changes in the amplitude of the sensed values with respect to time ✔

The correct answer is:
Hybrid sensing → Measuring the scalar and vector property of environments at the same time,

Multimedia sensing → Measuring the amplitude of a quantifiable property concerning space and time,

Virtual sensing → Deriving the property of one area having no sensors by considering the other area's sensors data,

Scalar sensing → Measuring changes in the amplitude of the sensed values with respect to time

Question **19**

Correct

Mark 1.00 out of 1.00

Give the frequency in MHz of the highest RF band used by the ZigBee.

- a. 24000 MHz
- b. 2400 MHz ✔
- c. 24 MHz
- d. 240 MHz

The correct answer is:
2400 MHz

Question **20**

Correct

Mark 1.00 out of 1.00

Which protocol is based on an active RFID standard?

Answer: DASH7 ✔

The correct answer is: DASH7

Question **21**

Correct

Mark 1.00 out of 1.00

Which protocol is based on IEEE 802.11 standard?

Answer: Wi-Fi ✔

The correct answer is: Wifi

Question **22**

Correct

Mark 0.50 out of 0.50

Link local (LL) Addresses of IoT devices are unique within a LAN and may be repeated in other LANs.

Select one:

- (●) True ✔
- ( ) False

The correct answer is 'True'.

Question **23**

Correct

Mark 1.00 out of 1.00

Which one is not an add-on on IoT devices?

- ( ) a. In-built clock circuits
- (●) b. Digital to analog conversion units ✔
- ( ) c. Connection to the USB and ethernet
- ( ) d. Inbuilt wireless access capabilities

The correct answer is: Digital to analog conversion units

Question **24**

Not answered

Marked out of 1.00

Which methodology is used by the Sigfox end devices to send the messages to Sigfox base station?

Answer: ✖

The correct answer is: Principle of spatial diversity

Question **25**

Correct

Mark 0.50 out of 0.50

Internet of Things (IoT) is a sensor network of billions of smart devices that connect people, systems and other applications to collect and share data.

Select one:

- True ✔
- False

The correct answer is 'True'.

Question **26**

Correct

Mark 1.00 out of 1.00

Which protocol is used to multiplex multiple logical connections between two Bluetooth devices?

Answer: L2CAP ✔

The correct answer is: Logical Link Control and Adaptation Protocol

Question **27**

Not answered

Marked out of 1.00

A proximity sensor can sense a object at a minimum distance of 8 cm and maximum distance of 1.2 M. Find the sensing range of the that sensor.

Answer:

The correct answer is: 1.12

Question **28**

Correct

Mark 1.00 out of 1.00

Which method is used to achieve aggregation, manipulation, bandwidth reduction, and data operations directly on an IoT device?

- a. Offloading to the cloud
- b. Offloading to the remote server
- c. Offloading to the fog
- d. Offloading to the edge

The correct answer is:
Offloading to the edge

Question **29**

Correct

Mark 1.00 out of 1.00

Who acts as an initiative for third generation partnership project to develop a cellular network.

Answer: NB-IOT

The correct answer is: NB-IoT

Question **30**

Correct

Mark 1.00 out of 1.00

What is the minimum power level of IEEE 802.15.4 protocol in watt?

Answer: 0.0005 ✔

The correct answer is: 0.0005 W

Question **31**

Partially correct

Mark 0.40 out of 2.00

Match the following.

Which modulation scheme is used in which communication protocol.

LoRa	Choose...	
NB-IoT	Choose...	
ZWave	Choose...	
Bluetooth	Gaussian phase shift keying (GPSK) encoding scheme	✖
IEEE 802.15.4	Direct Sequence Spread Spectrum (DSSS)	✔

The correct answer is:
LoRa → Frequency Modulated chirp coding,

NB-IoT → Orthogonal frequency division multiplexing (OFDM),

ZWave → Gaussian phase shift keying (GPSK) encoding scheme,

Bluetooth → Frequency hopping spread spectrum (FHSS),

IEEE 802.15.4 → Direct Sequence Spread Spectrum (DSSS)

Question **32**

Not answered

Marked out of 1.00

Identify the subnet address from the following IPv6 address.

1834:7B8F:1345:4E45:1234:AAAA:5B78:3421

Answer: ✖

The correct answer is: 4E45

Question **33**

Correct

Mark 1.00 out of 1.00

There are four temperature sensors namely A, B, C, D. A can detect up to 0.5°C, B can detect up to 0.25 °C, C can detect up to 0.125 °C and D can detect up to 0.0625 °C changes in temperature. Then find best resolution temperature sensor.

- a. The temperature sensor D ✔
- b. The temperature sensor B
- c. The temperature sensor A
- d. The temperature sensor C

The correct answer is: The temperature sensor D

Question **34**

Correct

Mark 2.00 out of 2.00

Match the following.

Smart Factories	monitor and manages plant processes	✔
Smart Meters	capable of communicating remotely with the power grid	✔
Digital locks	Smartphones can be used to lock and unlock doors remotely	✔
Unnamed Aerial Vehicles	A public domain solution for stock maintenance	✔
Smart dust	Microscopic computers	✔

The correct answer is:

Smart Factories
→ monitor and manages plant processes,

Smart Meters → capable of communicating remotely with the power grid,

Digital locks → Smartphones can be used to lock and unlock doors remotely,

Unnamed Aerial Vehicles → A public domain solution for stock maintenance,

Smart dust → Microscopic computers

Question **35**

Correct

Mark 1.00 out of 1.00

Which factor is not governing the selection and design of the IoT device?

- a. I/O routing ✔
- b. Design parameters
- c. Affordability
- d. Usability

The correct answer is: I/O routing

Question **36**

Correct

Mark 0.50 out of 0.50

Collaborative processing reduces the processing and network latencies.

Select one:

- True ✔
- False

The correct answer is 'True'.

Question **37**

Correct

Mark 1.00 out of 1.00

Which cellular type communications was developed by Grenoble, France?

Answer: LoRa ✔

The correct answer is: LoRa

Question **38**

Correct

Mark 0.50 out of 0.50

Active Tag is powered by RFID reader before data transmission between Tag and Database.

Select one:

- True
- False ✔

The correct answer is 'False'.

Question **39**

Correct

Mark 1.00 out of 1.00

Which mode enables an NFC device to act as a contactless credit card and make payments using just a simple tap on an NFC reader.

- a. Read/Write Mode
- b. Peer-to-Peer
- c. Machine-to-Machine
- d. Card Emulation mode ✔

The correct answer is: Card Emulation mode

Question **40**

Partially correct

Mark 1.60 out of 2.00

Match the following.

Peer-to-Peer	Devices may connect to a tree as a leaf node	✗
Star	Suffers with single point of failure	✓
Bus	Multiple drop lines and taps are used	✓
Mesh	Expensive topology with respect to number of links	✓
Ring	Each device has exactly two neighboring nodes irrespective of network size	✓

The correct answer is:
Peer-to-Peer → ad hoc, self-organizing, and self-healing topology,

Star → Suffers with single point of failure,

Bus → Multiple drop lines and taps are used,

Mesh → Expensive topology with respect to number of links,

Ring → Each device has exactly two neighboring nodes irrespective of network size

Jump to...

End Sem Exam May 2022 ►

PREMIDTERM EXAM

Total points 19/30

The respondent's email (**201951069@iiitvadodara.ac.in**) was recorded on submission of this form.

1. What is the standard length of IPv6 address? 1/1

- ○ 64
- ◉ 128
- ○ 127
- ○ 256

2. Which of the following is not a IoT networking components? 1/1

- ○ IoT LAN
- ◉ IOT MAN
- ○ All of these
- ○ Non of these

3. Which protocol dynamically allocate IPv6 addresses. 0/1

- ◉ DHCPv6
- ○ SLAAC
- ○ All of these
- ○ None of these

4.When a node/network is connected to multiple networks simultaneously for improved reliability, it is called 1/1

- ○ PAN
- ○ MAN
- ○ WAN
- ◉ Multihoming

5. Which statement is true about the characteristics of IoT? 1/1

- ○ Efficient, scalable and associated architecture
- ○ Unambiguous naming and addressing
- ○ Abundance of sleeping nodes, mobile and non-IP devices
- ◉ All the above

6. What is the main purpose of WoT (Web of Things) in the IoT? 1/1

- ○ Increase the cost
- ○ Complex the development
- ◉ Improve the usability and interoperability
- ○ Reduce the security

7. Which protocol is used to translate Internet domain name and host name into IP address? 1/1

- ○ Domain information system
- ○ Router
- ○ Domain name database
- ◉ Domain name system

8. Which of the following is not an advantage of IoT? 1/1

- ○ Improved Customer Engagement
- ◉ Security
- ○ Enhanced data collection
- ○ Reduced waste

9. Which statement is false about IoT? 0/1

- ○ "Things", in the IoT sense, can refer to a wide variety of devices.
- ○ Things can communicate with each other using Internet.
- ◉ All the things are IP protocol enabled.
- ○ None of these

10. Long range communication protocol includes 0/1

- (●) Wi-Fi
- ( ) Bluetooth
- ( ) Zigbee
- ( ) Non of these

11. Which statement is true. 0/1

- ( ) The accuracy of a sensor is the ability to measure the true environment parameter.
- ( ) A sensor's accuracy depends on its resolution.
- (●) The more is the resolution of a sensor, the less accurate is its precision.
- ( ) The resolution of a sensor is the largest change that it can detect.

12. Measuring changes in the amplitude and direction of the measured values with respect to time is called 1/1

- (●) Multimedia sensing
- ( ) Scalar sensing
- ( ) virtual sensing
- ( ) Hybrid sensing

13.. If the output signal differs from the correct signal value by a constant value, then that type of error is called 1/1

- (●) Offset error
- ( ) Aliasing error
- ( ) Sensitivity error
- ( ) Hysteresis error

14. The choice of sensors in IoT based solutions depends on 1/1

- ( ) Sensing range, Energy and Device size
- ( ) Accuracy
- ( ) precision
- (●) All the above

15. Which statement is true? 1/1

- (●) An actuator requires a control signal and a source of energy for its operation.
- ( ) Transducers converts electrical signal to mechanical energy.
- ( ) Sensor converts one form of energy to another form of energy.
- ( ) None of these

16. The selection of actuators in an IoT application depends on 1/1

- ○ Weight and power rating
- ○ Torque to weight ratio
- ○ Stiffness and compliance
- ◉ all the above

17. Internet of Things is the 0/1

- ○ Union of Information Technology and Operational Technology
- ○ Intersection of Information Technology and Operational Technology
- ◉ Difference of Information Technology and Operational Technology
- ○ none of these

18. Which topology is used between IoT node and IoT Gateway in Class 5 addresses? 1/1

- ◉ Star
- ○ Mesh
- ○ Ring
- ○ Point-to-point

19. The transfer of data from a private network to a public network in the form of encapsulated packets is called 1/1

- (●) Tunnelling
- ( ) Multihoming
- ( ) Security
- ( ) Non of these

20. Addressing of mobile nodes in IoT applications are done using 1/1

- ( ) Global prefix changes
- ( ) Prefix changes within WANs
- ( ) Remote anchoring
- (●) All the above

21. Global prefix part of IPv6 address is the 0/1

- (●) In between three blocks of the address
- ( ) Last three blocks of the address
- ( ) First two blocks of the address
- ( ) First three blocks of the address

22. Which one is called the digital twin system? 0/1

- (●) WoT
- ( ) CPS
- ( ) M2M
- ( ) IoP

23. Which network is restricted to individual usage? 1/1

- (●) PAN
- ( ) LAN
- ( ) MAN
- ( ) WAN

24. Which protocol is not an application layer protocol. 1/1

- ( ) HTTP
- (●) ARP
- ( ) DNS
- ( ) FTP

25. Which technology aims to decentralize online social interactions, payments, and transactions while maintaining privacy of user data. 0/1

- ○ IOT
- ○ IOP
- ○ IOE
- ◉ M2M

26. Which addresses are unique within a single network segment? 0/1

- ○ Link Local
- ◉ Unique Local
- ○ All the above
- ○ None of these

27. Which datalink layer addressing is not supported in IPv6. 1/1

- ○ Unicast
- ◉ Broadcast
- ○ Multicast
- ○ None of these

28. Which device forwards packets between LANs and WANs. 0/1

- ○ IoT Gateway
- ◉ IoT Router
- ○ IoT Proxy
- ○ All the above

29. Characteristic features of IoT includes 1/1

- ○ Any Time
- ○ Any Where
- ○ Any Thing
- ◉ All the above

30. The enablers of IoT paradigm include 0/1

- ◉ Services
- ○ Local and Global Connectivity
- ○ Processing
- ○ All the above

This form was created inside of Indian Institute of Information Technology, Vadodara.

Google Forms

Blank Quiz

Quiz on Data Protocol

The respondent's email (**201951069@iiitvadodara.ac.in**) was recorded on submission of this form.

Which statement is false?

- (●) It provides many-many distributions of messages over a constraint network.
- ( ) It is designed for constraint devices and networks.
- ( ) MQTT is a simple, light weight, publish subscribe protocol.
- ( ) Payload content of MQTT is agnostic.

Which one is not a component of SOAP Protocol?

- ( ) Encoding Rules
- (●) Request and Response Messages
- ( ) Envelope
- ( ) Conventions

Which data protocol supports 14 message types for data communication?

- ( ) XMPP
- ( ) COAP
- ( ) AMQP
- (●) MQTT

Which protocol handles the requirements and challenges of wireless communication over sensor network?

- ○ COAP
- ◉ MQTT-SN
- ○ AMQP
- ○ XMPP

Which web transfer protocol supports 8-bit processor.

- ○ XMPP
- ◉ COAP
- ○ MQTT
- ○ AMQP

COAP is

- ○ Constrained object Application Protocol
- ◉ Constrained Application Protocol
- ○ Constant object Application Protocol
- ○ Constant object Applied Protocol

HTTP binding for XMPP traffic is known as

- ○ Multi user chat
- ○ Pub-Sub
- ◉ BOSH
- ○ Jingle

Which one is not a feature of SOAP?

- ○ Neutrality
- ◉ Reliability
- ○ Extensibility
- ○ Independence

Which protocol is used for accessing, storage, and distribution of data over the IoT network?

- ○ Discovery Protocol
- ○ Device Management Protocols
- ◉ Data Protocol
- ○ Identification Protocols

Abbreviation of MQTT is

- ○ Message Query Telephony Transmission
- ○ Message Query Telemetry Transport
- ○ Manage Queue Telemetry Transport
- ◉ Message Queue Telemetry Transport

Which frame type of AMQP is responsible for message transfer over the link?

- ○ Flow
- ◉ Transfer
- ○ Attach
- ○ Disposition

Which data protocol supports request-response paradigm for communication over lossy networks?

- ○ XMPP
- ◉ COAP
- ○ MQTT
- ○ AMQP

Which protocol uses Jabber ID for data transmission?

- ○ Uniform Resource Identifier
- ○ Web sockets
- ○ Simple object access Protocol
- ◉ Extensible messaging and presence protocol

Which Id is similar to email address?

- ○ Unique Address
- ○ Electronic code Identifier
- ○ Resource Id
- ◉ Jabber Id

Which protocol supports Message format, Message exchange pattern, Transport protocol binding, Message processing model and Protocol extensibility layer.

- ○ XMPP
- ○ MQTT
- ◉ SOAP
- ○ COAP

Which protocol data unit is known as Frame?

- (●) AMQP
- ( ) XMPP
- ( ) MQTT
- ( ) COAP

Without user ID in JID is considered as

- ( ) Request Message
- (●) control message or system message
- ( ) Response Message
- ( ) Domain Identifier

Which data protocol is a language and platform independent protocol?

- ( ) COAP
- ( ) XMPP
- ( ) MQTT
- (●) SOAP

Piggybacking is defined as

- ○ The transmission of request with acknowledgement message
- ◉ The transmission of responses with acknowledgement message
- ○ The transmission of request message
- ○ The transmission of response message

Which method is used for sending data from the publisher to the broker?

- ◉ PUBLISH
- ○ PUBREL
- ○ PUBACK
- ○ PUBREC

This form was created inside of Indian Institute of Information Technology, Vadodara.

Google Forms

Blank Quiz

The respondent's email (**201951069@iiitvadodara.ac.in**) was recorded on submission of this form.

Which device is routing the universal metadata message to the destination or any other UMB-A by the Middleware Routing Table (MRT).

- ○ PTU
- ◉ UMB Core
- ○ UMB Adaptor
- ○ UMB

Which one is a closed communication protocol?

- ○ IEEE 802.11a
- ○ IEEE 802.15.1
- ○ IEEE 802.15.4
- ◉ Z-Wave

Which one is not a device classification solution?

- ○ eCl@ss
- ◉ URI
- ○ UNSPSC

Which device converts physical devices into virtually abstracted device, as described by Universal Device Template (UDT)?

- (●) UMB Adaptor
- ( ) UMB Core
- ( ) PTU
- ( ) UMB

The interoperability between devices and device user in term of message's meaning is known as

- ( ) User Interoperability
- ( ) Syntactic Interoperability
- (●) Semantics Interoperability
- ( ) Device Interoperability

Meaning of ontology is *

- (●) Knowledge extraction
- ( ) Physical domain Identifier
- ( ) Knowledge base
- ( ) Estimation procedure

Why Interoperability is Important in Context of IoT?

- ○ Physical objects can interact with any other physical objects and can share their information.
- ○ Any device can communicate with any other devices anytime from anywhere.
- ◉ All
- ○ None

Interoperability problem between a user and a device is known as

- ○ Device Interoperability
- ○ Semantics Interoperability
- ○ Syntactic Interoperability
- ◉ User Interoperability

Which method is used for generating unique device addresses in IoT Application?

- ○ a. Electronic Product Codes (EPC)
- ○ b. Universal Product Code (UPC)
- ○ c. Uniform Resource Identifier (URI)
- ○ d. IP Addresses (IPv6)
- ○ c and d
- ◉ All
- ○ a and d

Interoperability challenges include

- ○ Large Scale of Co-Operation and Global Heterogeneity
- ○ Unknown IoT Device Configuration and Semantic Conflicts
- ◉ All
- ○ None

This form was created inside of Indian Institute of Information Technology, Vadodara.

Google Forms

IoT communication Technologies

IoT communication Technologies

- List of common communication protocols in IoT.
- Identify the salient features and application scope of each communication protocol.
- Understand the terminologies and technologies associated with IoT communication.
- Determine the requirements associated with each of these communication protocols in real-world solutions.
- Determine the most appropriate communication protocol for their IoT implementation.

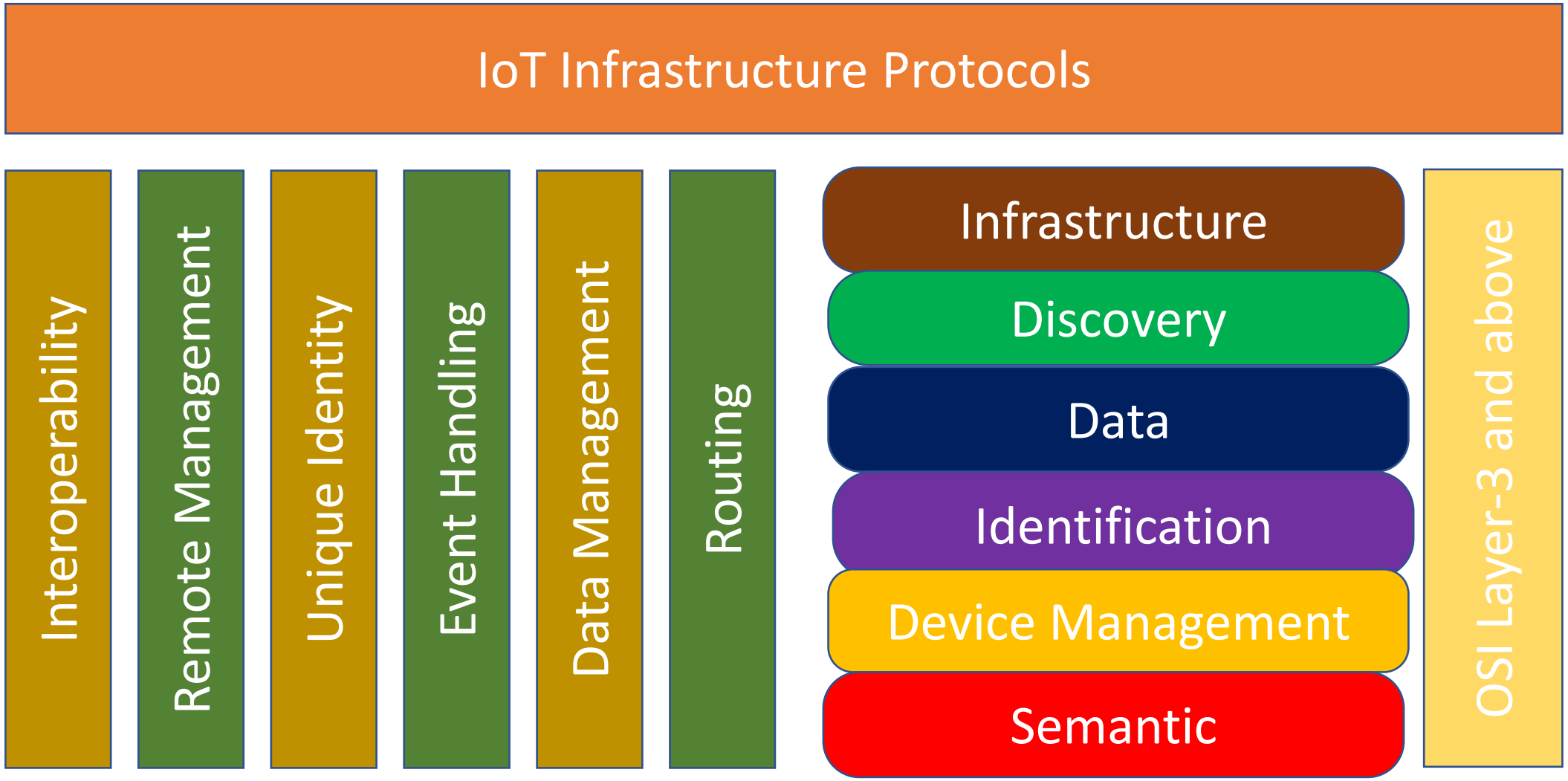
IoT communication Technologies

- According to the usage, the IoT communication protocols are divided into six groups.

- They are

  - ✓Infrastructure Protocols
  - ✓Discovery Protocols
  - ✓Data Protocols
  - ✓Identification Protocols
  - ✓Device Management Protocols
  - ✓Semantic Protocols

IoT communication Protocol Groups



IoT communication Technologies

Constraint Nodes

- Nodes having no Internet communicating devices.
- Applications having constraints of costs, size restriction, weight restriction, available power for the functioning of those nodes.
- Memory and processing power restriction.
- Lacks full connectivity features and broadcasting capability.
- Needs special design consideration.

IoT communication Technologies

Constraint Network

- Limited processing power resulting in restrictions on achieving smaller duty cycle.
- Low data rate and low throughput
- Asymmetric links and increased packet losses
- Lack of advance layer three functions such as multicasting and broadcasting
- Limited temporal device reachability from outside the network due to the inclusion of sleep states for power management in the devices.

IoT communication Technologies

Types of constraint devices

According to device functionalities, the constraint devices are divided into three classes.

- ✓Class 0
- ✓Class 1
- ✓Class 2

IoT communication Technologies

Class 0:

- These devices have resources and capability constraints.
- Barely feasible memory and processing available.
- Do not allow direct communication to the Internet.
- If the device manages to communicate to the Internet directly, then device's reduced capability constraint does not support to ensure security.
- This class of devices communicate to the Internet through Gateway or Proxy.

IoT communication Technologies

Class 1:

- This Class of devices have constraint on available code space and processing power.
- This can communicate to the Internet but can not employ a regular full protocol stack (ex:HTTP).
- Specially designed protocol stack (ex:CoAP) can be used to enable Internet based communication with other nodes.
- This class of devices does not need a gateway for accessing the Internet.
- It has security features which ensures safer communication over the Internet.
- These device has higher power budget compared to class 0 devices.

IoT communication Technologies

Class 2:

- It’s functionality is same as portable computers such as laptops and PDAs (Personal Digital Assistants).
- They have ability and capacity to support full protocol stack (ex: HTTP,TLS).
- These device has higher power budget compared to class 1 devices.

IoT communication Technologies

Low Power and Lossy networks (LLNs):

- Nodes or devices having limited power, small usable memory space, limited available processing resources.
- The network links between devices may be composed of low power Wi-Fi or IEEE 802.15.4
- The physical layer of the devices are characterized by delivery rate, packet loss.
- Application Areas:
    - ✓ Industrial automation and monitoring
    - ✓ Building automation
    - ✓ Smart health care
    - ✓ Smart homes
    - ✓ Logistics
    - ✓ Environment monitoring
    - ✓ Energy Management

Infrastructure Protocols

Infrastructure Protocols

- It depends on the network and the network infrastructure for its operation.

- It includes

  - ✓Internet Protocol version 6 (IPv6)
  - ✓Lightweight On-demand Ad hoc Distance vector Routing Protocol-Next Generation (LOADng)
  - ✓Routing Protocol for Low Power and Lossy Networks (RPL)
  - ✓IPv6 over Low-Power Wireless Personal Area Networks (6LoWPAN)
  - ✓Quick UDP Internet Connection (QUIC)
  - ✓Micro IP (uIP)
  - ✓nanoIP
  - ✓Content centric Networking

Internet Protocol version 6 (IPv6)

Internet Protocol version 6 (IPv6)

Introduction

- IPv6 is developed as an extension to IPv4 to increase the address ranges used in networking protocols.
- IP Version 6 was developed by IETF (Internet Engineering Task Force).
- It is also known as Internet version 2.
- It works at the network layer (layer 3) in OSI model same as the IPv4.

Internet Protocol version 6 (IPv6)

Introduction

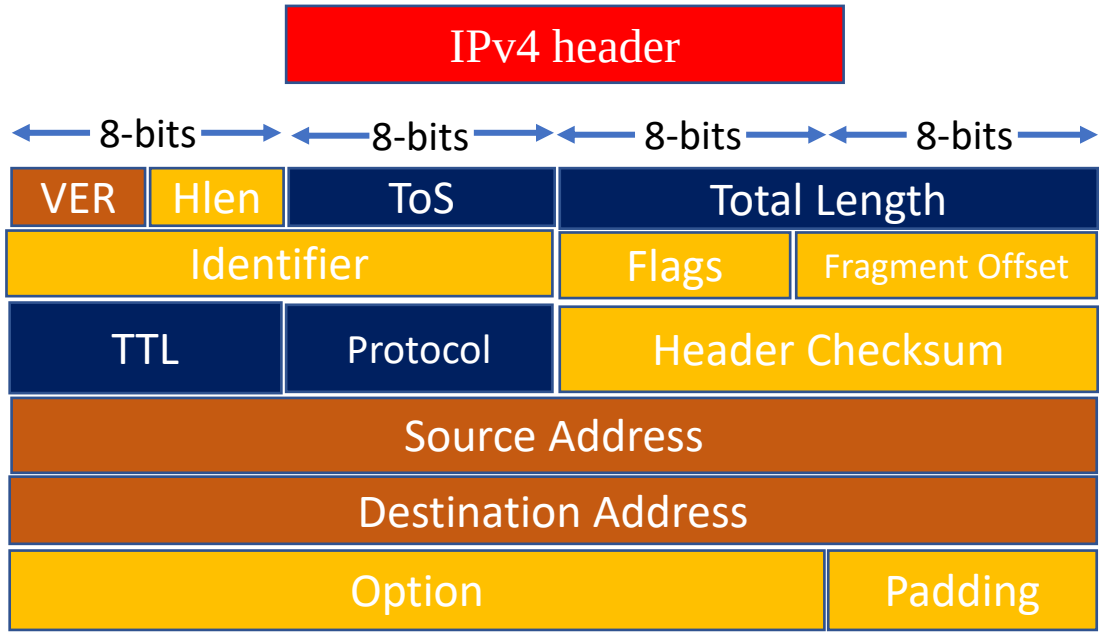
- IPv6 is enhanced protocol and is designed for a large range of addresses (typically 128 bits long) in contrast to IPv4 (32 bit length addresses).

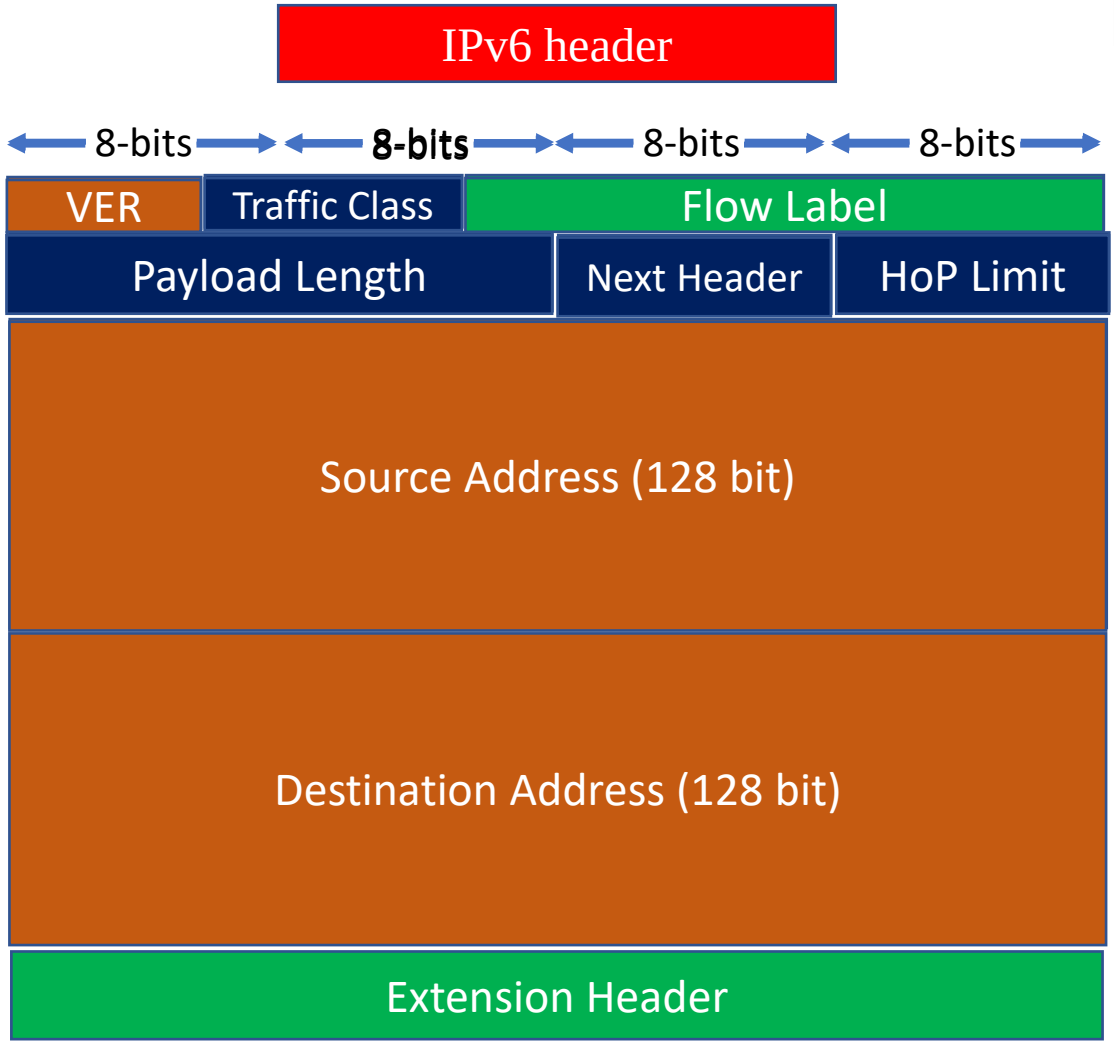
- Features:
  1. Auto-configuration
  2. End-to-end connectivity
  3. In-built security (Ipsec)
  4. Provision for fast routing capability
  5. Support for mobility

- Above features helps to deploy IPv6 practically in IoT.

- Ipv6 supports no backward compatibility as it designed completely from scratch; we cannot make IPv6 to support IPv4 applications directly.

Differences between IPv4 and IPv6 packets





Features of IPv6

1. Larger addressing range
2. Simplified header structure
3. End-to-End Connectivity
4. Auto Configuration
5. Faster Packet Forwarding
6. In-built Security
7. Anycast Support
8. Mobility Support
9. Enhanced Priority Support
10. Extensibility of Headers

Features of IPv6

1. larger addressing range

- IPv6 has roughly four times more addressable bits than IPv4.

- The magnanimous range of addresses can accommodate the address requirements for any number of connected or massively networked devices in the world.

Features of IPv6

2. Simplified header structure

- The header format of IPv6 is much simpler than IPv4.
- Header size of IPv6 is much bigger than IPv4.
- Increased size of IPv6 header is mainly attributed to the increased number of bits needed for addressing purpose.4

Features of IPv6

3. End-to-End Connectivity

- It allows for globally unique addresses on a massive scale.

- This addressing enables packets from a source node to directly reach the destination node without the need for network address translation in the route.

Features of IPv6

4. Auto-configuration

- The address configuration is done automatically in IPv6.
- It supports both stateless and stateful auto-configuration methods.
- This protocol works in the absence of DHCP (dynamic host configuration protocol) servers

Features of IPv6

5. Faster Packet Forwarding

- IPv6 header have all seldom-used optional fields at the end of its packet.
- The routing decisions are taken faster by the router by checking only starting few fields of the header.

Features of IPv6

6. In-built Security

- IPv6 supports inbuilt security mechanisms (IPSec) that IPv4 does not have.
- IPv4 security measures are attained using separate mechanisms
- The present day version of IPv6 has security as an optional feature.

Features of IPv6

7. Anycast Support

- Multiple networking interfaces are assigned the same IPv6 addresses globally are known as anycast addresses.

- This enables routers to send packets to the nearest available 3destination during routing.

Features of IPv6

8. Mobility Support

- It is an essential, crucial feature for IoT and modern day connected applications.
- It allows for mobile nodes to retain their IP addresses and remain connected even while changing geographic areas of operation.

Features of IPv6

9. Enhanced Priority Support

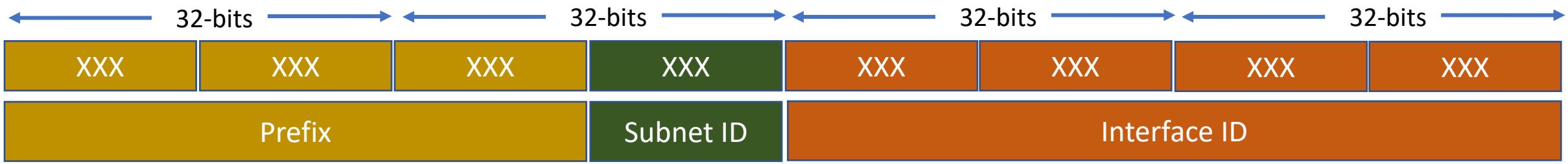
- Priority support system is simplified as compared to IPv4.
- The use of traffic classes and flow labels determine the most efficient routing paths of packets for the routers.

Features of IPv6

10. Extensibility of Headers

- IPv6 has options part in its header.
- This can be extended by adding more information to it.
- it is not limited in size.
- Some applications may require a larger option fields which may comparable to the size of the packet.

IPv6 Address Notation



Example:

IPv6 address :- 1034:7B6F:1345:4E44:1234:AAAA:5B78:3421

Global prefix:-1034:7B6F:1345
Subnet:-4E44
Interface identifiers:-1234:AAAA:5B78:3421

IPv6 Addressing

- IID (Interface Identifier) is a crucial part of IPv6.
- It is 64-bit length which occupies last 4 blocks of IPv6 Address.
- IID are generated from the device MAC addresses which make it globally unique.
- IID is auto configured by a host using IEEE extended unique identifier (EUI-64) format.

IPv6 Addressing

IPv6 has *three* types of unicasting:

a. Global Unicast Address (GUA)

b. Link Local Address (LL)

c. Unique Local address (ULA)

IPv6 Addressing

Global Unicast Address (GUA)

- GUA (IPv6) is synonymous with IPv4's static addresses (Public IP).
- It is *globally* identifiable and *uniquely* addressable.
- The first (most significant) 48-bits (MSBs) are for global routing prefix.
- The first 3 bits of this routing prefix is always set to *001*. This is most significant bits of the prefix.

IPv6 Addressing

Link Local Address (LLs)

- LLs are auto-configured IPv6 addresses.
- Its communication is limited to network segment (within a gateway or a router).
- The first 16-bits of LL addresses are fixed (FE80 in hex).
- The subsequent 48-bits are all set to Zeroes.
- The addresses are non-routable making LL to work within a router or a gateway.

IPv6 Addressing

Unique Local address (ULA)

- ULAs are locally global and unique.
- They work within local networks only.
- Packets from ULAs are not routed to the Internet.
- The first half of ULA is divided into 4 parts and last half is considered as a whole.
- The 4 parts of first half are : Prefix, local-bit, global ID & subnet ID
- The last half contains the IID.
- ULA's prefix is always assigned as FD in hexadecimal and (1111 1101) binary.
- If least significant bit in the prefix is 1then it is locally assigned addresses.

IPv6 Address Assignment

- Any node in IPv6 network is capable of auto-configuring its unique LL address.
- This helps node to become a part of many multicast groups responsible for communication within that segment of the network.
- The node then sends a neighbor solicitation message to all its IPv6 addresses.
- If node receives no response it assumes that no duplicate addresses are available in the network segment and the address is locally unique.
- This is known as duplicate address detection (DAD) in IPv6.
- The node then configures the IPv6 address to all its interfaces & sends out neighbor advertisement informing its neighboring nodes about the address assignment of its interfaces
- This marks the completion of IPv6 address assignment of a node

IPv6 Communication

Step-1

- The IPv6 configured node sends a router solicitation message (essentially a multicast pac its network segment. This helps the node to determine the presence of any routers in its network segment or path.

Step-2

- Upon receiving the solicitation message, a router responds to the node by advertising its presence on that link.

Step-3

- Once path is discovered, the router is set as that nodes default gateway. If selected gateway is unavailable, a new gateway is selected using same discussed procedure.

Step-4

- If a router upon receiving the solicitation message determines that it may not be the best option for serving as the nodes gateway, the router sends a redirect message to the node informing it about the availability of a better router (which can act as a gateway) within its next hop.

IPv6 Mobility

- A mobile IPv6 node located within its home link uses its home addresses for routing all communication to it.
- When a mobile IPv6 node is beyond its home link, the communication is established through foreign link.
- A new IPv6 address is then acquired from the foreign link, known as mobile node's care-of-address (*CoA*)
- The mobile node now binds its CoA to its home agent (a Router/Gateway to which the node was registered in its home agent)
- This binding between the CoA and home agent is done by establishing a tunnel between them.

IPv6 Mobility

- Whenever a node's home agent receives a corresponding messages, it is forwarded to the Mobile node's CoA over the established tunnel between CoA and home agent

- Upon receiving message from corresponding node; the mobile node may choose not to reply through its home agent

- It can communicate directly to the corresponding node by setting its home address in the packet source address field (mechanism known as *route optimization*)

LOADng

LOADng

- LOADng is Lightweight On-demand Ad hoc Distance vector Routing Protocol-Next Generation.

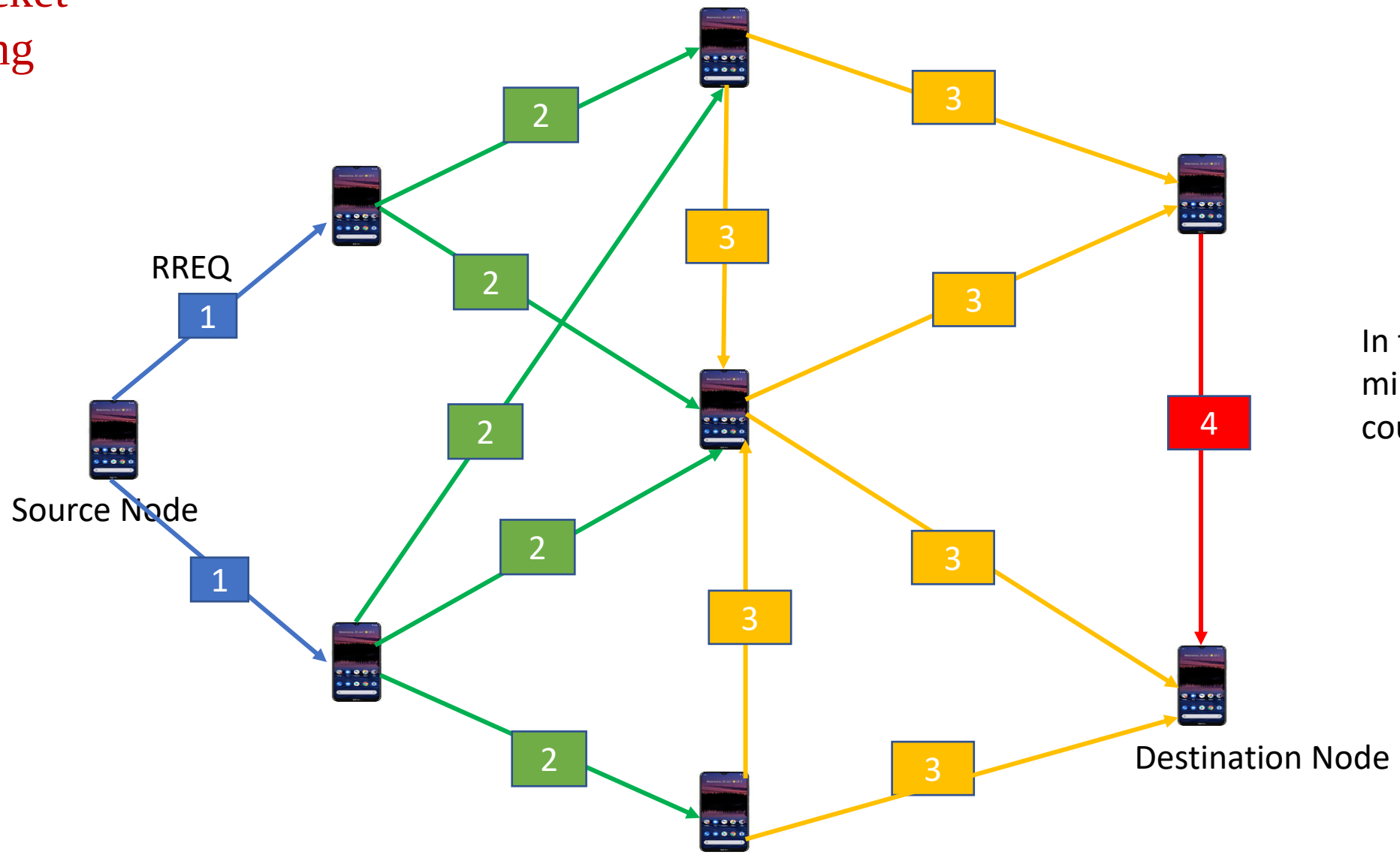
- Derived from AODV (Ad hoc On-demand Distance vector Routing Protocol) and extended for use in IoT.

- It is a *reactive* protocol.

- Basic operations of LOADng include:
  - ✓ Generation of **Route Requests (RREQs)** by a LOADng Router (originator) for discovering a route to a destination.
  - ✓ **Forwarding of such RREQs** until they reach the destination LOADng Router.
  - ✓ Generation of **Route Replies (RREPs)** upon receipt of an RREQ by the indicated destination, and unicast hop-by-hop forwarding of these RREPs towards the originator.

LOADng

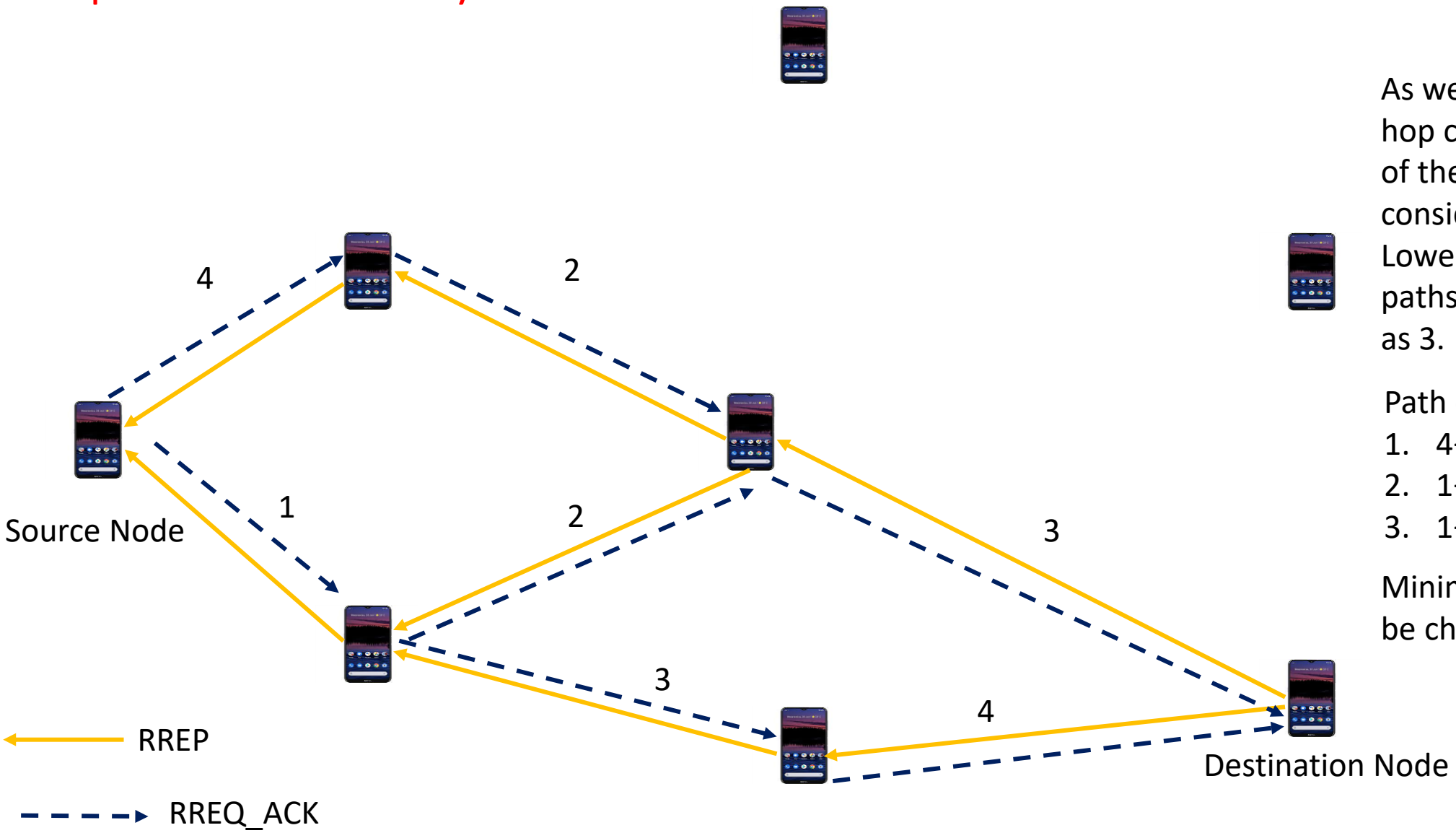
Step-1. Flooding based packet forwarding



In this figure minimum hop count is 3.

LOADng

Step-2 Route Discovery



As we choose minimum hop count so, lower part of the network is considered.
Lower part have three paths having hop count as 3.

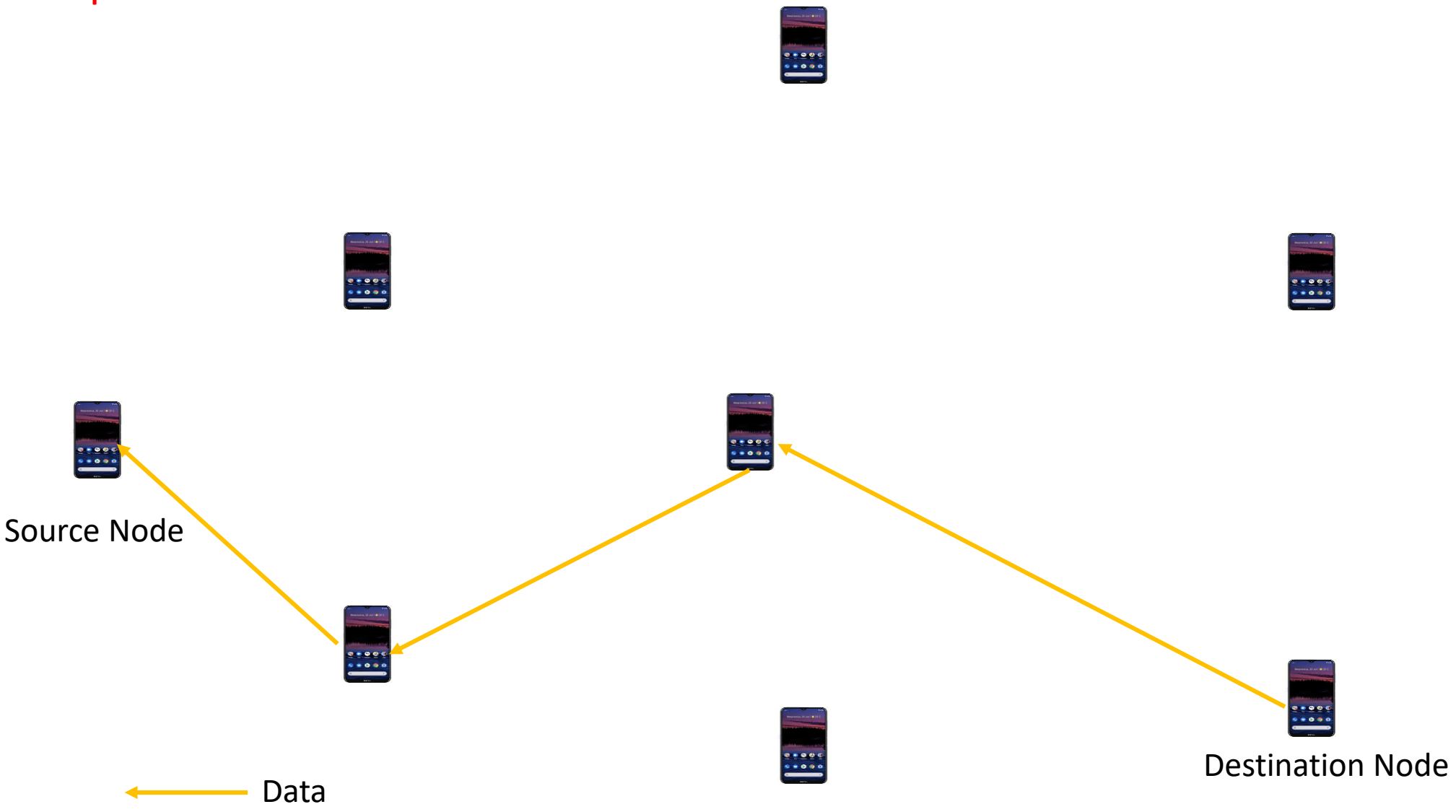
Path cost

1. 4+2+3=9
2. 1+2+3=6
3. 1+3+4=8

Minimum cost path will be chosen as Final path.

LOADng

Step-3 Route Establishment



LOADng

Step-1

- Source Node (S) sends Rreq packet to its neighboring nodes (I1, I2) by mentioning the hop count as 1.
- The intermediate node forwards the packets to their neighbors by increasing one to the hop count.
- This procedure follows till the Rreq packet reaches the Destination.

Step-2

- Choose the minimum hop count path and discards all other paths.

Step-3

- If more than one path have same hop count (minimum value) then calculate communication cost of each of the path.
- Minimum total cost path will be chosen as the final low cost path between source to destination on which data is forwarded.

LOADng

- If a route is detected to be broken, a **Route Error (RERR)** message is returned to the originator of that data packet to inform the originator about the route breakage.

- **Optimized flooding** is supported, reducing the overhead incurred by RREQ generation and flooding.

- Only the destination is permitted to respond to an RREQ.

- Intermediate LOADng Routers are explicitly prohibited from responding to RREQs, even if they may have active routes to the sought destination.

- RREQ/RREP messages generated by a given LOADng Router share a single unique, monotonically increasing sequence number.

RPL

RPL

- IPv6 routing protocol designed for low power and lossy network.
- It uses Destination oriented directed acyclic graph (DODAG).
- The network DODAG is formed based on an objective function and a set of network metrics.
- The DODAG is a logical routing topology built over the physical network.
- The logical topology is based on certain criteria set by the network administrators.
- The most optimum path is calculated from objective function, a set of metrics and constraints.

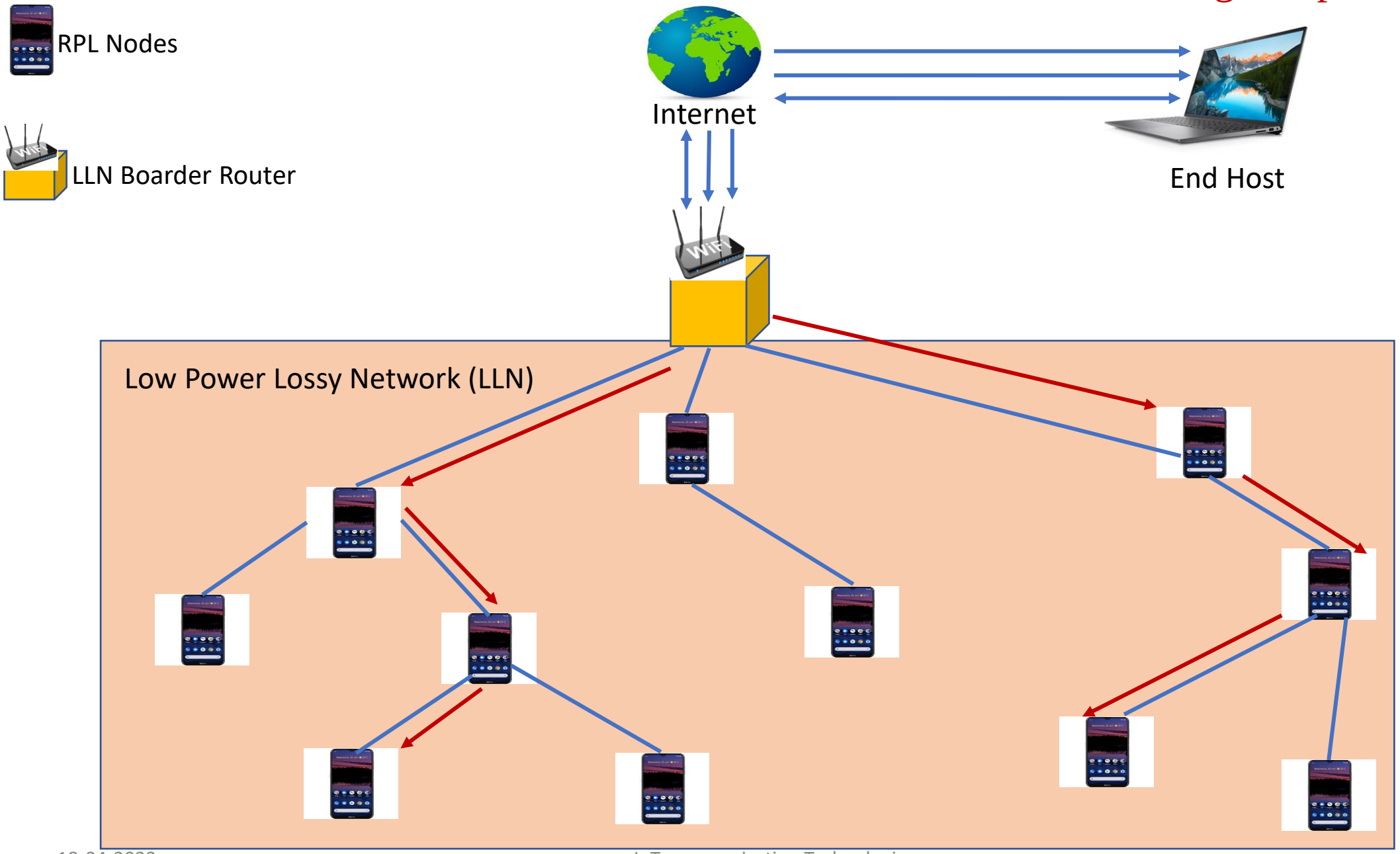
RPL

- A set of metrics include
  - ✓ transmission values
  - ✓ path latencies
- The constraints include
  - ✓ Encryption on links
  - ✓ presence of battery operated nodes
- The metrics are need to be minimized or maximized.
- The constraints need to be minimized.
- The objective function dictates the rules for the formation of the DODAG.

RPL

- A single node in mesh network may have multiple objective functions.
- The primary reason for this is attributed to the presence of different network traffic path quality requirements that needs separate addressal within the same mesh network.
- Using RPL, a node within a network can simultaneously join more than one RPL instance (graphs).
- This enables RPL to support QoS-aware and constraint based routing.
- An RPL node can take multiple network roles such as leaf node and router.
- The RPL node handles intra mesh addressing.

RPL information flow mechanism with different intra-mesh addressing and paths



RPL Instances

- It has two instances.
  - ✓ Global RPL instance
  - ✓ Local RPL instance

Global RPL instance

- It is characterized by coordinated behaviour and possibly the presence of multiple DODAG.
- It has long life time.

Local RPL instance

- It is characterized by single DODAGs.
- The local RPL DODAG's root is associated directly with DODAG-ID.
- The DODAG-ID is collaboratively and unilaterally allocated.
- The control and data messages are tagged with their corresponding RPL instances ID to avoid ambiguity in operations

6LoWPAN

6LowPAN

Introduction

- Low-power Wireless Personal Area Networks over IPv6.
- Allows for the smallest devices with limited processing ability to transmit information wirelessly using an Internet protocol.
- Allows low-power and constraint devices/nodes to connect to the Internet.
- Created by the Internet Engineering Task Force (IETF) - RFC 5933 and RFC 4919.
- It enables IPv6 support for WPANs which have limited concerning power, communication range, memory and throughput.
- It is designed to be operational and straightforward over low cost system and extend IPv6 networking capabilities to IEEE802.15.4-based networks.

6LowPAN

Features of 6LoWPANs

- Allows IEEE 802.15.4 radios to carry 128-bit addresses of Internet Protocol version 6 (IPv6).
- Header compression and address translation techniques allow the IEEE 802.15.4 radios to access the Internet.
- IPv6 packets compressed and reformatted to fit the IEEE 802.15.4 packet format.
- Uses include IoT, Smart grid, and M2M applications.

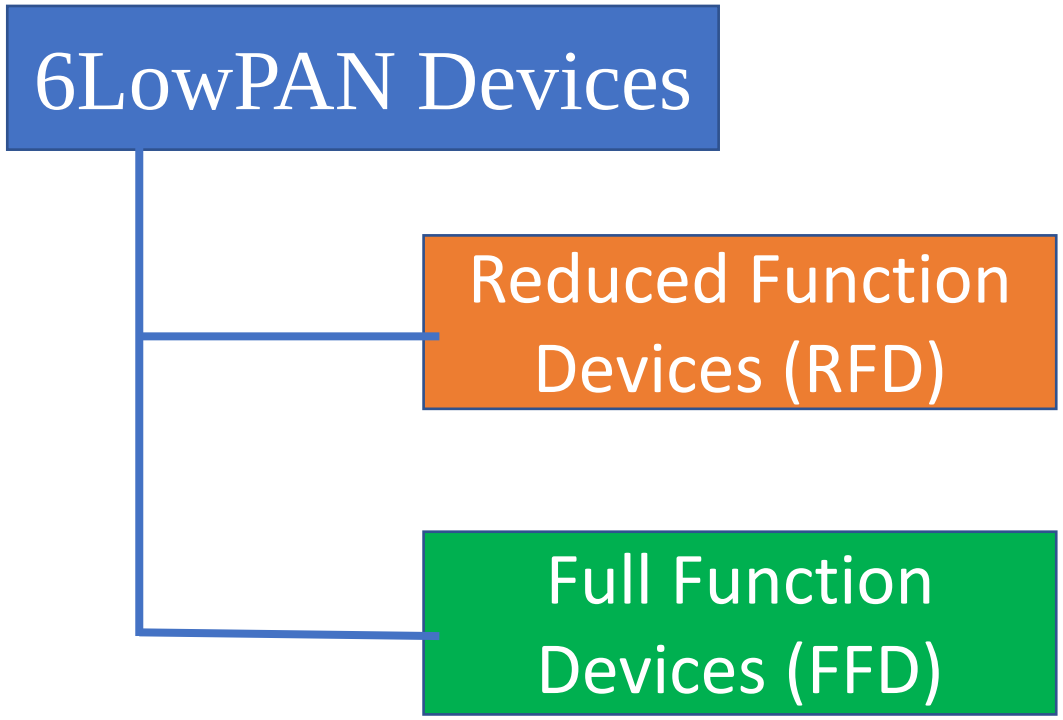
6LowPAN Devices

RFD

Limited capability devices (throughput, memory, communication range, processing)

FFD

Significantly better capability devices



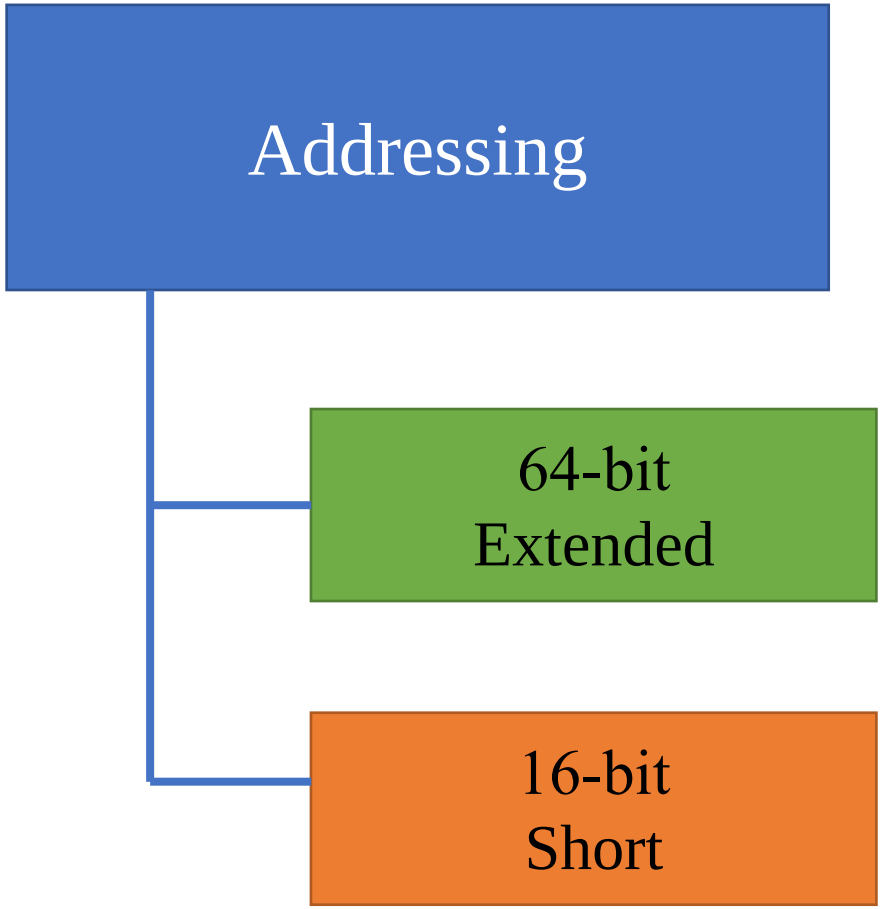
6LowPAN Devices

- For accessing IP based network, the RFD forward their data packets to FFD in their PANs.
- The FFD forward the received data from RRD to 6LowPAN gateway in a multi hop manner.
- The 6LowPAN gateway connect the packets to the IPv6 domain in communication network.
- Finally packet is forwards to the destination IP-enabled node/devices using regular IPv6 based networks.

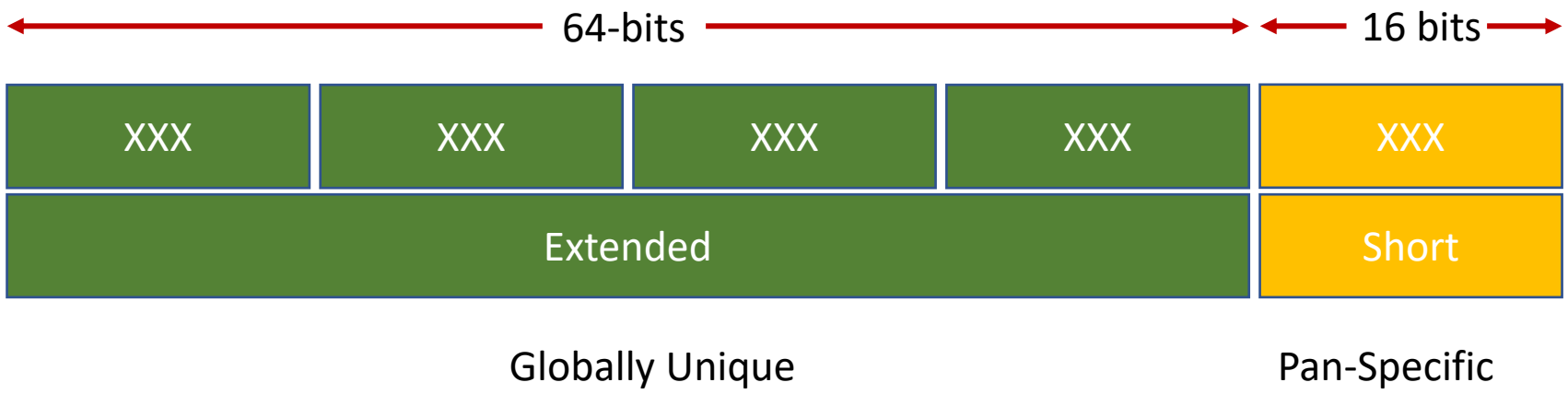
6LowPAN

Addressing in 6LoWPAN

- 64-bit addresses: globally unique and used to identify devices outside the PAN.
- 16 bit addresses: PAN specific; assigned by PAN coordinator and used for identifying devices within the PAN only. Its scope is restricted within the PAN only.
- IPv6 multicast not supported by 802.15.4
- IPv6 packets carried as link layer broadcast frames.



6LowPAN Address Format



6LowPAN Stack

1. PHY and MAC Layers

- It consists of 27 wireless channels.
- Each having separate frequency band and varying data rate.
- The MAC layer defines the means and methods of accessing the defined channels and use them for communication.

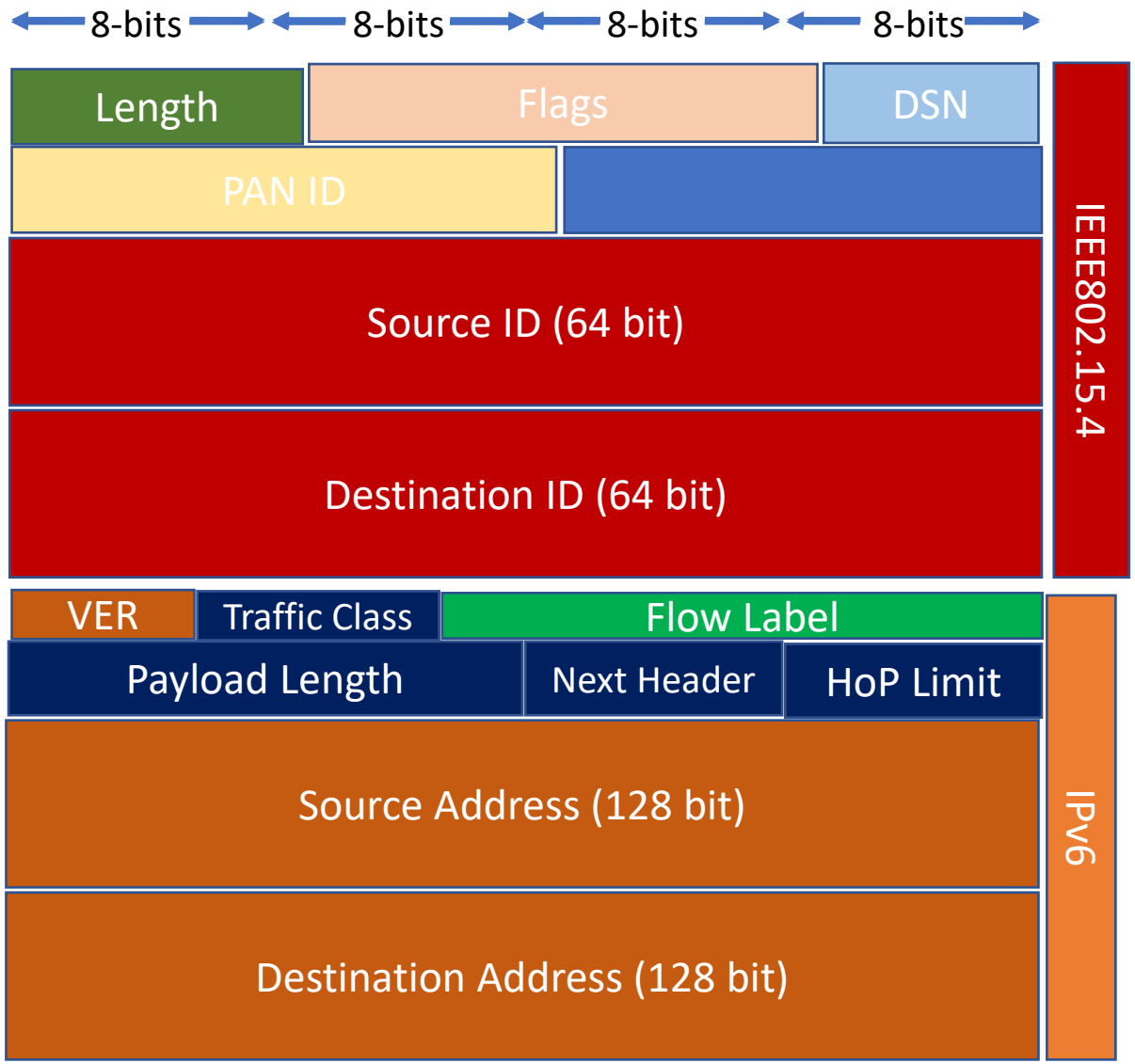
- MAC layer is characterized by
  - ✓Beaconing tasks for device identification. The task includes both beacon generation and beacon synchronization.
  - ✓Channel access control is provided by CSMA/CA.
  - ✓PAN membership control functions. PAN membership includes both association and disassociation tasks.

6LowPAN Stack

2. Adaptation Layer

- 6LowPAN accommodate and retro-fits the IPv6 packets to IEEE 802.15.4 packet format.
- IPv6 packets require 1280 octets for transmission and IEEE802.15.4 requires 1016 octets (25 octets for frame overheads and 102 octets for payload).
- Security in IEEE 802.15.4 frame leaves 81 octets for IPv6 packets (40 octets for itself + 8 octets for UDP + 20 octets for TCP + 13 octets for data).
- 6LowPAN adaptation layer takes care of these issues through the use of header compression, packet forwarding and packet fragmentation.
- 6LowPAN adaptation layer present between the MAC and Network layer.

6LowPAN Packet Format



6LowPAN Header Format

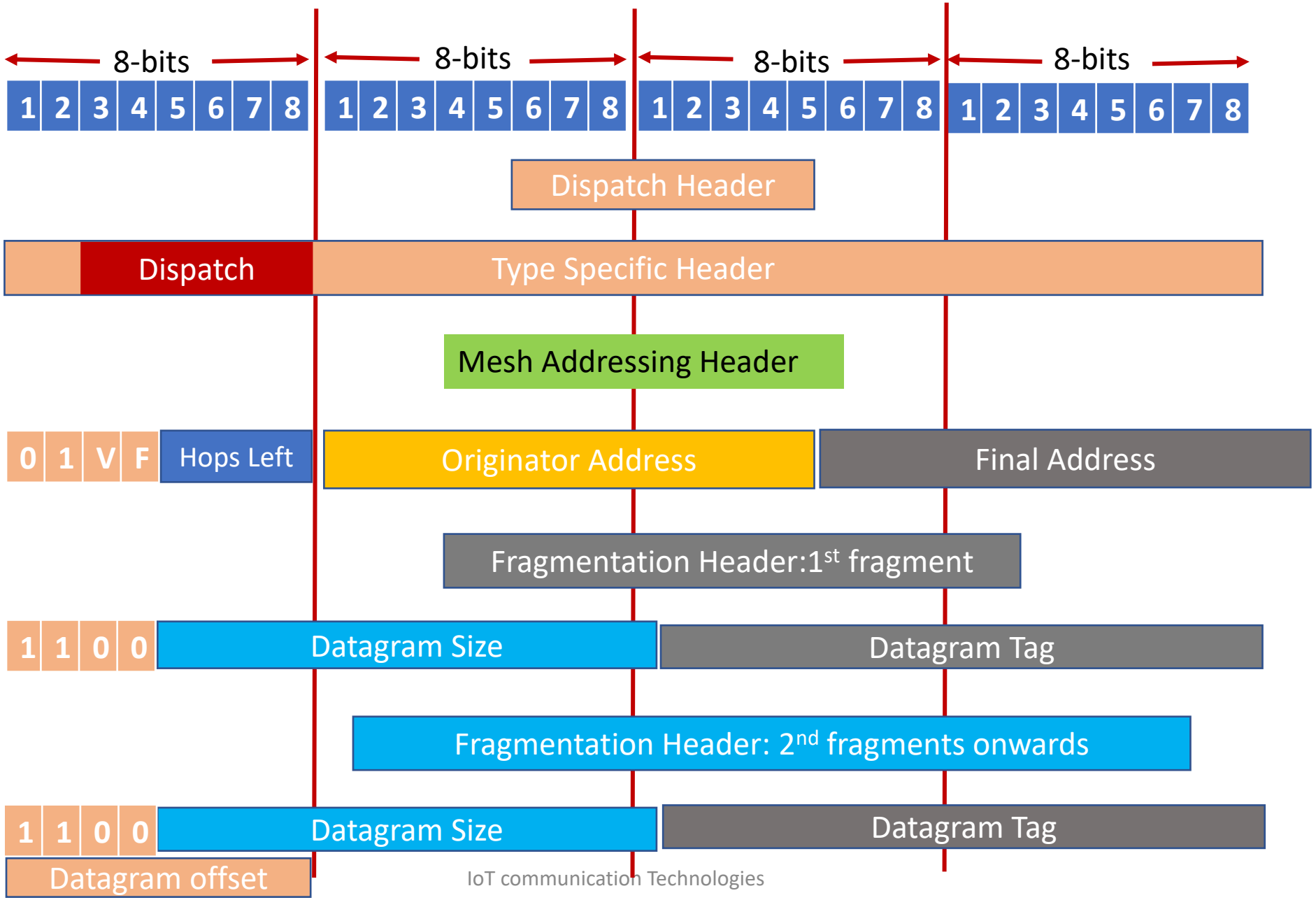
- 6LowPAN encapsulates the IPv6 payloads within IEEE 802.15.4 frame.

- 6LowPAN has three encapsulated header types.
  - ✓Dispatch
  - ✓Mesh Addressing
  - ✓Fragmentation

- The headers are identified by header types field placed at the front of the header.

- Dispatch header is used to initiate communication between a node and destination node.
- Mesh addressing header is used for multi-hop forwarding by providing support for the layer to forwarding of messages.
- Fragmentation header is used to fit large payloads to IEEE 802.15.4 frame size.

6LowPAN header structures



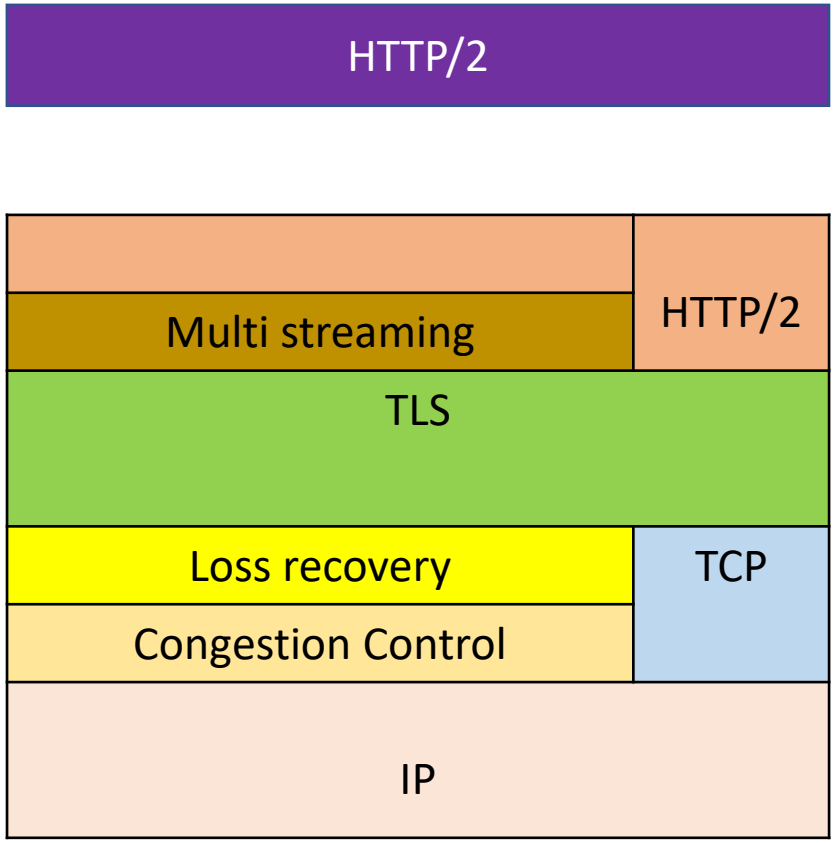
QUIC

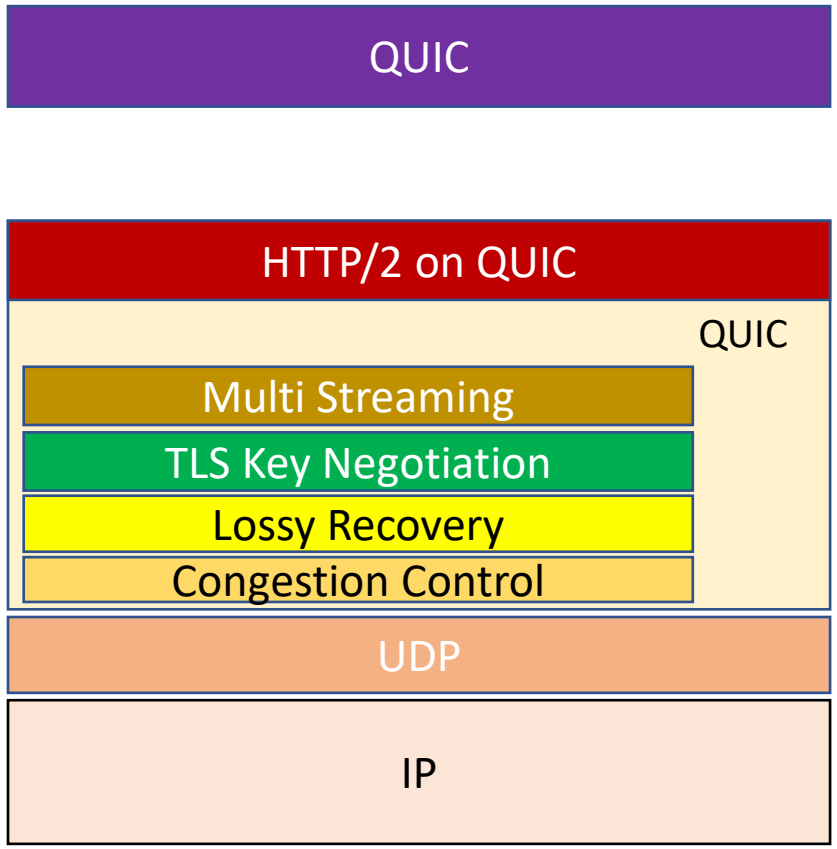
QUIC

Introduction

- Quick UDP Internet Connection
- A low latency and independent TCP connection.
- Aim of this protocol is to achieve highly reduced latency communication scheme with stream and multiplexing support.
- It is similar to SPDY protocol developed by Google.

Differences between HTTP and QUIC Protocol





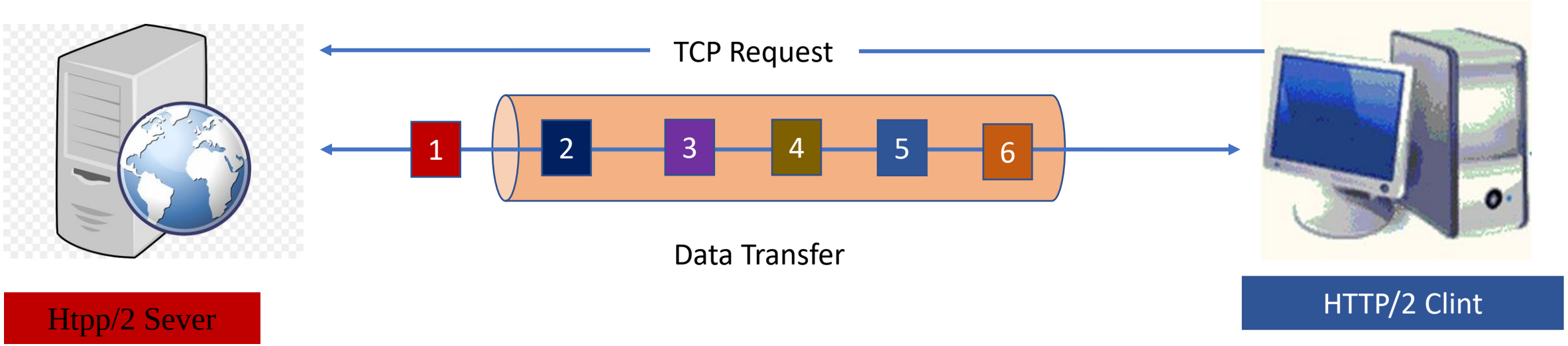
QUIC

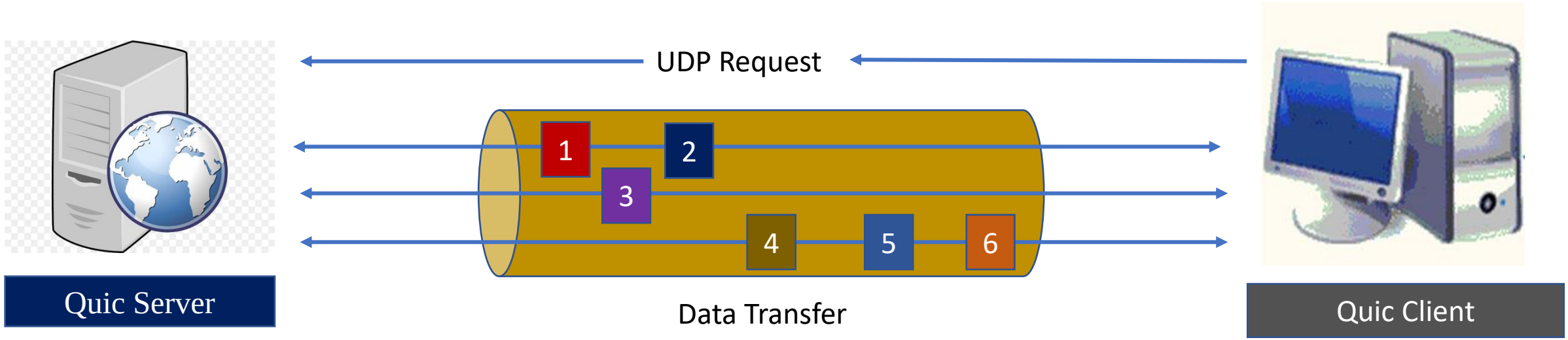
- The connection latency in QUIC is reduced by reducing the number of round trips incurred during connection establishment in TCP, such as handshaking, data request, encryption exchanges.
- This is achieved by including session negotiation information in the initial packet.
- The QUIC server can enhances the compression by publishing a static configuration record corresponding to the connections.
- Client synchronization connection information through cookies received from QUIC server.

QUIC

- To avoid congestion, QUIC uses packet pacing and proactive speculative retransmission.
- Proactive speculative retransmission sends copies of most essential packets which contain the initial negotiation for encryption and error correction.
- Speed up is achieved using compression of data such as header which is redundant and repetitive.
- This enables QUIC connection to make multiple secured request within a single congestion window which is not possible in TCP.
- The use of UDP and multiple transmission paths speed up the performance of streaming over QUIC as compared to HTTP based packet streaming.

Differences between stream of packets over HTTP and QUIC Protocols





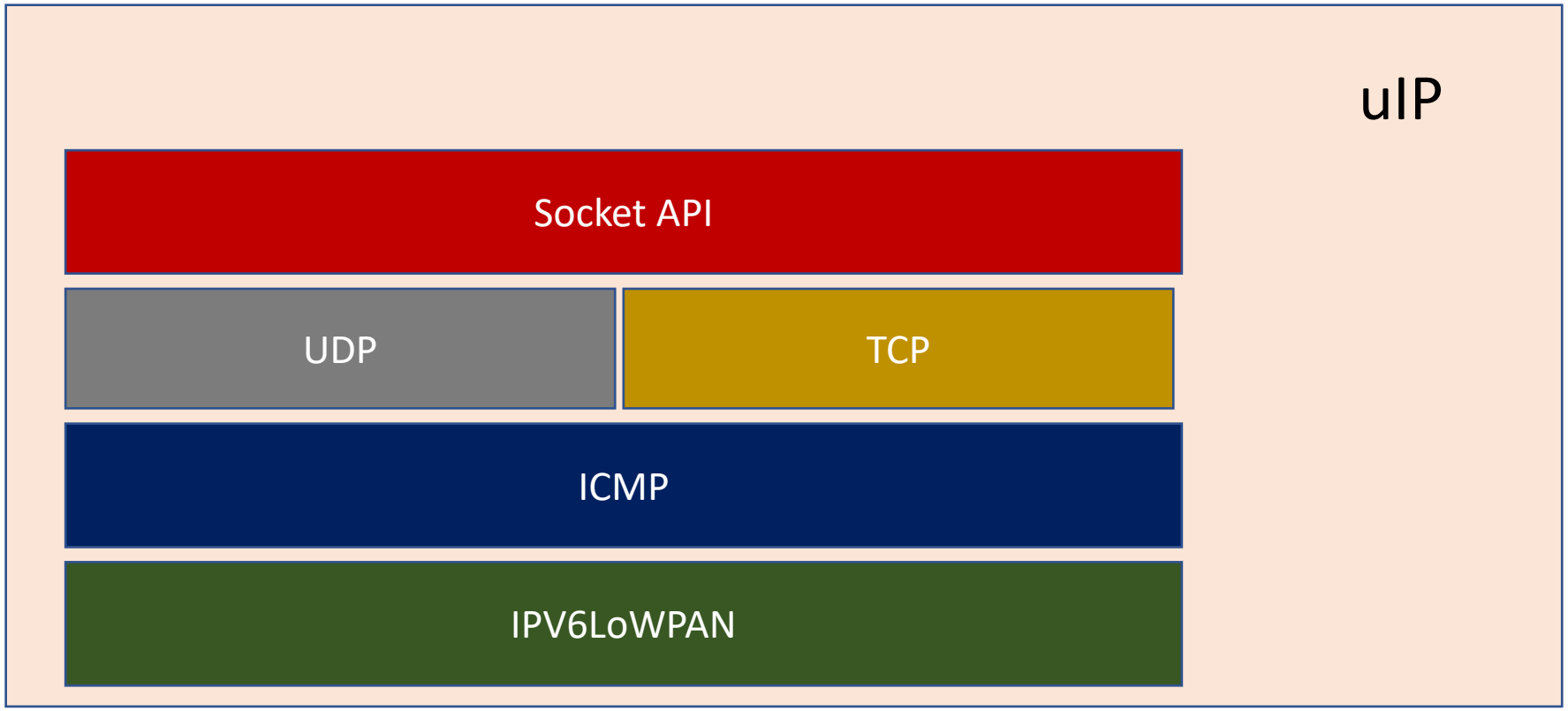
Micro Internet Protocol (uIP)

Micro Internet Protocol (uIP)

Introduction

- Micro IP is developed to extend the TCP/IP protocol stack capabilities to 8-bit and 16-bit microcontrollers.
- It is a open source protocol developed by Swidesh Institute of Computer Science (SICS).
- The low code space and memory requirement make it significantly useful for networking low-cost and low-power embedded system.
- It follows full IPv6 stack which is developed by Atmel, Cisco, SICS.

The uIP Protocol



Micro Internet Protocol (uIP)

Features

1. The software interface of uIP does not require any operating system for working which make it quite easy to integrate with small computers.

2. When called in a timed loop within the embedded system it also manages all the network behavior and connection retries.

3. The hardware driver for uIP is responsible for packet builds, packet sending, and response reception for packet send.

4. It uses a minimal packet buffer which makes suitable for low power operations.

Micro Internet Protocol (uIP)

Features

5. Packet buffer is used in half duplex manner so that the same buffer can be used for both transmission and reception.

6. It does not store data in the buffer, incase if required for retransmission. If retransmission required then packet is reproduced and recalled from the application code.

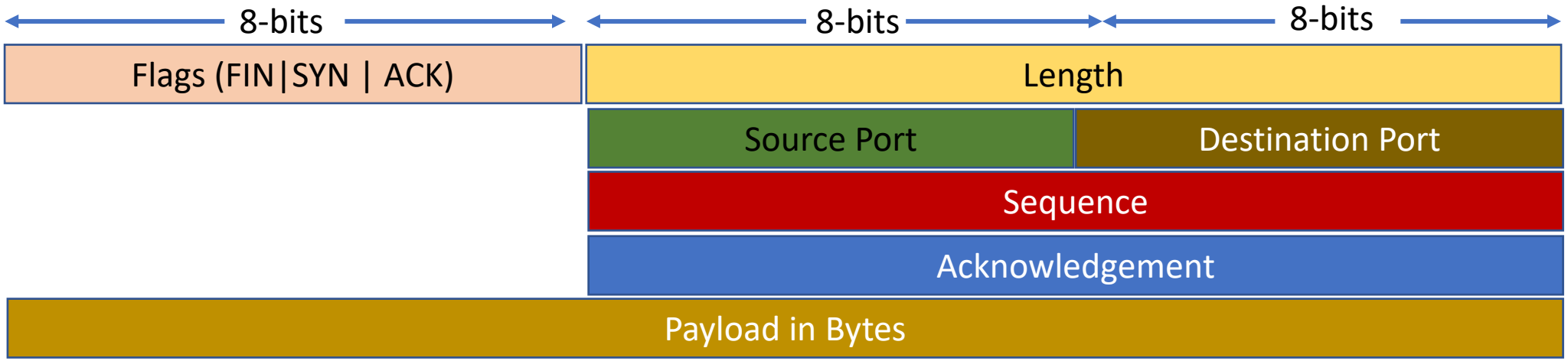
7. It stores connection in an array and serves each connection sequentially through subroutine calls to the application for sending data.

Nano Internet Protocol (nanoIP)

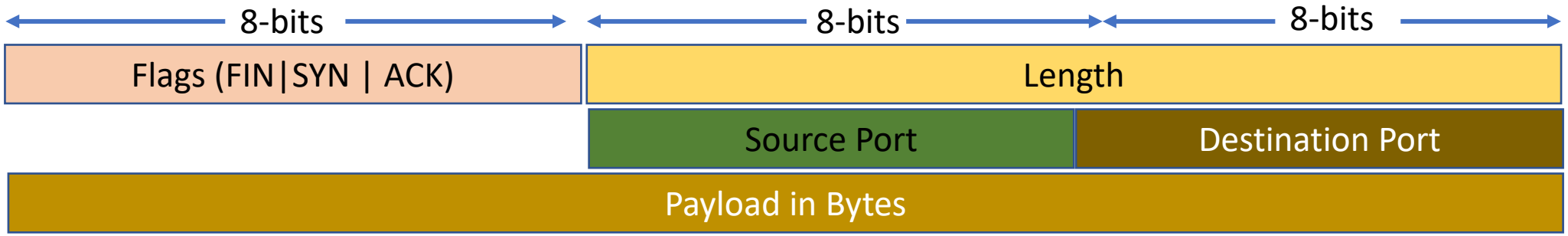
Nano Internet Protocol (nanoIP)

- It is used to work with embedded devices, sensor devices by enabling Internetworking among these devices.
- It enables wireless networking among low-power sensor devices.
- It uses nono-TCP and nano-UDP transport mechanisms.
- It is analogous to TCP and UDP.
- Nano TCP uses packet retransmission, flow control.
- It uses hardware addresses of devices for networking.
- It supports 256 port range for source and destination nodes which requires 8-bit port representation.
- It supports nPing and nHTTP.

The Nano-IP TCP Protocol



The Nano-IP UDP Protocol

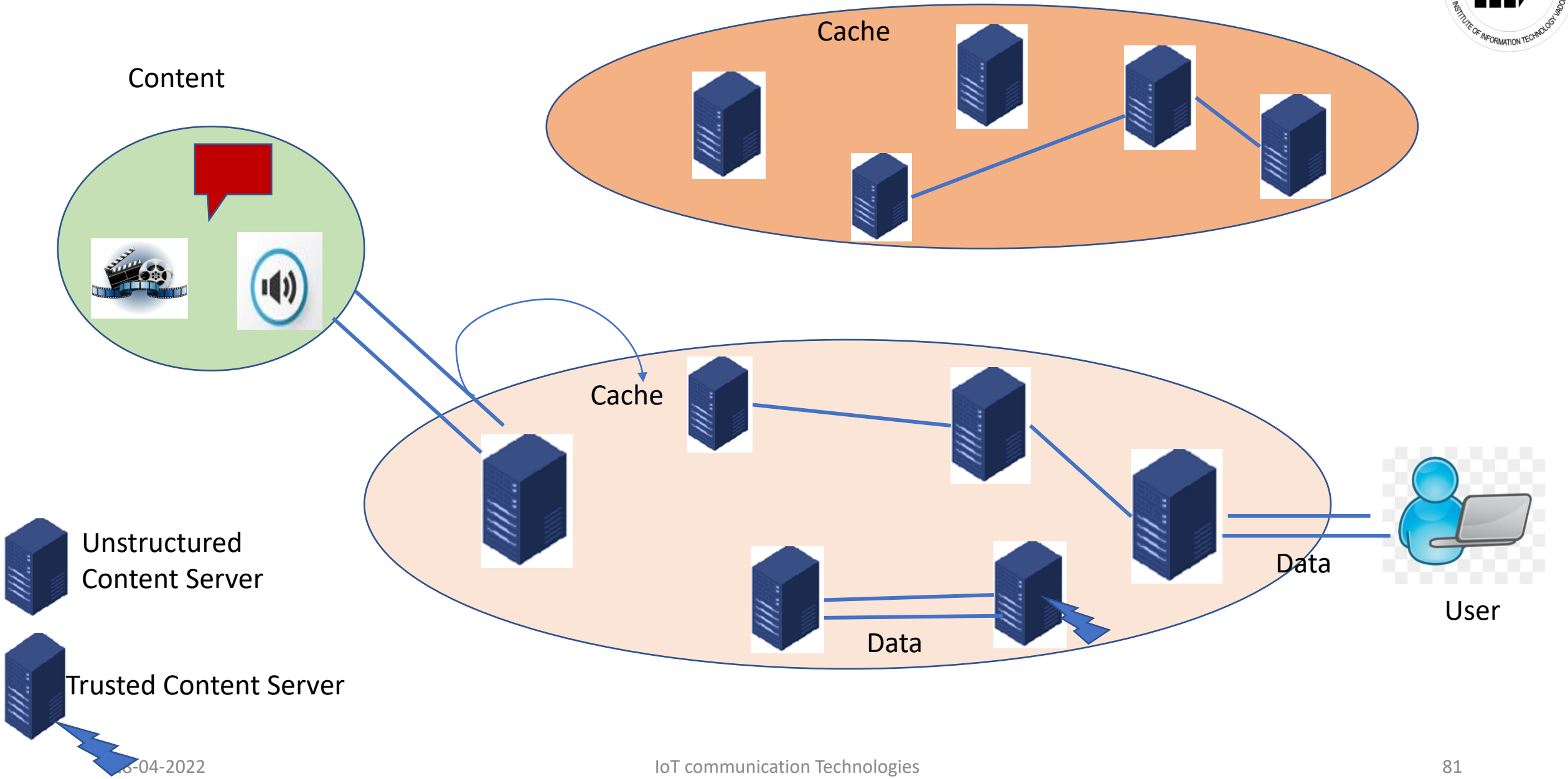


Content-centric Networking (CCN)

Content-Centric Networking (CCN)

- It is also known as information-centric networking (ICN), named data networking (NDN), Publish-subscribe networking (PSN).
- It is independent of location, application, and storage requirements.
- It is anchorless which enables mobility and focuses on in-network caching for operations.
- This measures extend the feature of data and communication efficiency, enhances scalability, robustness, even in constrained and challenged networks.
- Users can access cached content from multiple content generating sources by accessing data from trusted content servers, which enables security of the data.

Content Centric networking operation and its scope



Content-centric Networking (CCN)

- In CCN, a forwarder checks a named request through hierarchical prefix matching with a forwarding information base (FIB).
- A binary comparison is performed for prefix matching.
- The CCN request is a hierarchical sequence of network path segments.
- The FIB matching is then used to forward the named request to the appropriate network or network segment which can respond to the issued request.
- The forwarder has to additionally determine the reverse path from the responder to the requester.

Content-centric Networking (CCN)

- All these operations are carried out without specifically binding a request to a network end point.
- The FIB at each CCN router stores information in a table which is updated by a routing mechanism.
- The path segments and names are theoretically unbounded, they are restricted by the routing protocol being used for practical reasons.

Discovery Protocols

Discovery Protocols

List of discovery protocols include

- Physical web
- mDNS
- Universal plug and play (UPnP)

Discovery Protocols

Physical Web

- The seamless integration of several standalone smart systems through the web to provide information on demand to its users.

- Example:

- User friendly buses which provides its users about the route related information.
- Smart home appliances that can teach new users how to use them.
- Self diagnostic robots and machinery in Industries.
- Smart Pet tags which can provide information about pet's owner and home location.

Discovery Protocols

- Physical Web

- The physical web broadcast a list of URLs within a short radius around it so that anyone in range can see the available URLs and interact with them.

- This paradigm is built upon the Bluetooth low energy (BLE), which is used to broadcast the content as beacons.

- The primary requirement of beacons to function in the physical web and broadcast URLs is their ability to support the Eddystone protocol specification.

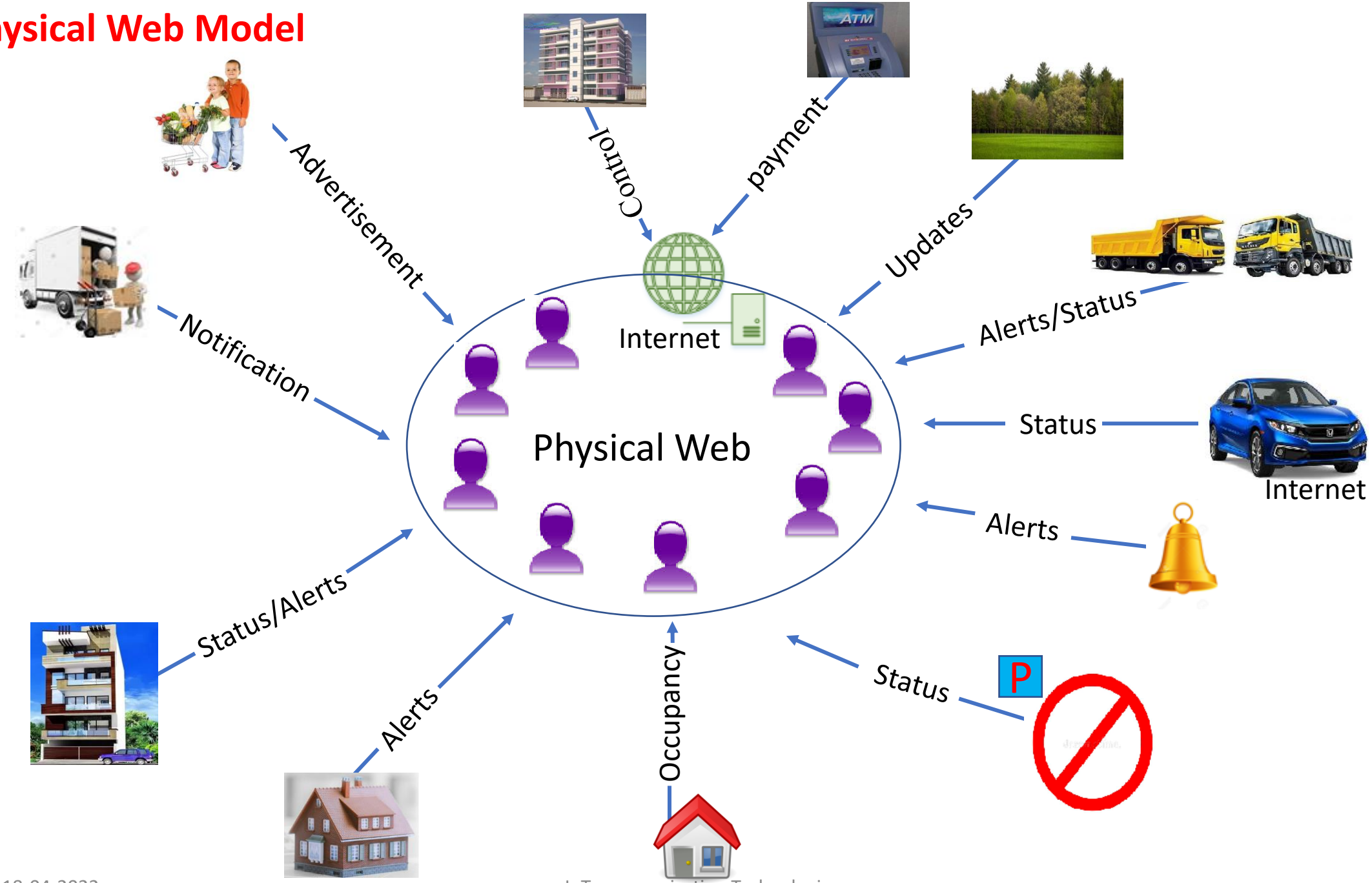
- BLE was chosen for physical web due to its ubiquity, efficiency, and extended battery life of several years.

Discovery Protocols

Physical Web

- URLs are the core principle of the web.
- It is flexible or decentralized concept.
- It allows any applications to have a presence on the web.
- It enables the digital presence of an object or thing.
- Deployment of physical web is done in public place and any device with a physical web scanner can detect these URLs.
- The URLs extends the benefits of web security model in physical web.
- Secured login, secure communication over HTTPs, domain obfuscation features are easily integrated in physical web.

The Physical Web Model



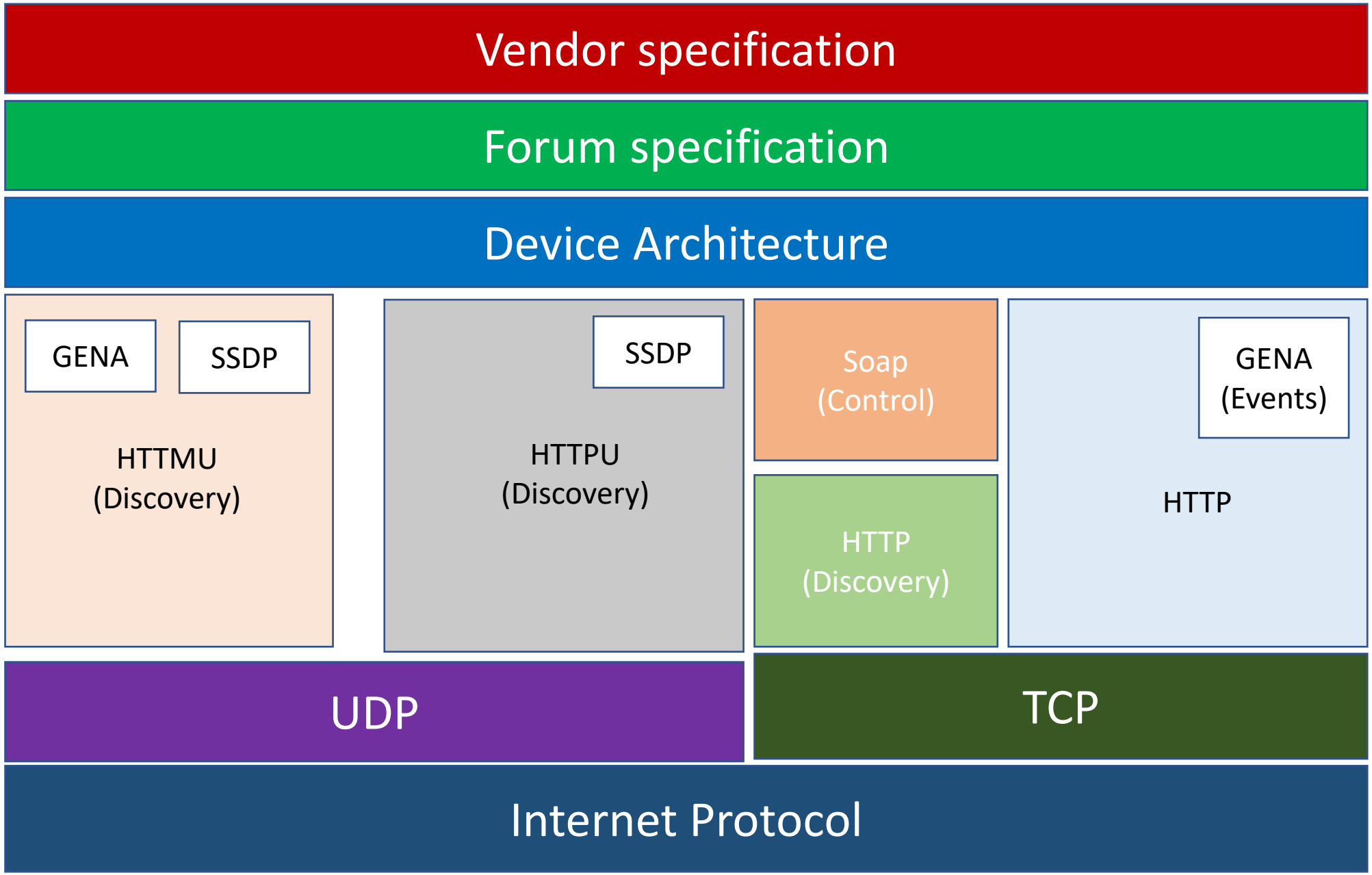
Multicast DNS (mDNS)

- Designed for small networks.
- It is analogous to DNS.
- It is zero configuration service.
- It use multicast UDP for resolving host name.
- mDNS Client initiates a multicast query on the IP network.
- The query includes a question to a remote server/host to identify the name.
- The mDNS cache in the associated network subnet is updated with the multicast response received from the target.
- A node can give up its claim to a domain name by setting the time to live field to zero in its response packet to an mDNS query.
- Example : Apple Bonjour Service and Network printer discovery service in Windows 10.
- Drawback: Host name resolution reach to top level domain only.

Universal plug and play (UPnP)

- Universal plug and play encompasses a set of networking protocols aimed at service disc and the establishment of functional network based data sharing and communication services.
- It is used for enabling dynamic connections of devices to computing platforms.
- It is called plug and play as devices attaching to a computer networks can configure themselves and update their hosts about their working configuration over a network.
- The UpNp is backed by a forum of many consumer electronics vendors and industries and managed by the open connectivity Foundation.
- It designed for non-enterprise devices.
- Its scope include the discovery and intercommunication between networked devices (mobiles, printers, access point, gateways, television, regular commercial devices enabled with IP capabilities)

An outline of the basic UPnP stack



Universal plug and play (UPnP)

- The UPnp has been designed to run on IP enabled networks and makes use of the networking services of HTTP, XML, SOAP for data transfer, device description and event generation and monitoring.
- It enables UDP based HTTP device search requests and advertisements using multicasting.
- The responses to device request are unicast messages.
- Upnp advertisement use UDP port 1900 for multicasting.
- The unnecessary overhead and traffic generated by UPnP systems and their multicast behavior make them unsuitable for enterprise systems.
- The reason behind this is, on a large scale, the cost of the solution would be infeasible from an operational point of view.

DATA PROTOCOLS

Data Protocols

- The protocols used for accessing, storage, and distribution of data over the IoT network is known as data protocols.

- Various data protocols includes

1. MQTT (Message Queue Telemetry Transport)
2. MQTT-SN (Message Queue Telemetry Transport for Sensor Network)
3. CoAP (Constrained Application Protocols)
4. AMQP (Advanced Message Queueing Protocols)
5. XMPP (The eXtensible Messaging and Presence Protocol)
6. SOAP (Simple Object Access Protocol)
7. REST (REpresentational State Transfer)
8. WS (Web Sockets)

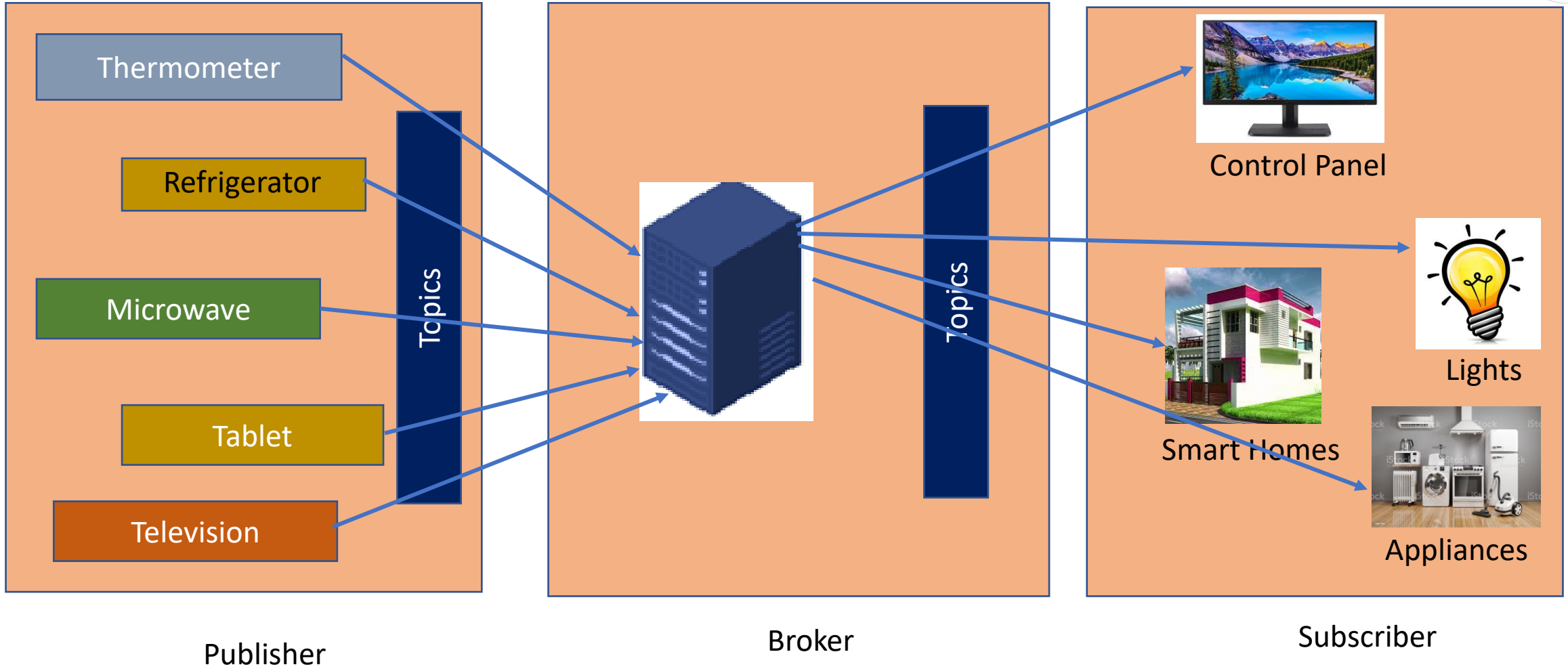
MQTT
(Message Queue Telemetry Transport)

MQTT

Introduction

- MQTT is a simple, light weight, publish subscribe protocol.
- It is designed for constraint devices and networks.
- It provides a one-many distribution of messages and is payload content agnostic.
- It works reliably and flawlessly over high latency and limited bandwidth of unreliable networks without the need for significant device resources and device powers.

MQTT Operation and its stakeholders



MQTT

Description of figure

- In MQTT, numerous clients connecting to a server, the server is known as broker.
- The clients can have the roles of information publishers (sending messages to the broker) or information subscribers (retrieving message from the broker).
- This allows MQTT to be largely decoupled from the applications being used with MQTT.

MQTT

Operational Principle

- It is built upon the principle hierarchical topics and works on TCP for communication over the network.
- Brokers receive a new message in the form of topics from the publishers.
- A publisher first send a control message along with the data message.
- Once updated in the broker, the broker distributes this topic's content to all the subscribers of that topic for which the new message has arrived.
- This paradigm enables publishers and subscribers to be free from any consideration of the address and ports multiple destination/subscribers or network considerations of the subscribers and vice versa.
- In the absence of any subscribers of a topic, a broker normally discards messages received for that topic unless specified by the publisher.

MQTT

- This feature removes data redundancy and ensures that maximally updated information is provided to the subscriber.
- It also reduces the requirements of storage at the broker.
- The publisher can set up default messages for the subscriber in agreement with the broker if the publishers connection is abruptly broken with the broker.
- This arrangement is termed as "*Last will and testament* " feature of MQTT.
- Multiple brokers can communicate in order to connect to a subscriber's topic if it is not present directly with the subscriber's primary broker.

MQTT Control Message

- It ranges from 2 bytes to 256 megabytes of data with a fixed header size of 2 bytes.
- It enables the MQTT to reduce the network traffic.
- The connection credential are unencrypted and often sent as plain text.
- The responsibility of protecting the connection lies with the underlying TCP layer.
- It provides 14 different message types which range from connect/disconnect operations to acknowledgements of data.

MQTT

Message Types

1. CONNECT : Publish/subscriber request to connect to the broker.
2. CONNACK : Acknowledgement after successful connection between publisher/ subscriber and broker.
3. PUBLISH : Message published by a publisher to a broker or a broker to a subscriber.
4. PUBACK : Acknowledgement of the successful publishing operation.
5. PUBREC : Assured delivery component message upon successfully receiving publish.
6. PUBREL : Assured delivery component message upon successfully receiving publish release signal.
7. PUBCOMP : Assured delivery component message upon successfully receiving publish completion.

MQTT

Message Types

8. SUBSCRIBE : Subscription request to a broker from a subscriber.

9. SUBACK : Acknowledgement of successful subscribe operation.

10. UNSUBSCRIBE : Request for unsubscribing from a topic.

11. UNSUBACK : Acknowledgement of successful unsubscribe operation.

12. PINGREQ : Ping request message.

13. PINGRESP : Ping Response Message.

14. DISCONNECT : Message for publisher/subscriber disconnecting from the broker.

MQTT

MQTT Message delivery QoS

It supports three QoS features.

1. At most once : It is a best effort delivery service and largely depend on the best efforts of the TCP/IP network on which the MQTT is supported. It may result in message duplication or loss.

2. At least once : This delivery service guarantees assured delivery of messages. However, message redundancy through duplication is a possiblility.

3. Exactly once : This delivery service guarantees assured message delivery. Additionally, this service also prevents message duplication.

MQTT-SN
(MQTT for Sensor Network)

MQTT-SN

Introduction

- It is a robust protocol to handle the requirements and challenges of wireless communication networks in sensor network.

- It has
  - ✓ Low bandwidth usage
  - ✓ Ability to operate under a high link failure conditions

- It is more suitable for low powered, low cost constraint nodes and networks.

Difference between MQTT *and* MQTT-SN

1. CONNECT Message is broken into three messages in which two are optional and are tasked with the communication of the testament message and testament topic to the broker.

2. The topic name in the PUBLISH messages are replaced by topic identifier which are only 2 bytes long. This reduces traffic generated from the protocol and enables the protocol to operate over bandwidth constrained network.

3. A separate mechanism is used for topic name registration with the broker in MQTT-SN. After topic identifier is generated for the topic name, the identifier is informed to the publisher/subscriber. This mechanism also supports the reverse pathway.

4. In special case, pre-defined topic identifier are present that need no registration mechanisms. The mapping of topic name and identifier are known in advance to the broker as well as the publisher/subscriber.

MQTT-SN

5. The presence of spatial discovery process is used to link the publisher/subscriber to the operational broker network address in the absence of a preconfigured broker address.

6. The subscription to a topic, Will topic, and Will message are persistent in MQTT-SN. The publisher/subscriber can modify their Will message during a session.

7. Sleeping publisher/subscriber are supported by a keep-alive procedure which is offline and which helps buffer the message intended for them in the broker until they wake up. This feature is not present in MQTT.

MQTT-SN Gateway

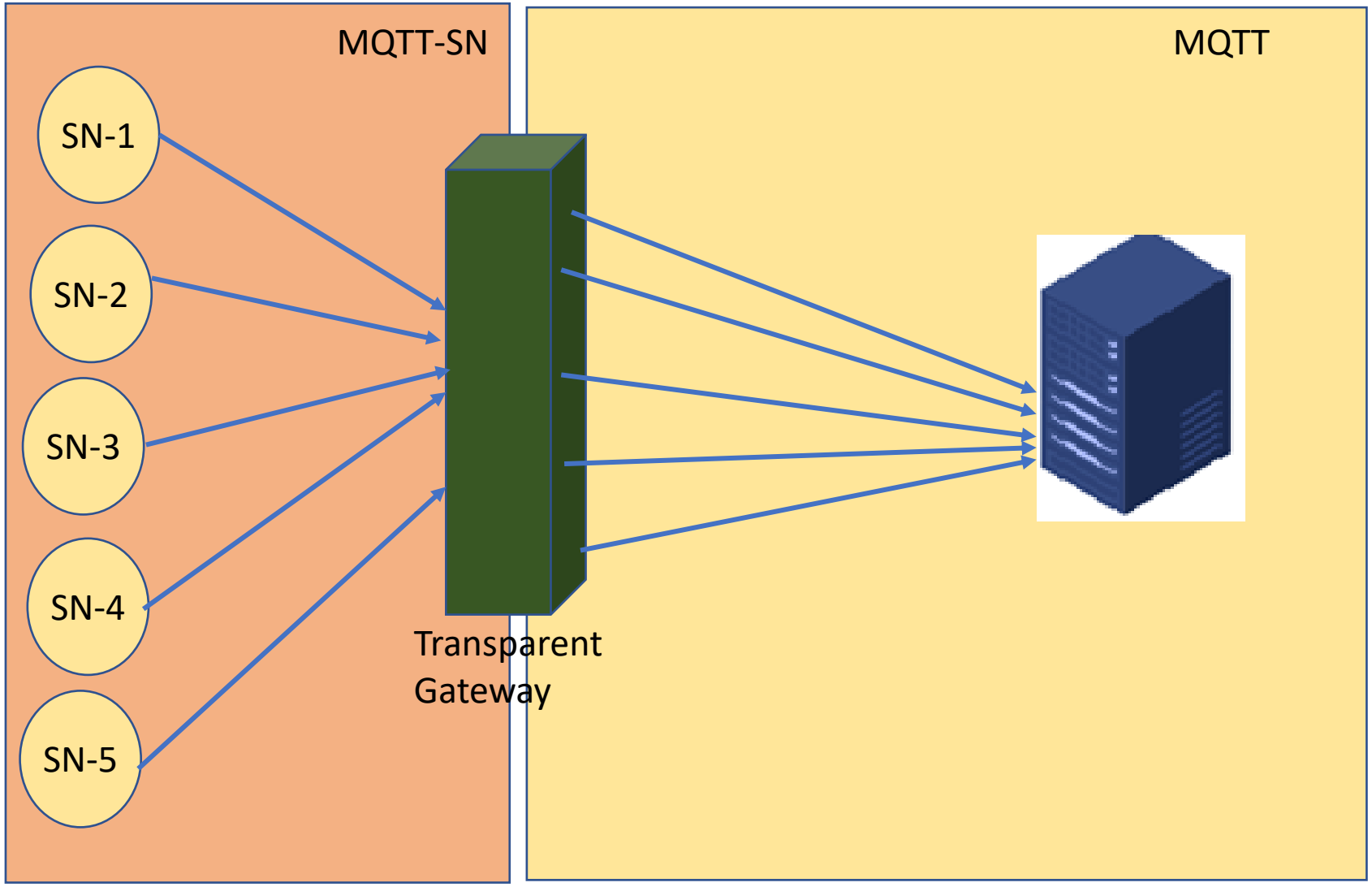
- It supports two gateway types.
  - ✓Transparent gateway
  - ✓Aggregating gateway

- The MQTT-SN converts/translates MQTT and MQTT-SN traffic by acting as a bridge between these two network types.

- The transparent gateway creates as many connections to the MQTT broker as there are MQTT-SN nodes within its operational purview.

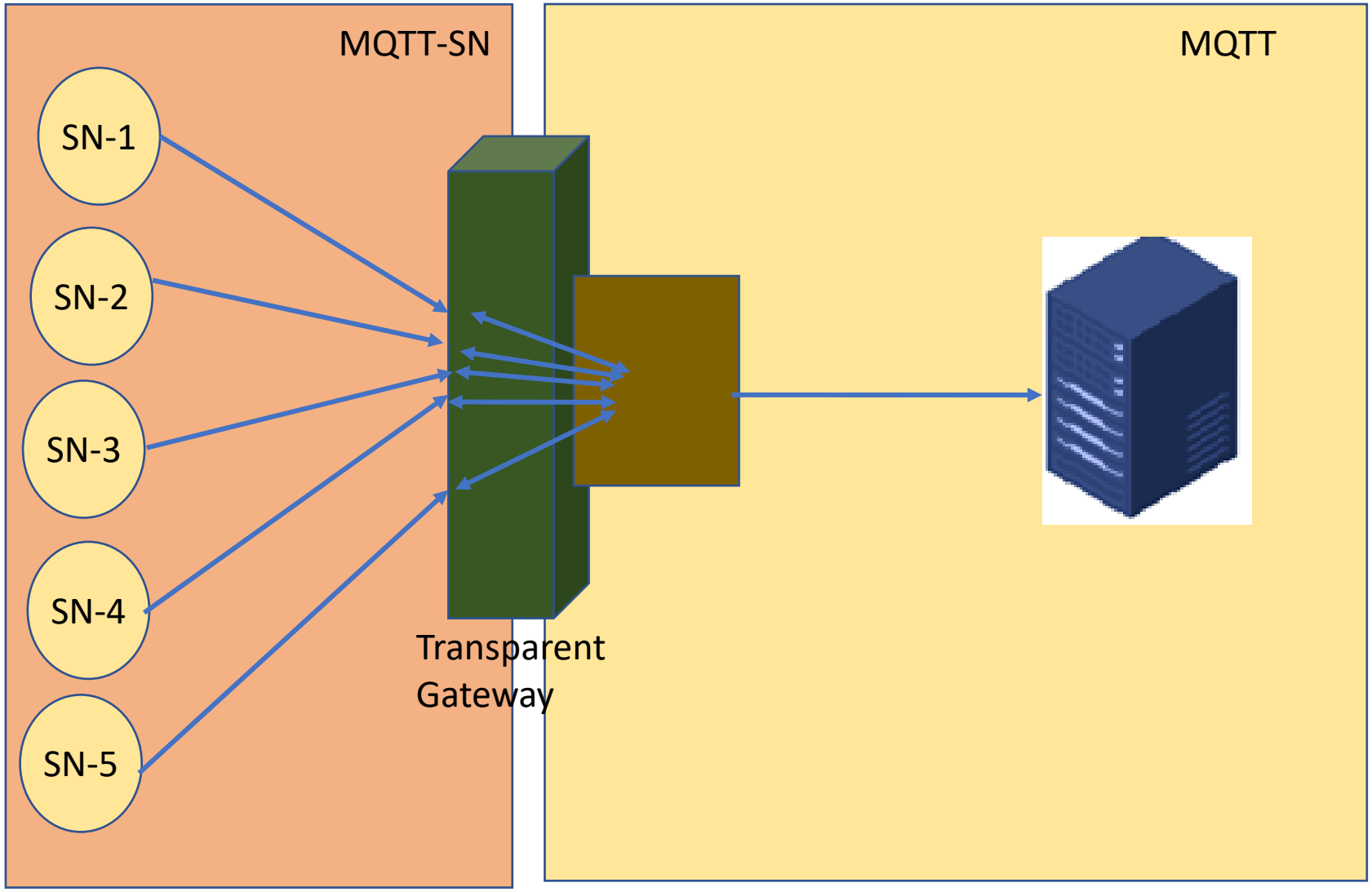
- The aggregating gateway creates a single connection to the MQTT broker irrespective of the number of MQTT-SN nodes under it.

The MQTT-SN types



Transparent Gateway

The MQTT-SN types



Aggregating Gateway

CoAP
Constrained Application Protocol

CoAP

Introduction

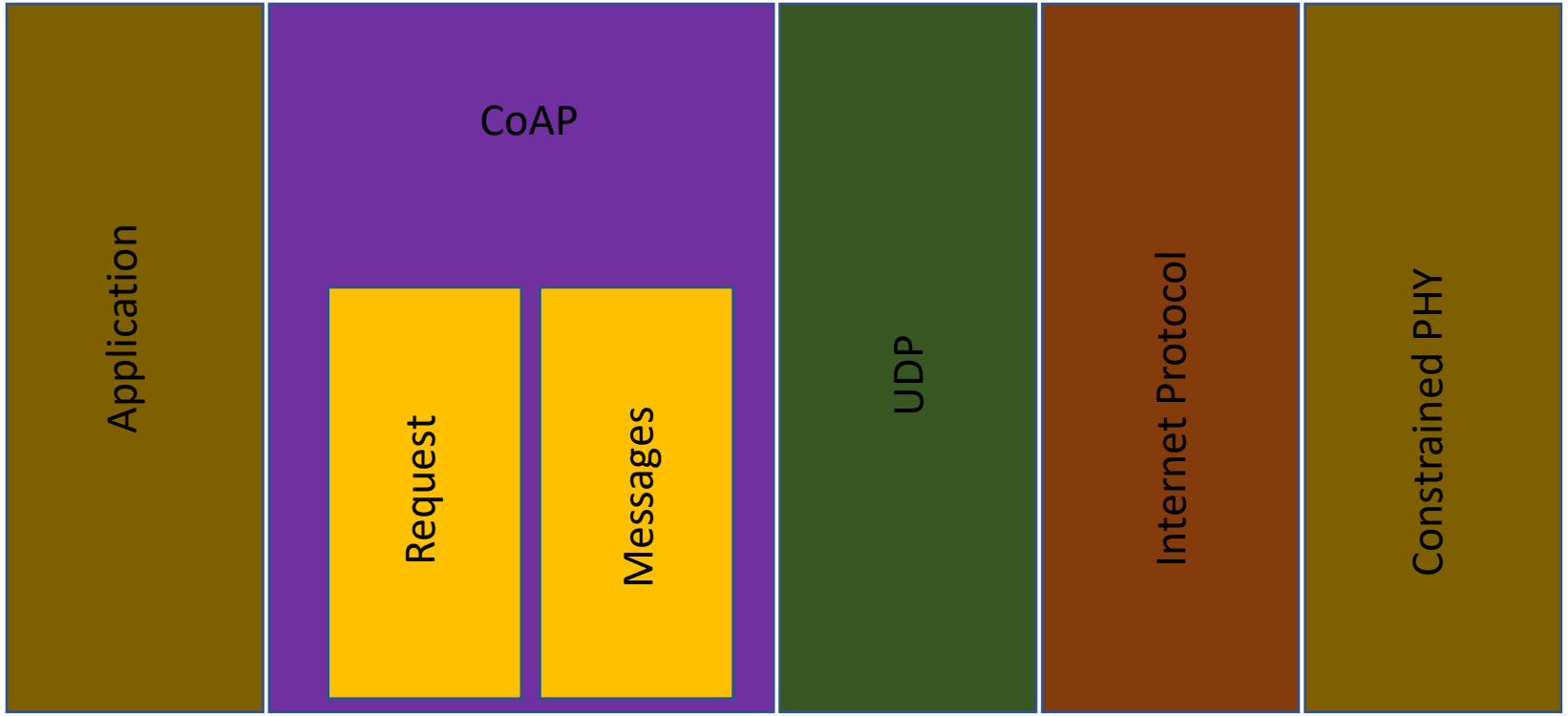
- It is a web transfer protocol in constrained devices (low power, minimal RAM, 8-bit processor) and networks (low power and lossy).
- CoAP can work efficiently when these devices connected to the highly lossy networks with high packet loss, high error rates, and bandwidth in range of kilobits.
- It follows request-response paradigm for communication over lossy networks.

CoAP

- It supports
  - ✓ Service discovery
  - ✓ Resource discovery
  - ✓ URIs (Uniform Resource Identifiers)
  - ✓ Internet media handling support
  - ✓ Easy HTTP integration
  - ✓ Multicasting support

- CoAP implementation is based on client-server architecture.
- A CoAP device can act as client and server, but not simultaneously.
- A CoAP client's request signifies a request for action from an identified resource on a server.
- A response sent by the server in the form of response code can contain resource representation also.

Position of COAP Protocol in a stack



CoAP Messaging

- It supports four message types.
  1. Confirmable
  2. Non-confirmable
  3. Acknowledgement
  4. Reset

- Request messages are carried using Confirmable and Non-confirmable message types.

- Response messages are carried using Confirmable and Non-confirmable, and acknowledgement message types.

- The transmission of responses with acknowledgement message is known as *piggybacking*.

CoAP Features

1. It has suitable web protocol for integrating IoT and M2M services in constrained environments with the Internet.

2. CoAP enables UDP binding and provides reliability concerning unicast as well as multicast request.

3. Message exchanges between end points in the network or between nodes is asynchronous.

4. The limited packet header incurs significantly lower overheads. This also results in less complexity and processing requirements for parsing of packets.

CoAP Features

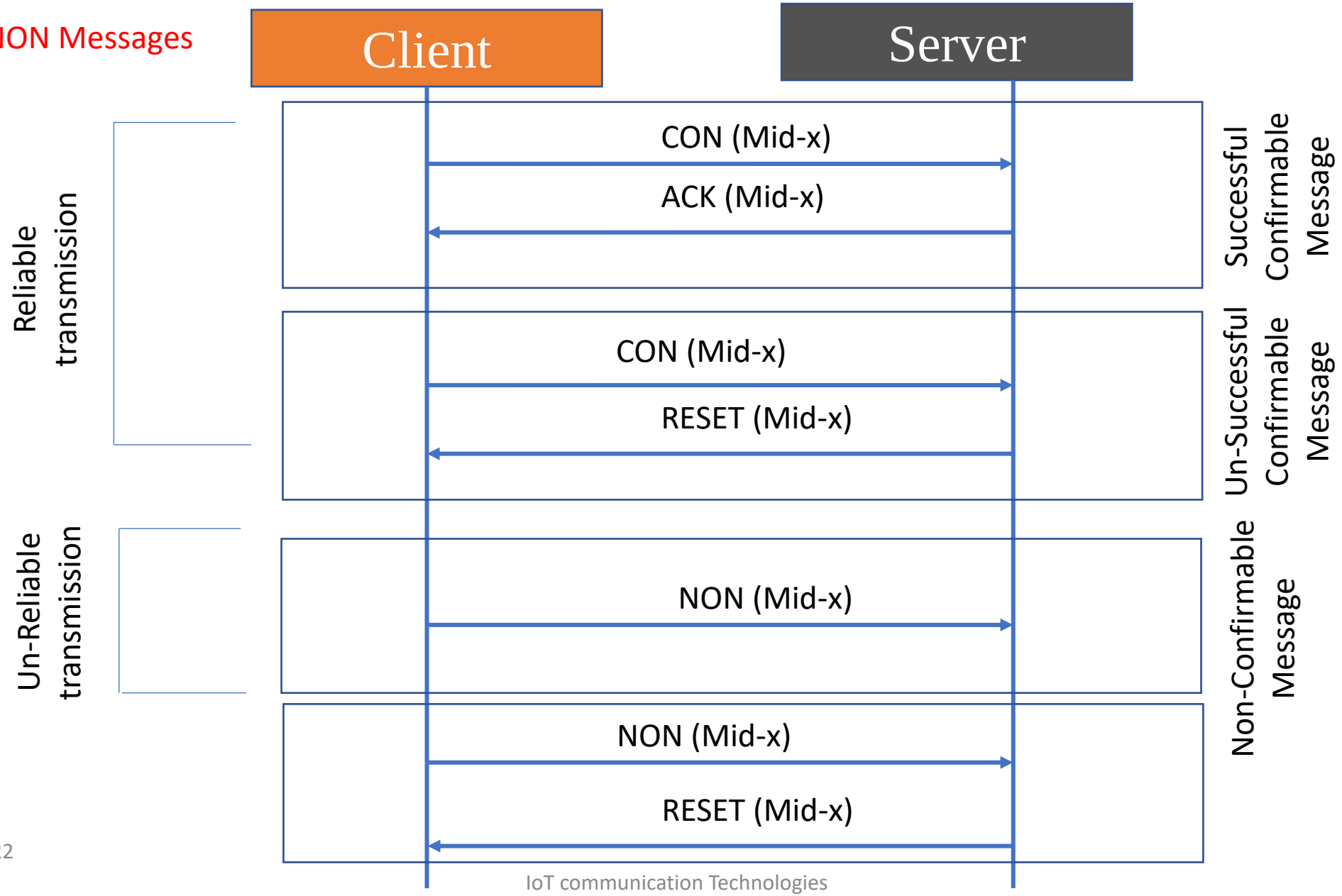
- CoAP has provision for URI and other content type identification support. CoAP additionally provides DTLS binding.

- It has a straightforward proxy mechanism and caching capability which is responsible for overcoming the effects of the lossy networks without putting extra constraints on the low power devices. The caching is based on the concept of the maximum age of packets.

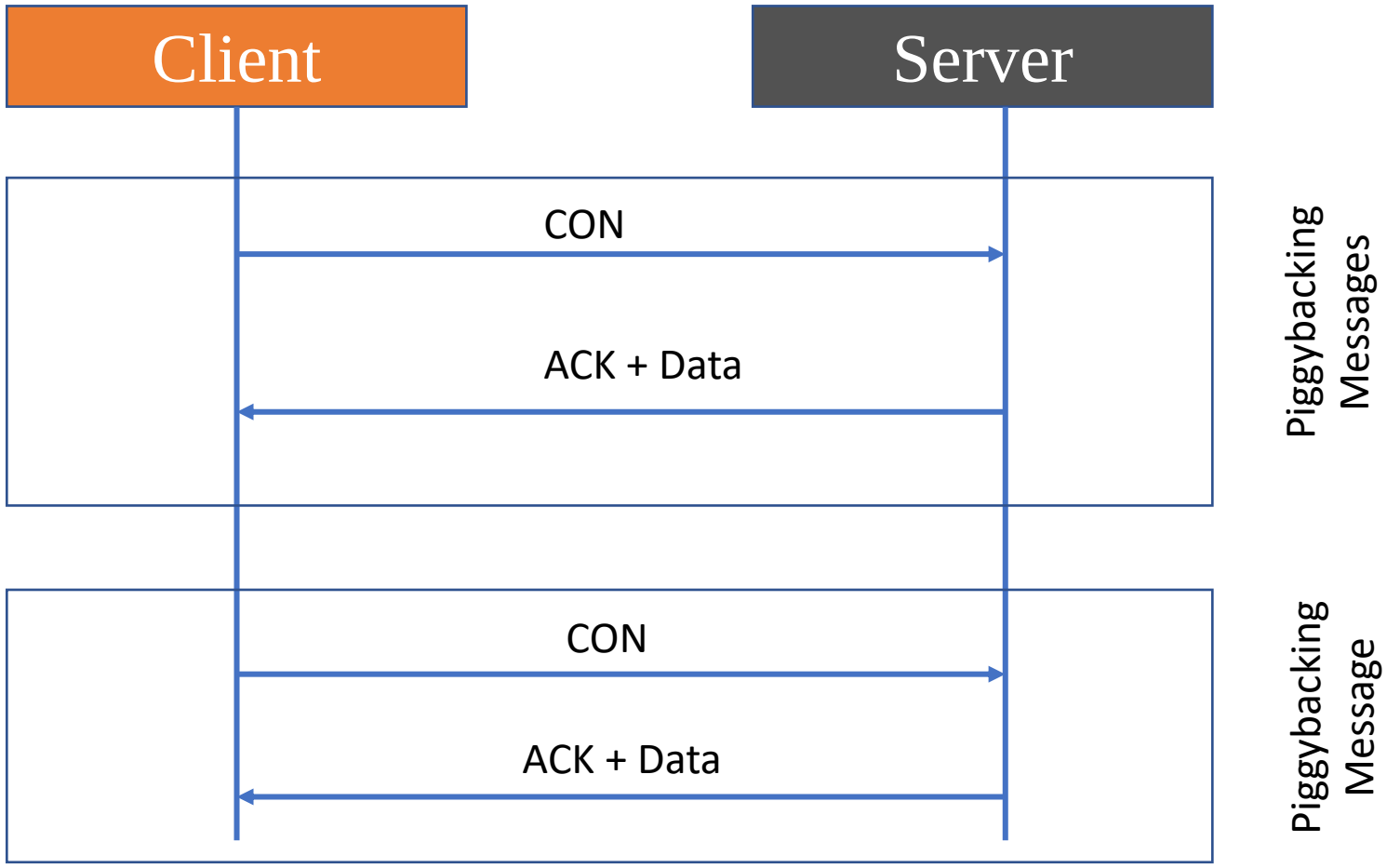
- This protocol provides a stateless mapping with HTTP. The server and receiving node does not retain information about the source of messages. Rather it is expected that the message packet carries that information with it. This enables CoAP's easy and uniform integration with HTTP.

CoAP request-response model

A : CON and NON Messages

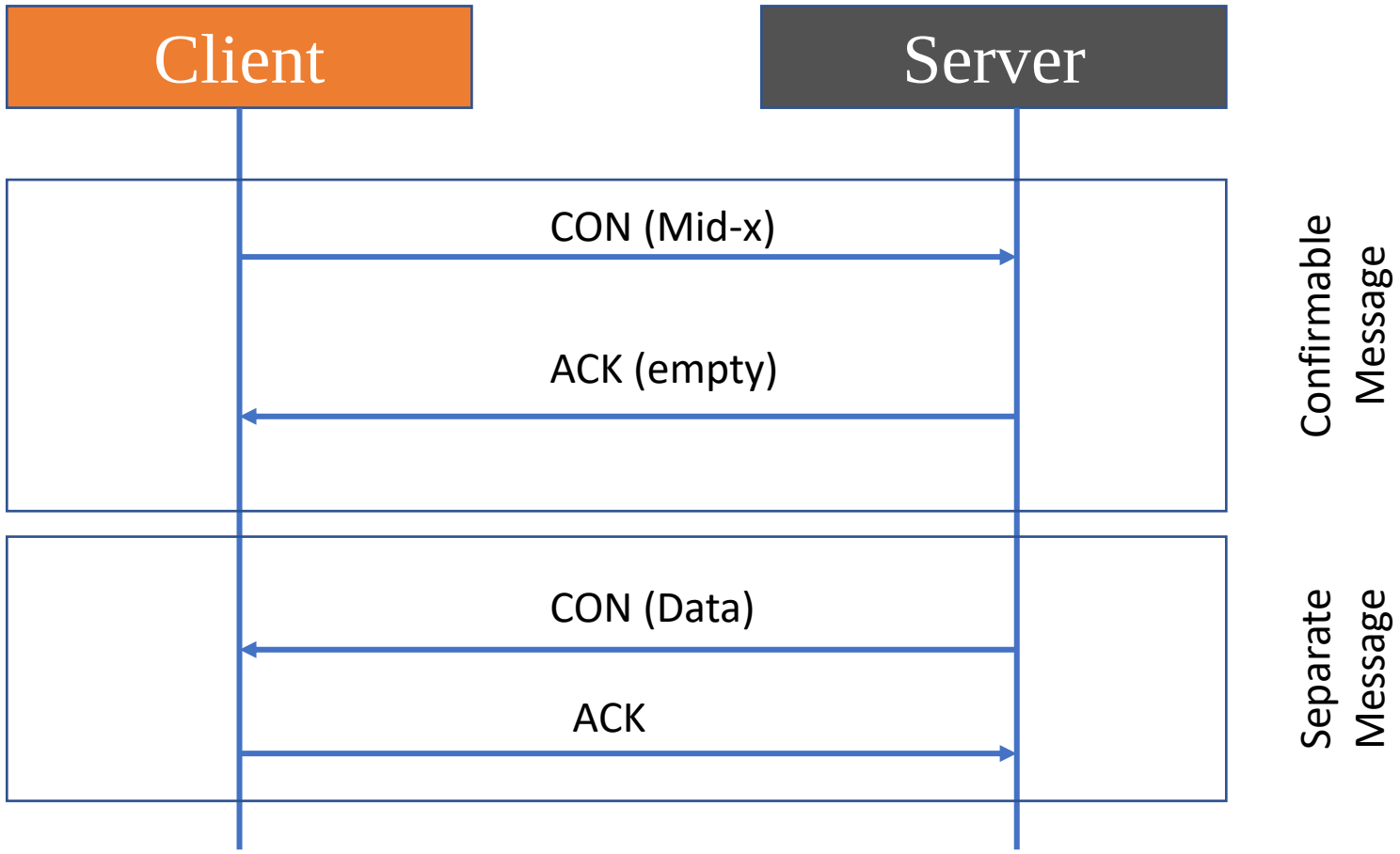


CoAP request-response model



B : Piggyback Messages

CoAP request-response model



C : Separate Messages

CoAP Operational Features

- CoAP is build upon the exchange of information between two or more UDP end points.

- Components of CoAP packet is header (4 byte length), message Id (2 byte), option and payload.

AMQP
(Advanced Message Queueing Protocol)

AMQP

Introduction

- It is an open standard middleware at the application layer developed for message oriented operations.
- It supports both publish-subscribe, and request-response methods.
- It is a wire level protocol.
- Components of AMQP are Publisher, subscriber and broker.

AMQP

- Features
  - ✓ Flow controlled communication
  - ✓ Message oriented communication
  - ✓ Message delivery guarantees
  - ✓ Authentication support
  - ✓ TLS based encryption support

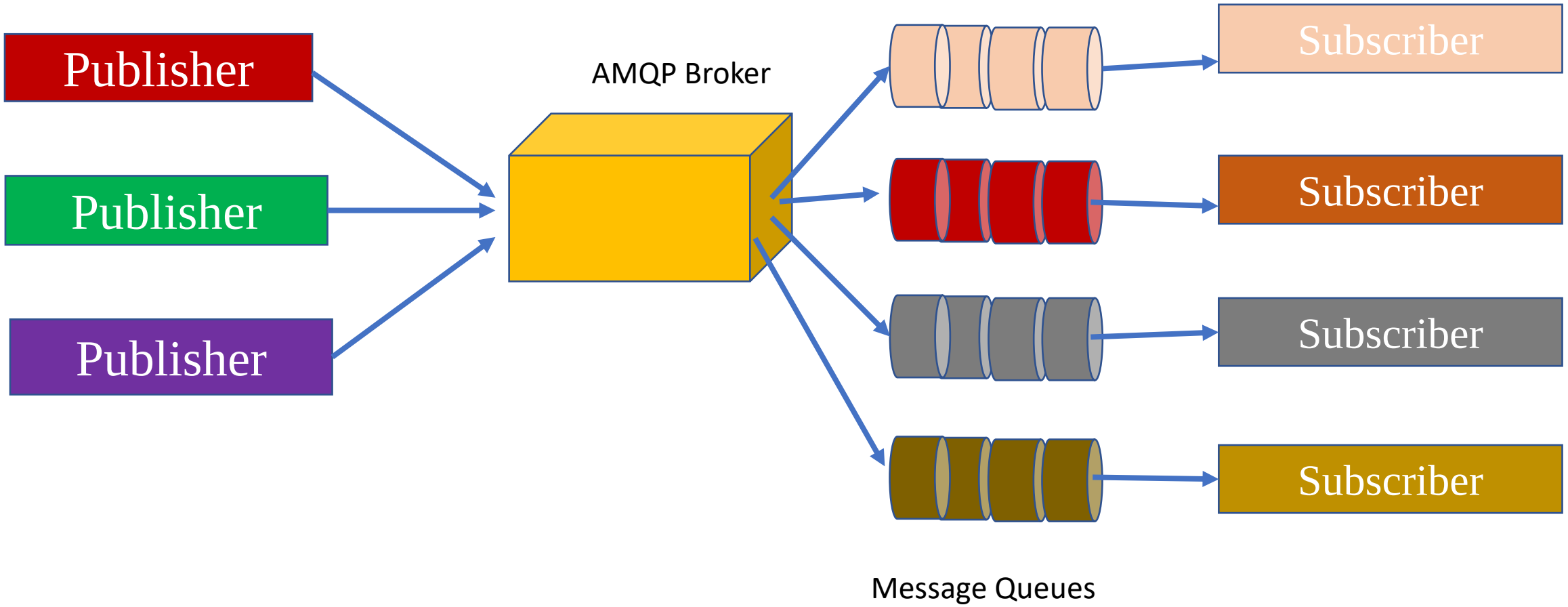
- Layers
  - ✓ Type system
  - ✓ Process to process asynchronous and symmetric message transfer protocol
  - ✓ Extensible message format
  - ✓ Set of extensible messaging capabilities

- Data Unit
  - ✓ Frame
  - ✓ Supports 9 frame types

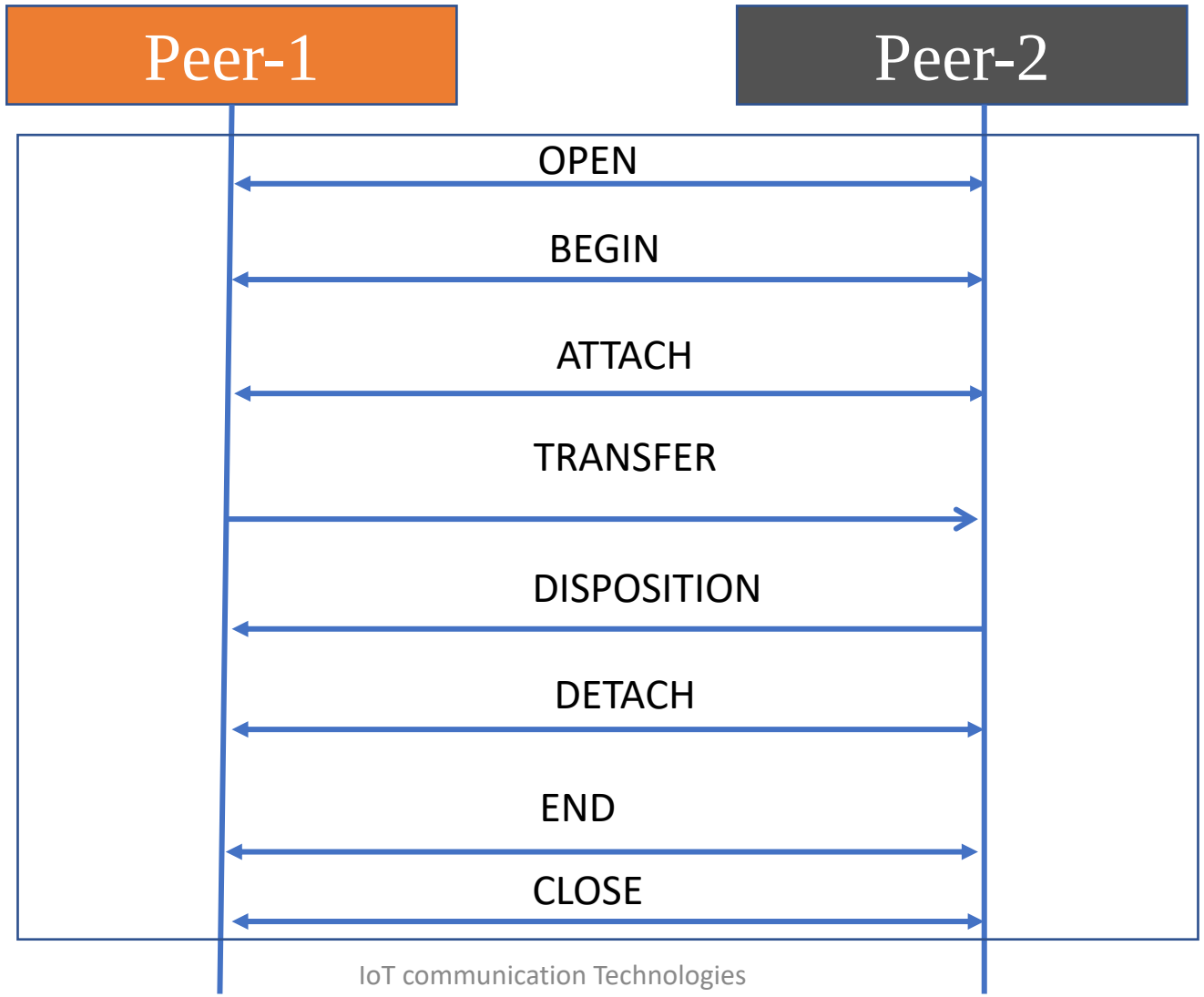
Frame types in AMQP

- Open: Responsible for opening the connection between peers.
- Begin: Responsible for setup and control of messaging sessions between peers.
- Attach : Responsible for link attachment.
- Transfer : Responsible for message transfer over the link.
- Flow : Responsible for updating the flow control state.
- Disposition : Responsible for updating of transfer state.
- Detach : Responsible for detachment of link between two peers.
- End : Responsible for truncation of a session.
- Close: Responsible for closing/ending a connection.

AMQP Components and their relationships



AMQP Operational Principle

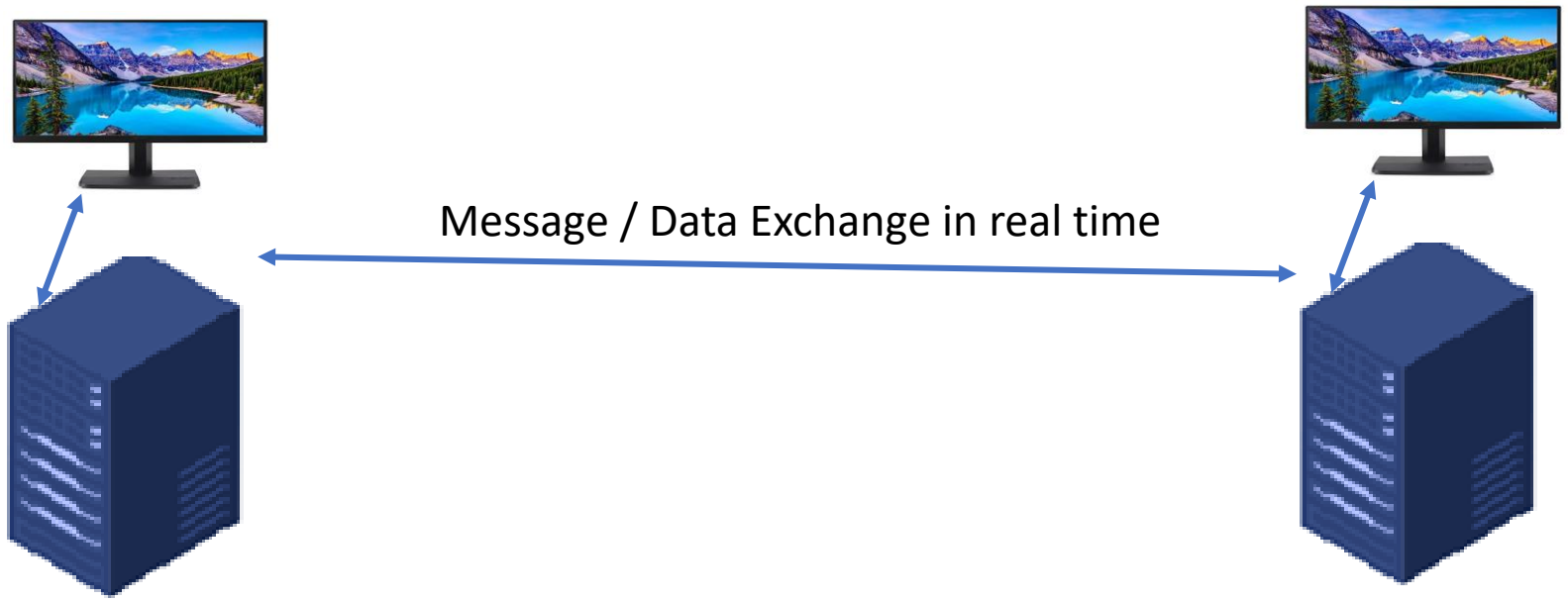


XMPP

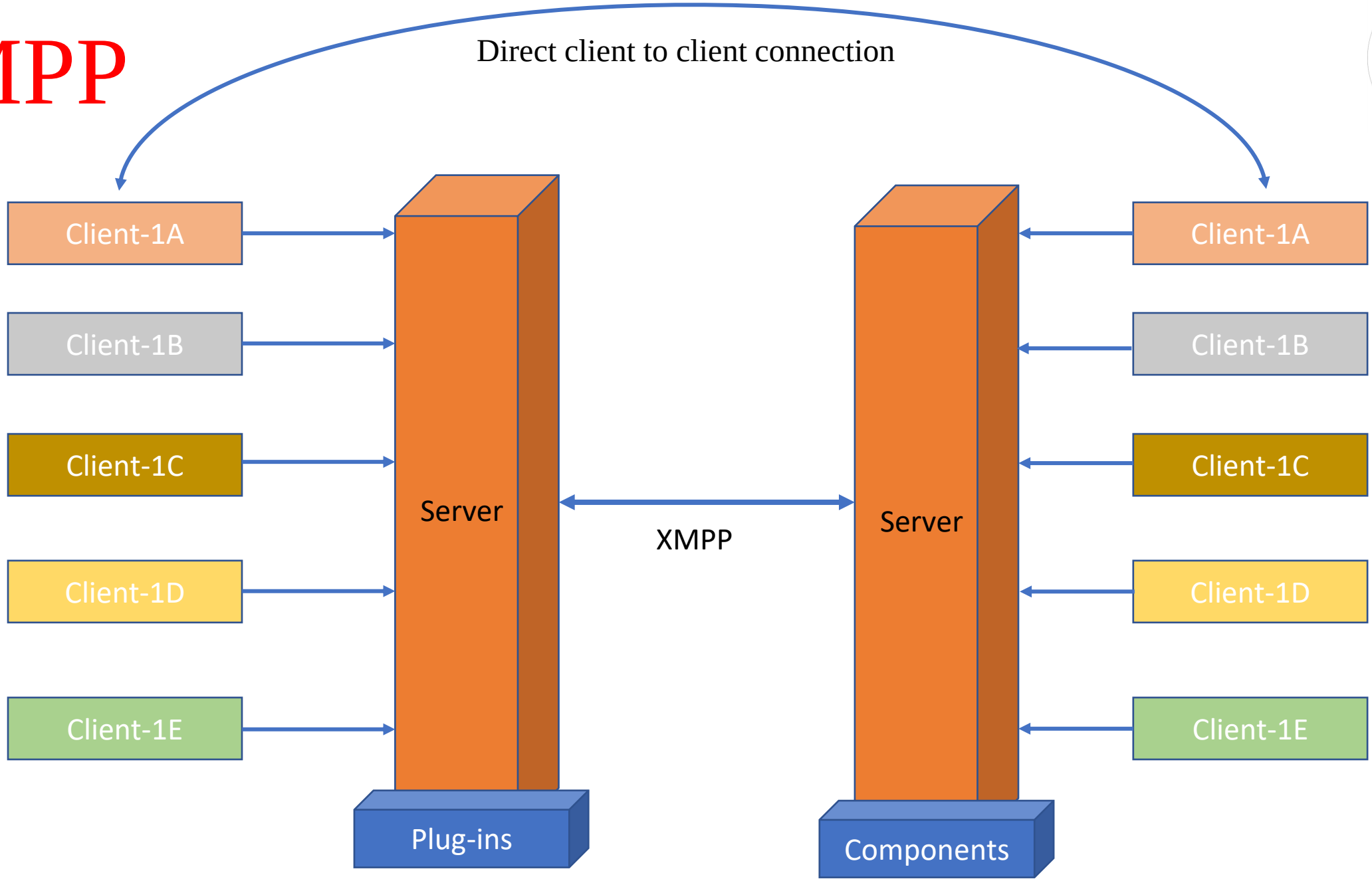
XMPP

- Extensible messaging and presence protocol
- Jabber ID
- Message oriented middleware based on the XML
- Functionalities
  - ✓Instant messaging
  - ✓Maintenance of contacts
  - ✓Information about network presence

XMPP



XMPP


Direct client to client connection
Client-1A
Client-1B
Client-1C
Client-1D
Client-1E
Server
Plug-ins
XMPP
Server
Components
Client-1A
Client-1B
Client-1C
Client-1D
Client-1E

XMPP

- Widely used in
  - ✓VOIP (Voice over Internet Protocol)
  - ✓Video and file transfer
  - ✓Smart Grid
  - ✓Social Network
  - ✓Publish Subscribe network

- It follows client Server architecture

- All communication between peers has to be carried through XMPP server

XMPP

Operational Principle

- A unique XMPP address is known as Jabber ID.
- It is assigned to every user on the XMPP network.
- It is similar to email address.
- Address has two parts.
  - ✓ User name (Any name)
  - ✓ Domain name (IP address of the server)
- user@domain.com

XMPP

- It allows its user to login from multiple devices by specifying its resources.
- Resources are home, mobile, work, laptop, and others.
- Resources are prioritized using numerical IDs.
- User @ domain.com / resource
- Any message arriving with default JID is forwarded to resource with highest priority.
- Without user ID JID is considered as the control message or system message.

XMPP

XMPP Technology

- ✓Core
- ✓Jingle
- ✓Multi user chat
- ✓Pub-Sub
- ✓BOSH

XMPP

Core

- ✓Base XML layer of streaming
- ✓Provides TLS-based encryption
- ✓Impacts simple authentication and security layer
- ✓Informs about availability of the network
- ✓Provides UTF-8 (Unicode transformation format-8 bit) supports

XMPP

Jingle

- It is a session initiation protocol.
- It is compatible for multimedia signaling for voice, video, file transfer and other applications.
- Various media transfer protocols are TCP, UDP, RTP.
- Jingle session initiation signal is sent over XMPP and media transfer takes place in a peer-to-peer manner and over media relays.

XMPP

Multi User Chat

- It is flexible multiparty communication exchange extension for XMPP.
- Here multiple users can exchange information in a chat room or channel.
- It supports strong chat room support which enables the banning of users and updation of chat room moderators.

XMPP

Pub-Sub

- It provides publish-subscribe functionalities to XMPP by providing alerts and notification for data syndication, vibrant presence.

- It enables XMPP client to create topic at a pub-sub service and publish/subscribe to them.

XMPP

BOSH

- Bidirectional streams over synchronous HTTP.
- It is HTTP binding for XMPP traffic.
- It incurs lower latencies and lesser network bandwidth usage.
- It is used for XMPP traffic exchange between clients and servers.

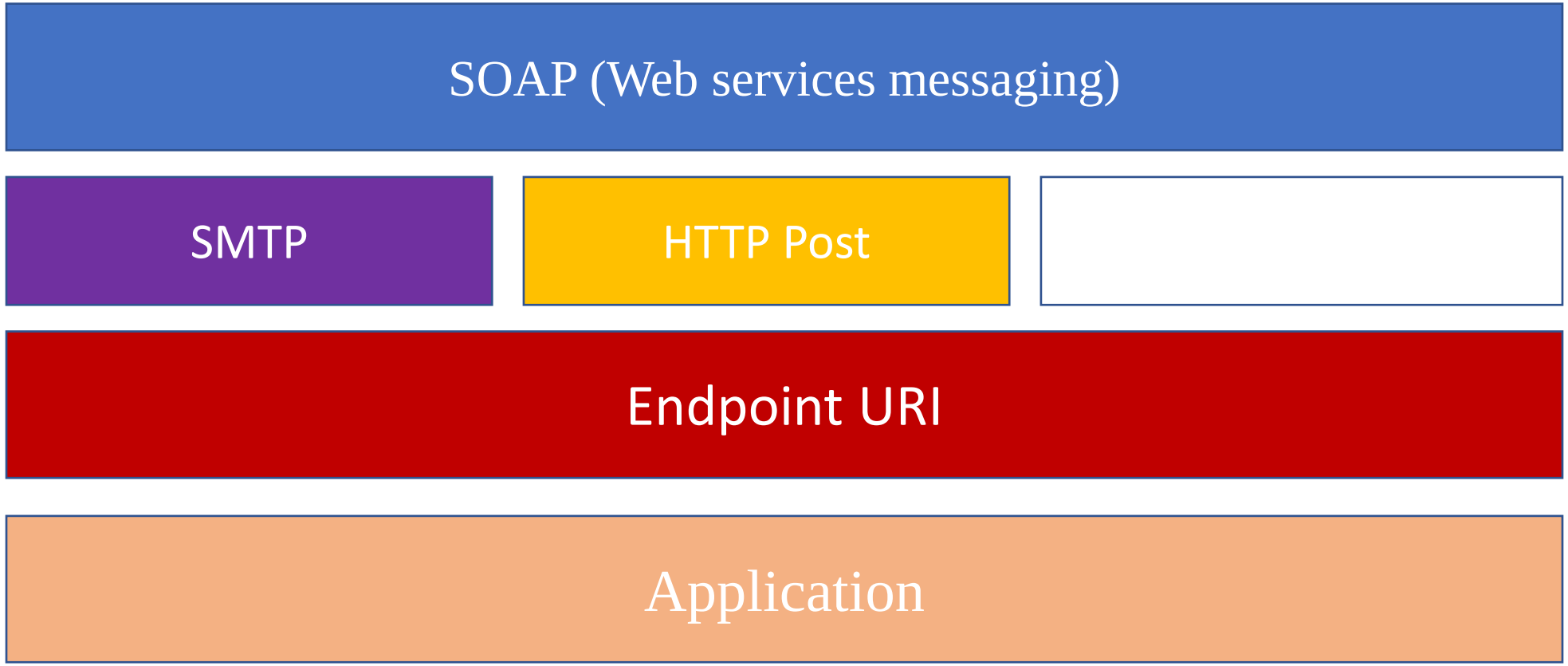
SOAP

SOAP

Introduction

- Simple object access Protocol.
- It exchanges structured information using web services (XML).
- Application layer protocol uses HTTP, SMTP (transmission and negotiation of messages).
- It is language and platform independent protocol

A representation of the position of the SOAP API in a stack



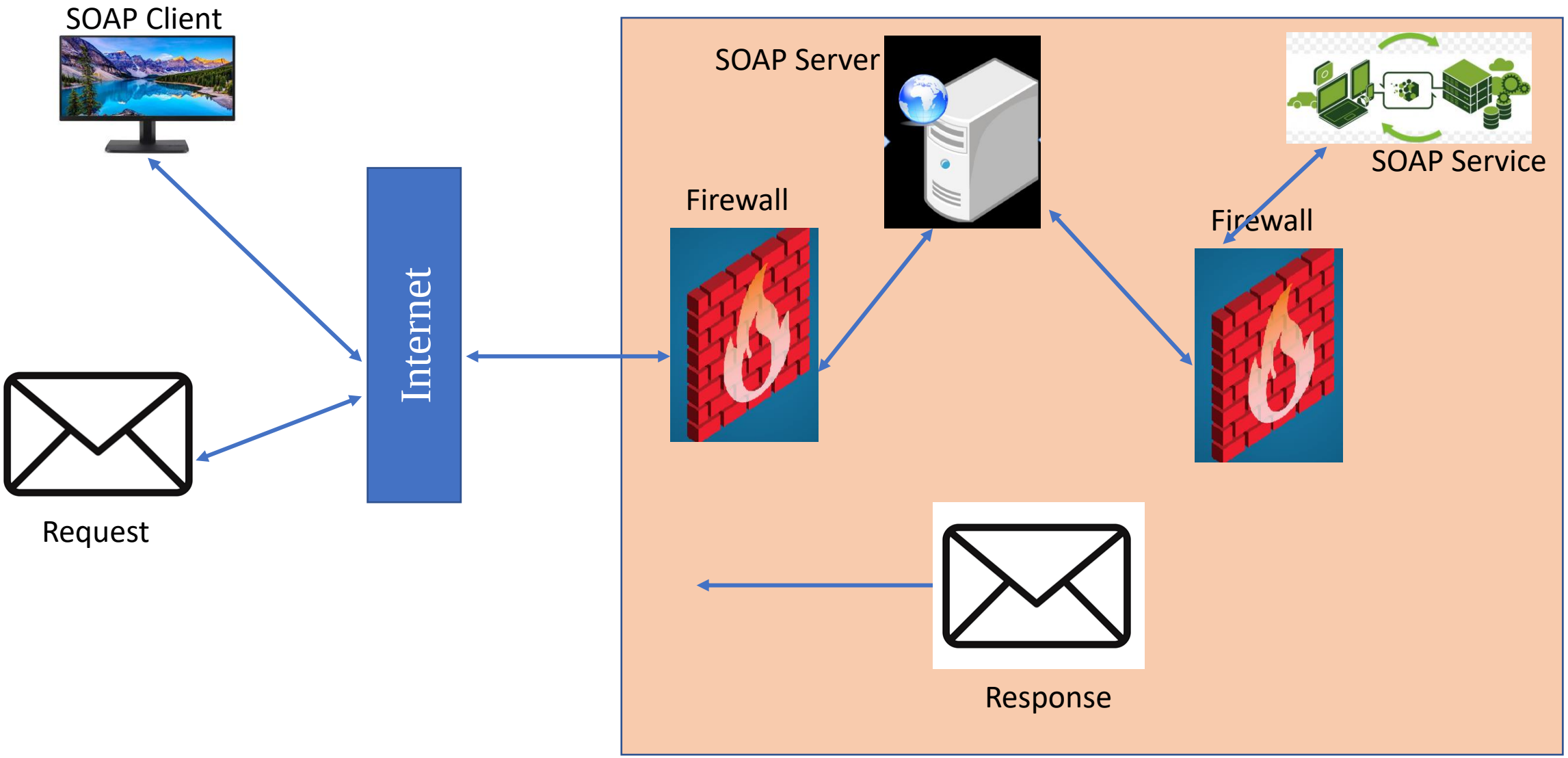
SOAP

Working Principle

- A SOAP Application can send a request with requisite search parameters to a server with web service enabled.

- A target server responds in a SOAP response format with result of server.

Working of SOAP



SOAP

SOAP Components

It has *three* components.

1. Envelope (It defines the structure of the message and its processing instructions)
2. Encoding Rules (It handles various data types arising out of the numerous applications)
3. Conventions (It is responsible for web procedure call and their responses)

SOAP

Features

It extends the feature of

- Neutrality (can operate over any application layer protocols)
- Independence (Independent of programming models)
- Extensibility (Security and web service addresses can be extended)

SOAP

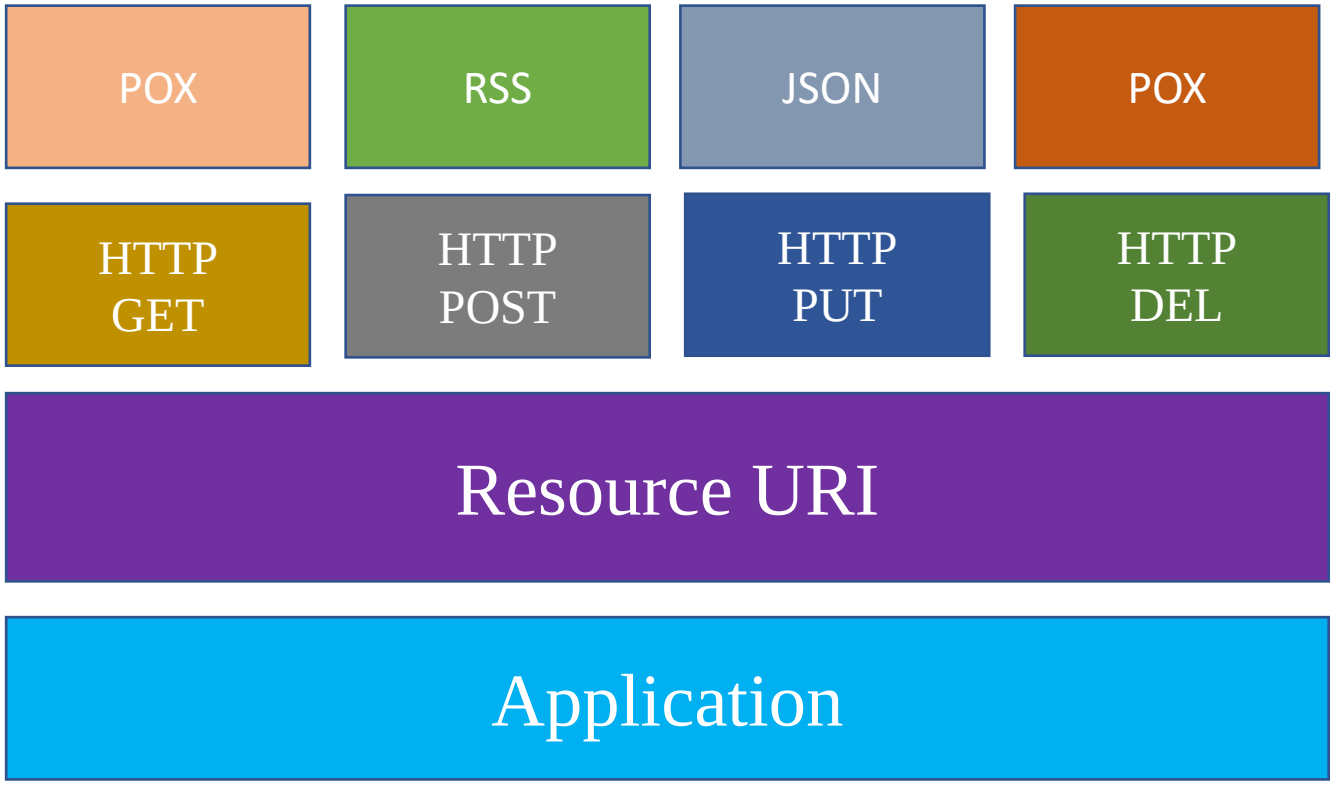
- The use of SOAP with HTTP based request and response exchanges does not require the modification of communication and processing infrastructure.
- It can easily pass through network or system firewalls and proxies.
- Use of XML affects the parsing speed and performance of protocol.
- The verbose nature of this protocol is not recommended for use every where.

SOAP

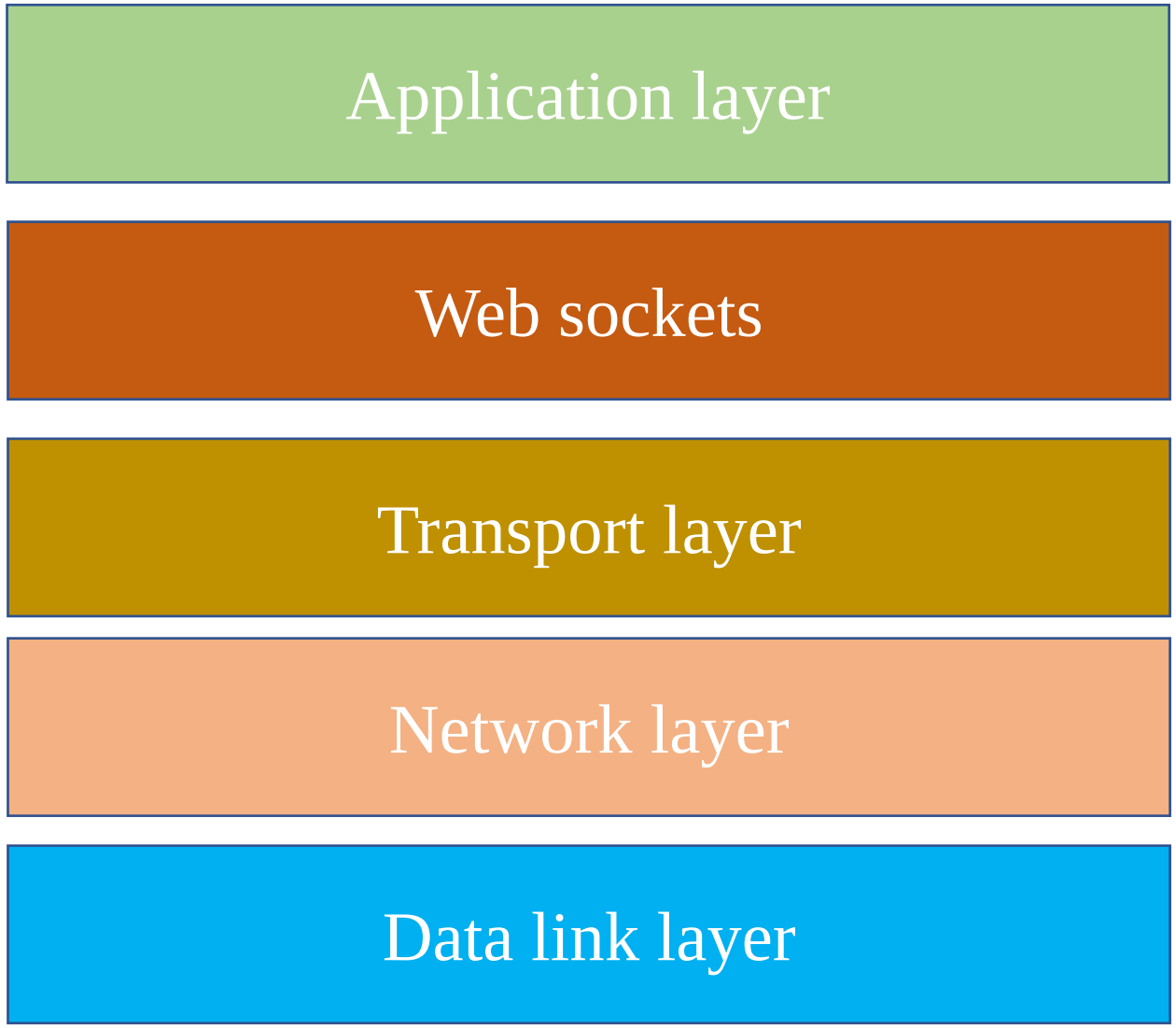
Its specification is explained over

- Message format layer
- Message exchange pattern layer
- Transport protocol binding layer
- Message processing model layer
- Protocol extensibility layer.

A representation of the REST style and its components



A representation of the position of web sockets in a stack



THANK YOU

Interoperability in Internet of Things

Current Challenges in IoT

- Large Scale of Co-Operation
  - ✓ The cooperation and coordination of millions of distributed devices are required on Internet

- Global Heterogeneity
  - ✓ Heterogeneous IoT devices and their subnets

- Unknown IoT Device Configuration:
  - ✓ The different configuration modes for IoT devices which come from unknown owners

- Semantic Conflicts:
  - ✓Different processing logics applied to same IoT networked devices or applications.

What is Interoperability?

- Interoperability is a characteristic of a product or system, whose interfaces are completely understood, to work with other products or systems, present or future, in either implementation or access, without any restrictions.

- Communicate meaningfully

- Exchange data or services

Why Interoperability is Important in Context of IoT ?

- To fulfill the IoT objectives

✓Physical objects can interact with any other physical objects and can share their information.

✓ Any device can communicate with other devices anytime from anywhere.

✓Machine to Machine communication(M2M), Device to Device Communication (D2D), Device to Machine Communication (D2M).

✓Seamless device integration with IoT network.

Why Interoperability is required?

✓Heterogeneity

- Different wireless communication protocols such as ZigBee (IEEE 802.15.4), Bluetooth (IEEE 802.15.1), GPRS, 6LowPAN, and Wi-Fi (IEEE 802.11)
- Different wired communication protocols like Ethernet (IEEE 802.3) and Higher Layer LAN Protocols (IEEE 802.1)
- Different programming languages used in computing systems and websites such as JavaScript, JAVA, C, C++, Visual Basic, PHP, and Python
- Different hardware platforms such as Crossbow, NI, etc.

Why Interoperability is required? (Contd.)

- ✓Different operating systems
  - As an example for sensor node: TinyOS, SOS, Mantis OS, RETOS, and mostly vendor specific OS
  - As an example for personal computer: Windows, Mac, Unix, and Ubuntu
- ✓Different databases: DB2, MySQL, Oracle, PostgreSQL, SQLite, SQL Server, and Sybase
- ✓Different data representations
- ✓Different control models
- ✓Syntactic or semantic interpretations

Different Types of Interoperability?

- User Interoperability

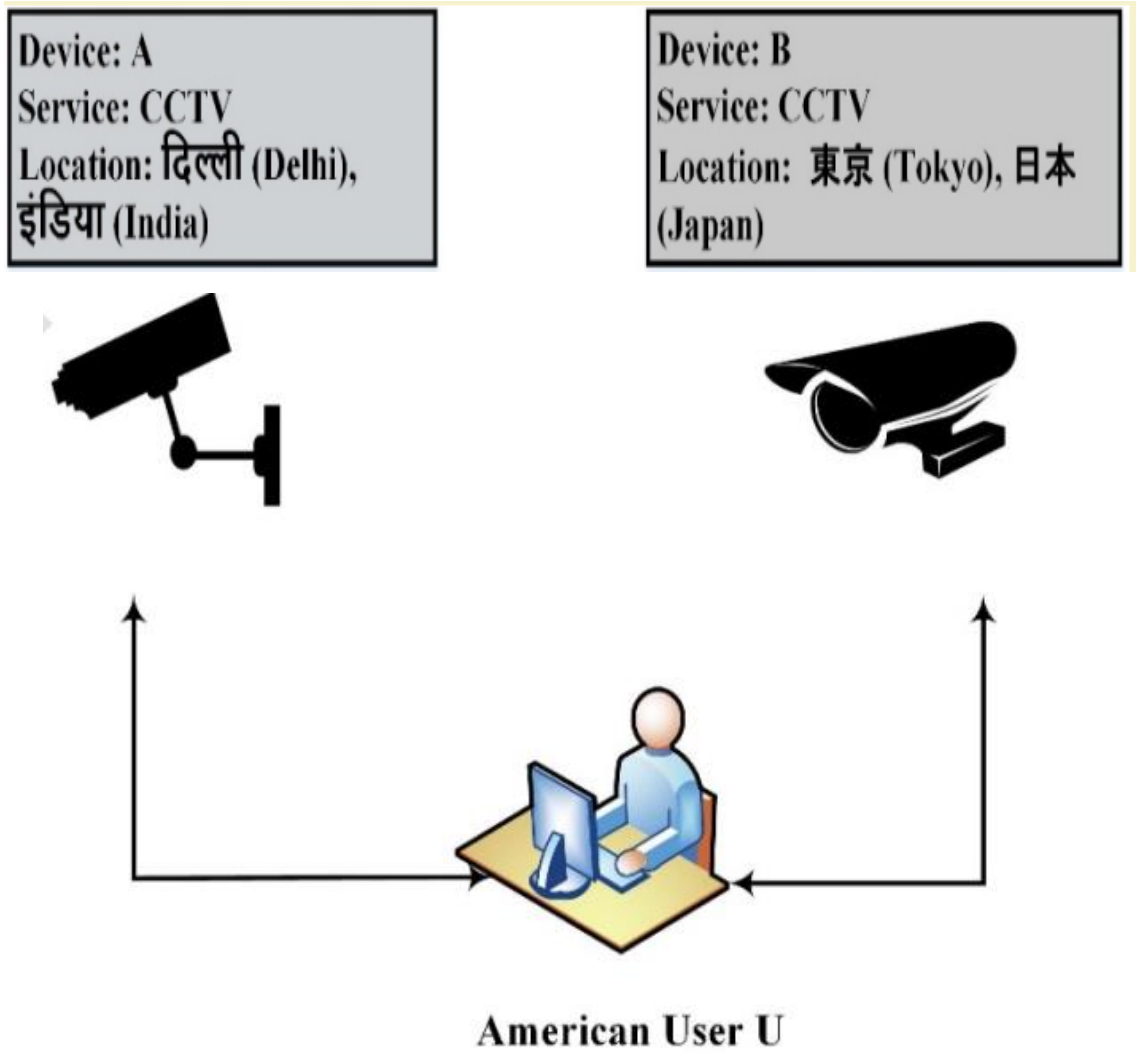
✓Interoperability problem between a user and a device

- Device Interoperability

✓Interoperability problem between two different devices

Example of Device and User Interoperability

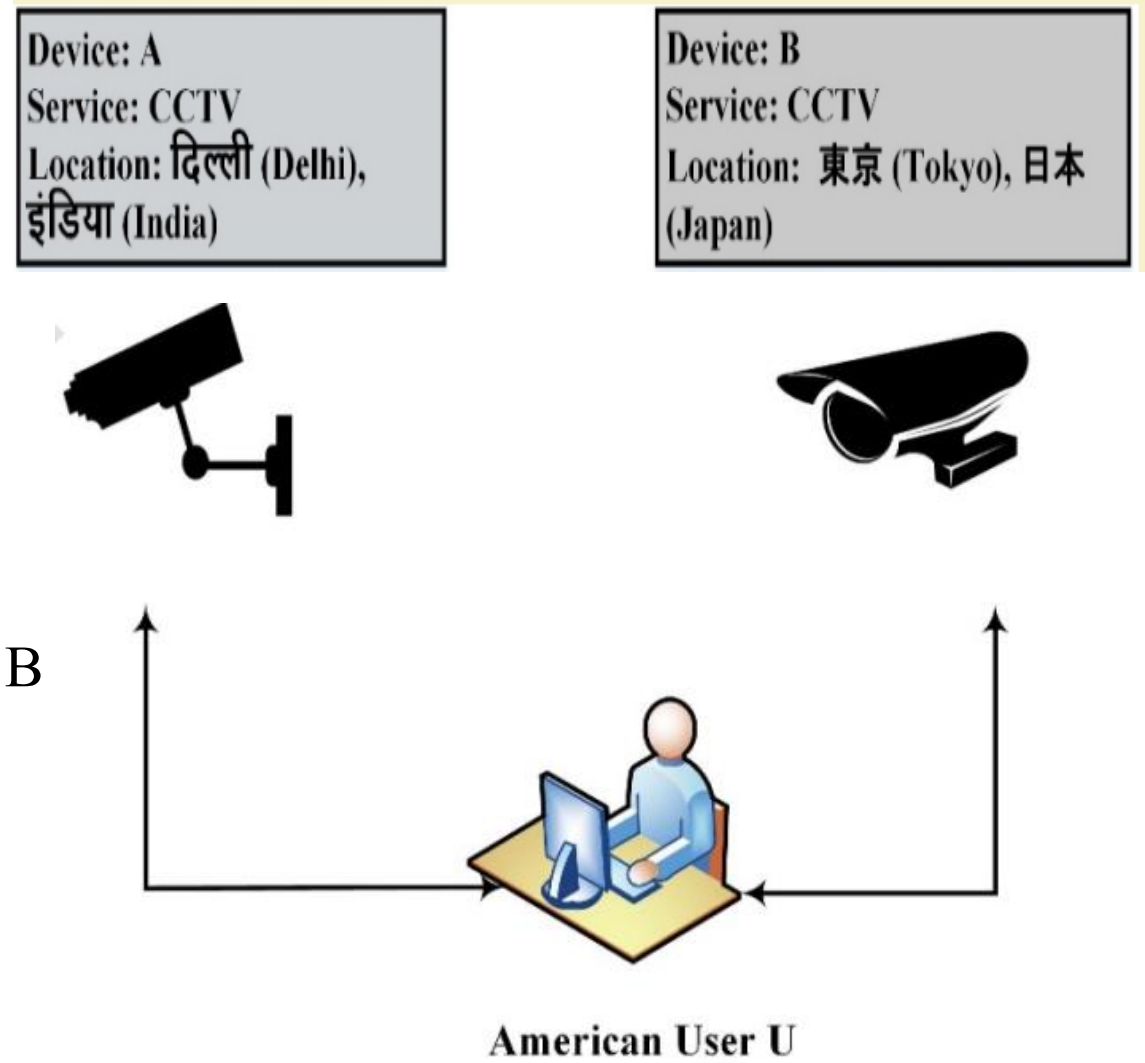
- Using IoT, both A and B provide a real-time security service
- A is placed at Delhi, India, while B is placed at Tokyo, Japan
- A, B, U use Hindi, Japanese, and English language, respectively.
- User U wants real-time service of CCTV camera from the device A and B .



Example of Device and User Interoperability

Problems are listed below

- The user U does not know the devices A and B.
- Devices A and B are different in terms of syntactic and semantic notions
- Therefore, it is difficult to find CCTV device
- User U can’t understand the service provided by A and B
- Similarly, A and B do not mutually understand each other



User Interoperability

The following problems need to be solved

- Device identification and categorization for discovery
- Syntactic interoperability for device interaction
- Semantic interoperability for device interaction

Device identification and categorization for discovery

There are different solutions for generating unique address

- Electronic Product Codes (EPC)
- Universal Product Code (UPC)
- Uniform Resource Identifier (URI)
- IP Addresses (IPv6)

Device identification and categorization for discovery (Contd.)

There are different device classification solutions

- United Nations Standard Products and Services Code (UNSPSC)

✓An open, global, multi-sector standard for efficient, accurate, flexible classification of products and services.

- eCl@ss

✓The standard is for classification and clear description of cross-industry products

Syntactic Interoperability for Device Interaction

- The interoperability between devices and device user in term of message formats
- The message format from a device to a user is understandable for the user's computer
- On the other hand, the message format from the user to the device is executable by the device

Syntactic Interoperability for Device Interaction (Contd.)

Some popular approaches are

- Service-oriented Computing (SOC)-based architecture
- Web services
- RESTful web services
- Open standard protocols such as IEEE 802.15.4, IEEE 802.15.1, and Wireless HART*
- Closed protocols such as Z-Wave*

*But these standards are incompatible with each other

Syntactic Interoperability for Device Interaction (Contd.)

- Middleware technology

✓Software middleware bridge

✓Dynamically map physical devices with different domains

✓ Based on the map, the devices can be discovered and controlled, remotely

- Cross-context syntactic interoperability

✓Collaborative concept exchange

✓Using XML syntax

Semantic Interoperability for Device Interaction

- The interoperability between devices and device user in term of message's meaning
- The device can understand the meaning of user's instruction that is sent from the user to the device.
- Similarly, the user can understand the meaning of device's response sent from the device

Semantic Interoperability for Device Interaction (Contd.)

Some popular approaches

- Ontology
- Device ontology
- Physical domain ontology
- Estimation ontology

Ontology-based solution is limited to the defined domain/context.

Semantic Interoperability for Device Interaction (Contd.)

- Collaborative conceptualization theory

✓Object is defined based on the collaborative concept, which is called cosign

✓The representation of a collaborative sign is defined as follows:

✓cosign of a object = (A, B, C, D), where A is a cosign internal identifier, B is a natural language, C is the context of A, and D is a definition of the object

✓As an example of CCTV, cosign = (1234, English, CCTV, “Camera Type: Bullet, Communication: Network/IP, Horizontal Resolution: 2048 TVL”)

- This solution approach is applicable for different domains/contexts

Device Interoperability

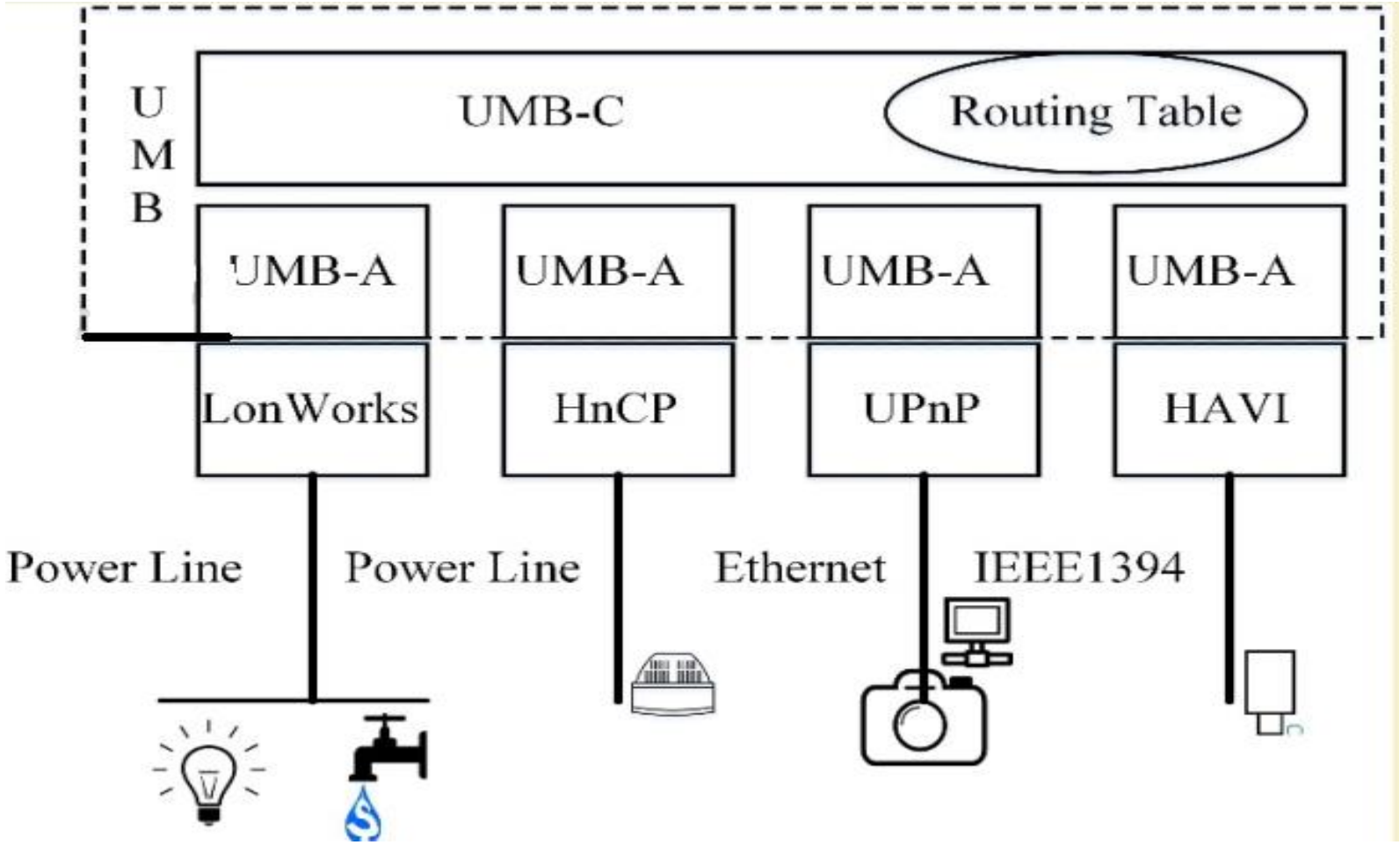
Solution approach for device interoperability

✓Universal Middleware Bridge (UMB)

- Solves seamless interoperability problems caused by the heterogeneity of several kinds of home network middleware
- UMB creates virtual maps among the physical devices of all middleware home networks, such as HAVI, Jini, LonWorks, and UPnP
- Creates a compatibility among these middleware home networks

Device Interoperability (Contd.)

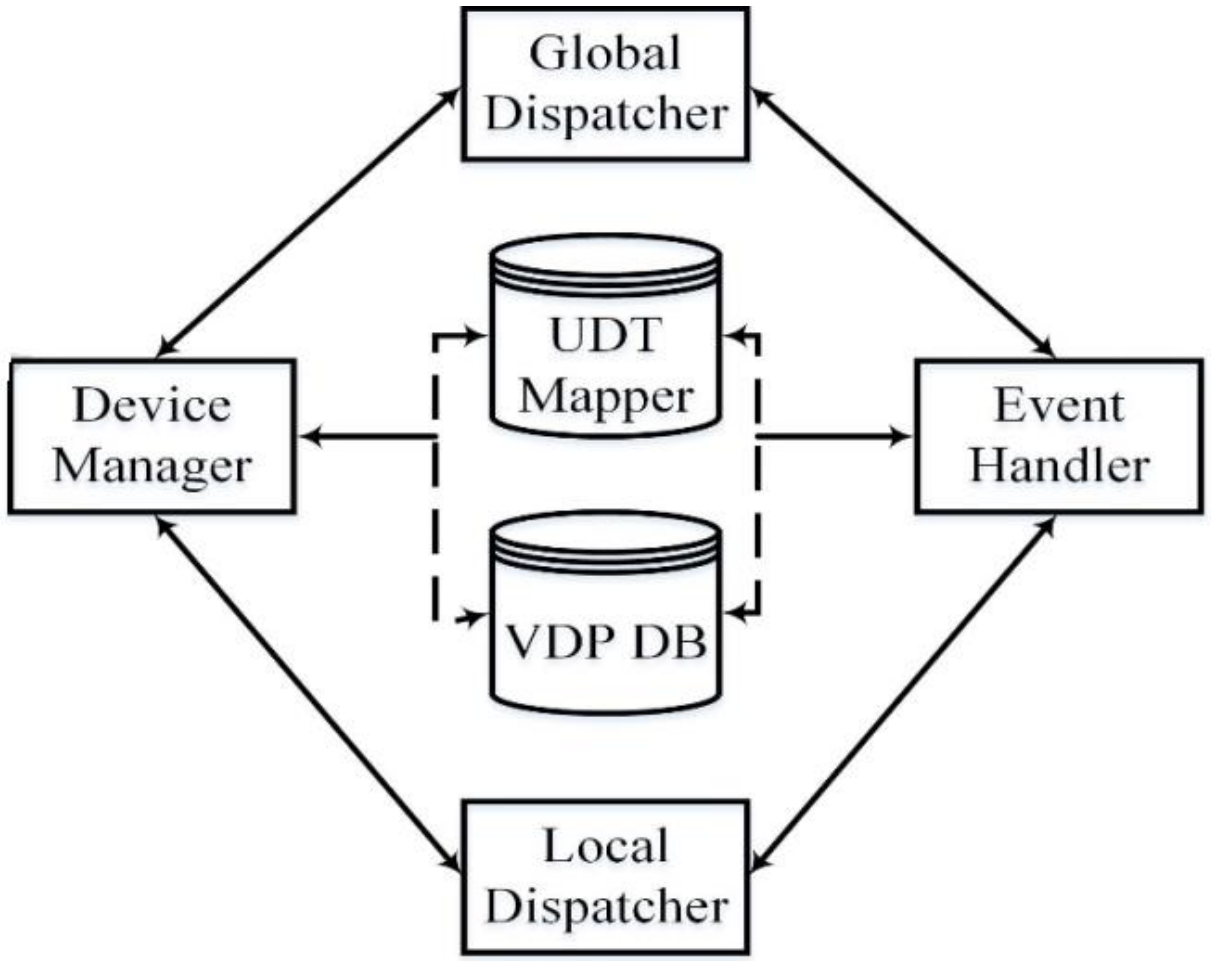
- UMB consists
  - UMB Core (UMB-C)
  - UMB Adaptor (UMB-A)



Device Interoperability (Contd.)

UMB Adaptor

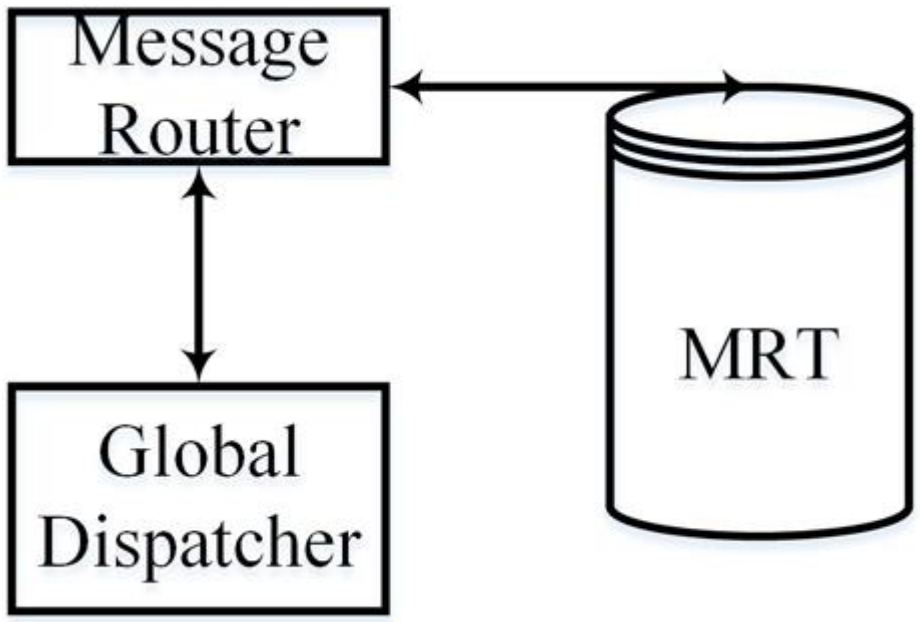
- UMB-A converts physical devices into virtually abstracted one, as described by Universal Device Template(UDT).
- UDT consists of a Global Device ID, Global Function ID, Global Action ID, Global Event ID, and Global Parameters.
- UMB Adaptors translate the local middleware's message into global metadata's message



Device Interoperability (Contd.)

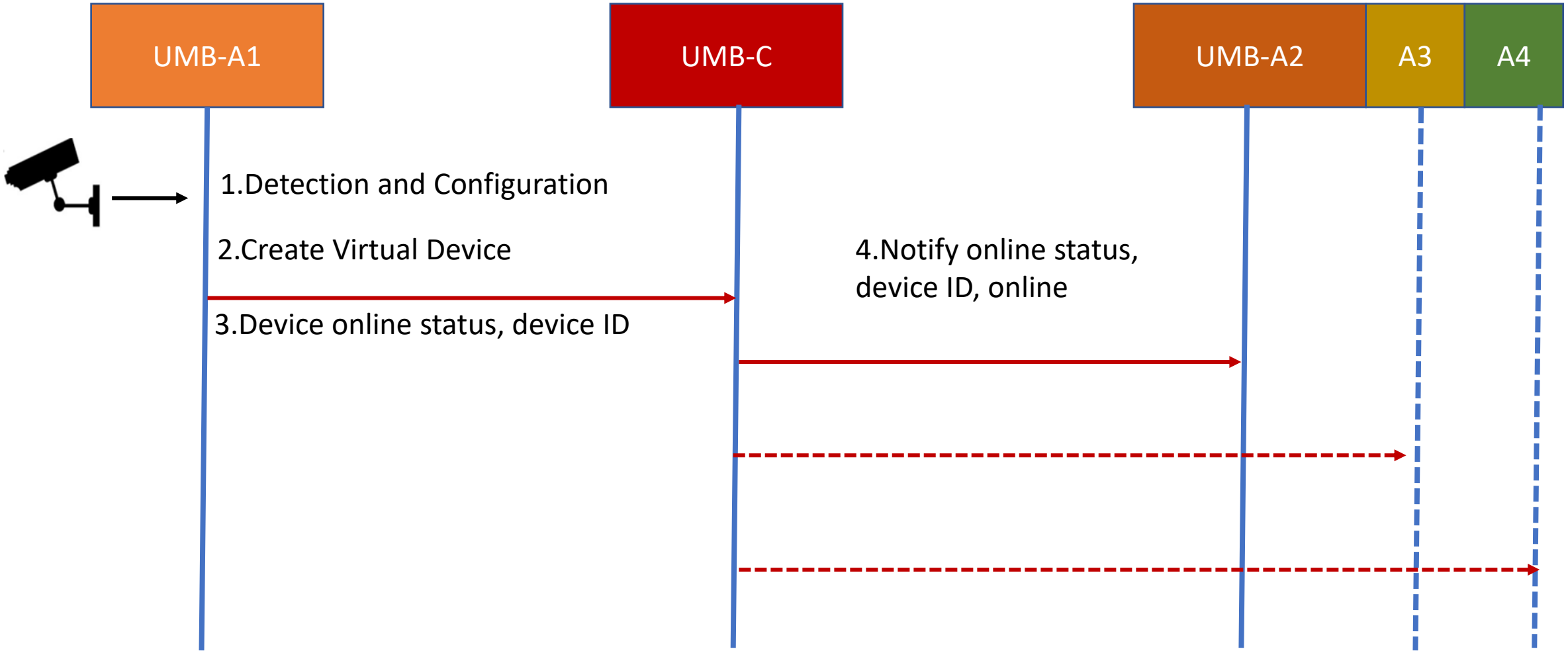
UMB Core

- The major role of the UMB Core is routing the universal metadata message to the destination or any other UMB Adaptors by the Middleware Routing Table (MRT).



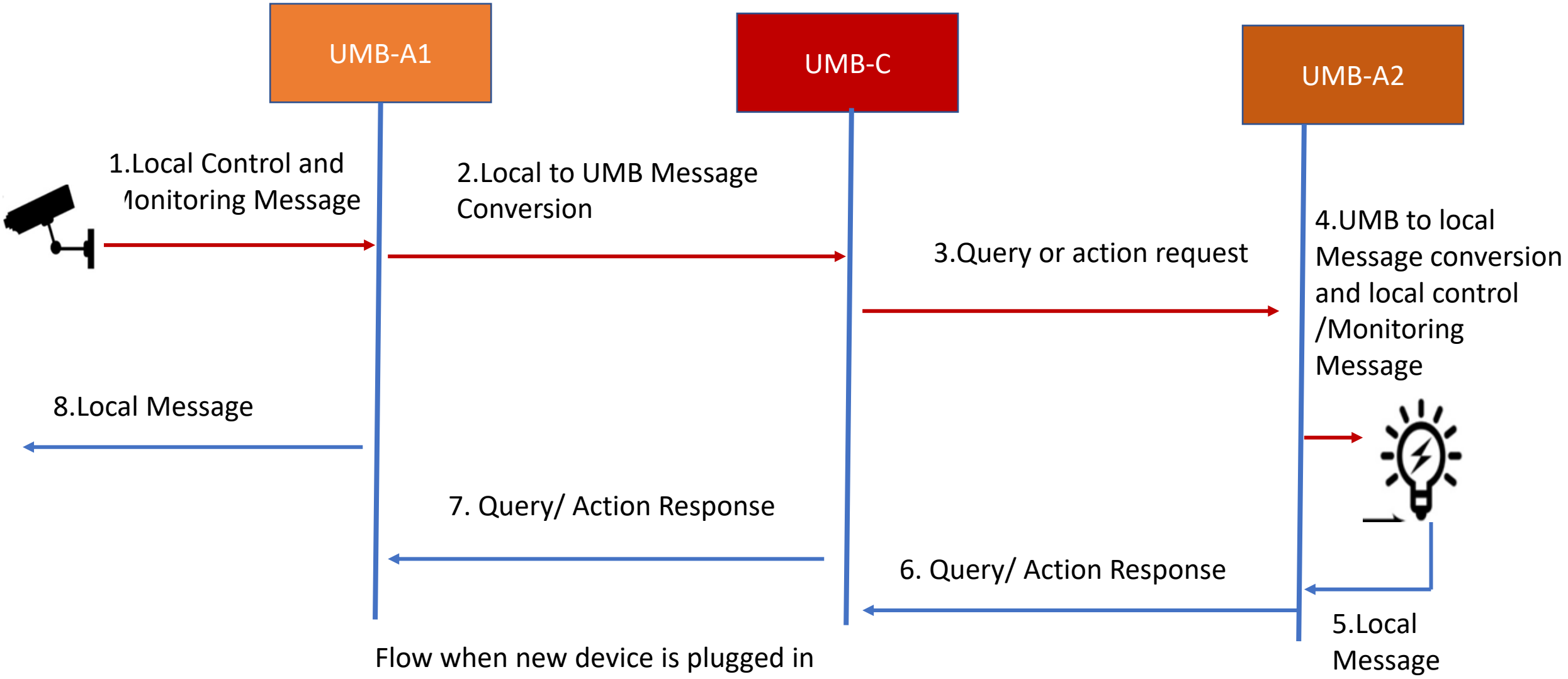
The Structure of UMB-C

Device Interoperability (Contd.)



Flow when new device is plugged in

Device Interoperability (Contd.)



Flow when new device is plugged in

THANK YOU

Emergence of IoT Healthcare

Advances in sensor and connectivity

- Collect patient data over time
- Enable preventive care
- Understanding of effects of therapy on a patient
- Ability of devices to collect data on their own
- Automatically obtain data when and where needed by doctors
- Automation reduces risk of error
- Lower error implies increased efficiency and reduced cost

Components of IoT Healthcare

Components of IoT is organized in 4 layers

- Sensing layer: Consists of all sensor, RFIDs and wireless sensor networks (WSN). E.g: Google glass, Fitbit tracker
- Aggregated layer: Consists of different types of aggregators based on the sensors of sensing layer. E.g: Smartphones, Tablets
- Processing layer: It consists of servers for processing information coming from aggregated layer.
- Cloud platform: All processed data are uploaded in cloud platform, which can be accessed by large number of users

Components of IoT Healthcare

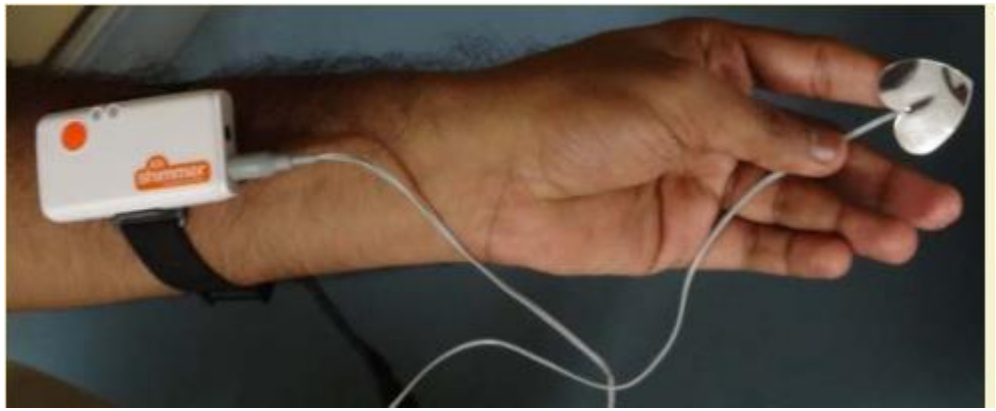
Sensing and Measurement

Data Aggregation

Cloud storage & Analytics

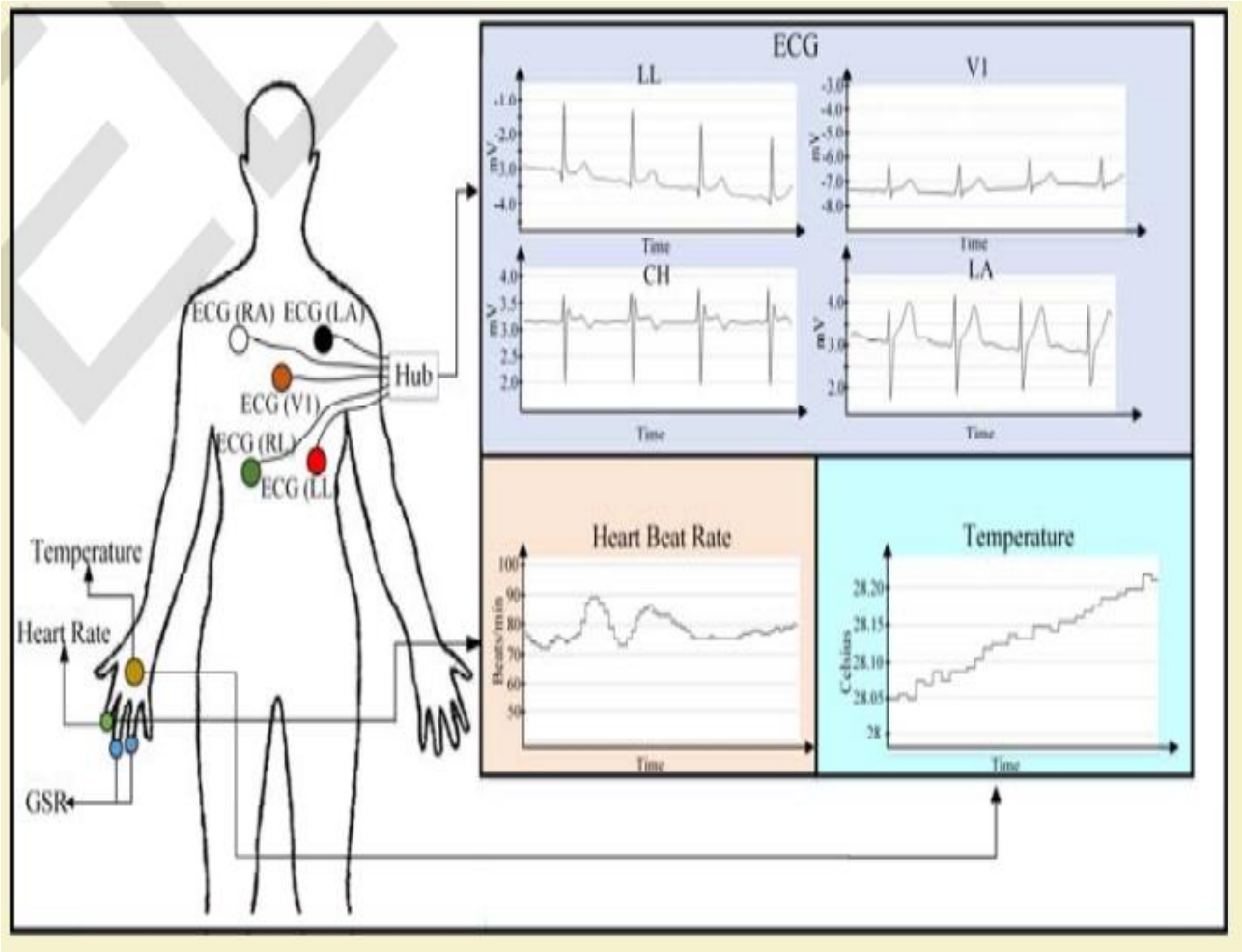
IoT Healthcare : Remote Healthcare

- Many people without ready access to effective healthcare
- Wireless IoT driven solutions bring healthcare to patients rather than bring patients to healthcare
- Securely capture a variety of medical data through IoT based sensors, analyze data with smart algorithms
- Wirelessly share data with health professionals for appropriate health recommendations



IoT Healthcare : Real-time Monitoring

- IoT-driven non-invasive monitoring
- Sensors to collect comprehensive physiological information
- Gateways and cloud-based analytics and storage of data
- Wirelessly send data to caregivers
- Lowers cost of healthcare



IoT Healthcare : Preventive care

- Fall detection for seniors
- Emergency situation detection and alert to family members
- Machine learning for health trend tracking and early anomaly detection

Case Studies on IoT

- Health Care IoT
- Vehicular IoT
- Agriculture IoT

Architecture of Health Care IoT

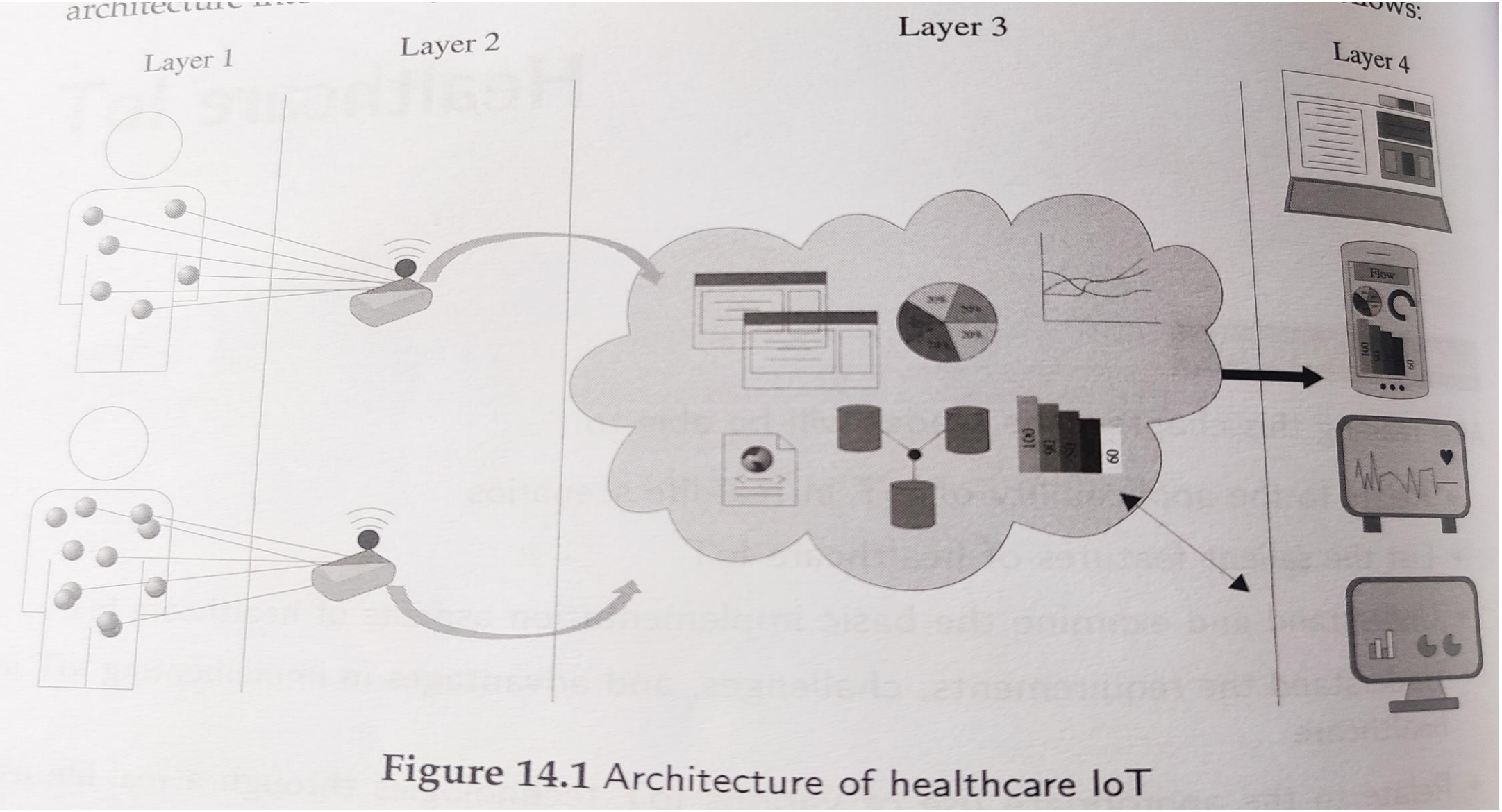


Figure 14.1 Architecture of healthcare IoT

Components of healthcare IoT

Sensors	Sense the physiological parameter value from a patient body
Wireless Connectivity	Transmit data from sensors to LPU and LPU to cloud/server
Privacy and Security	Secure the sensitive health data
Analytics	Extract a meaningful inference from data and apply them in an application
Cloud and Fog Computing	Store the data for short term and long term basis for future use
Interface	Provide an easy access the application

Emergence of IoT Healthcare

Advances in sensor and connectivity

- Collect patient data over time
- Enable preventive care
- Understanding of effects of therapy on a patient
- Ability of devices to collect data on their own
- Automatically obtain data when and where needed by doctors
- Automation reduces risk of error
- Lower error implies increased efficiency and reduced cost

Components of IoT Healthcare

Components of IoT is organized in 4 layers

- Sensing layer: Consists of all sensor, RFIDs and wireless sensor networks (WSN). E.g: Google glass, Fitbit tracker
- Aggregated layer: Consists of different types of aggregators based on the sensors of sensing layer. E.g: Smartphones, Tablets
- Processing layer: It consists of servers for processing information coming from aggregated layer.
- Cloud platform: All processed data are uploaded in cloud platform, which can be accessed by large number of users

Components of IoT Healthcare

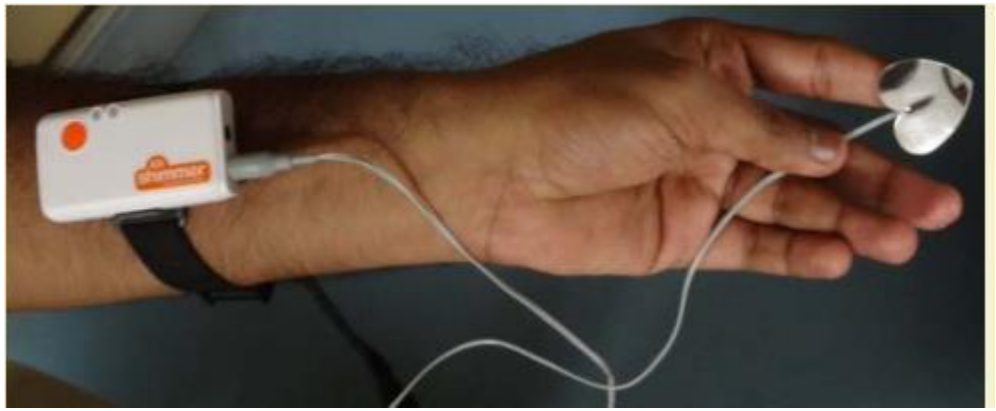
Sensing and Measurement

Data Aggregation

Cloud storage & Analytics

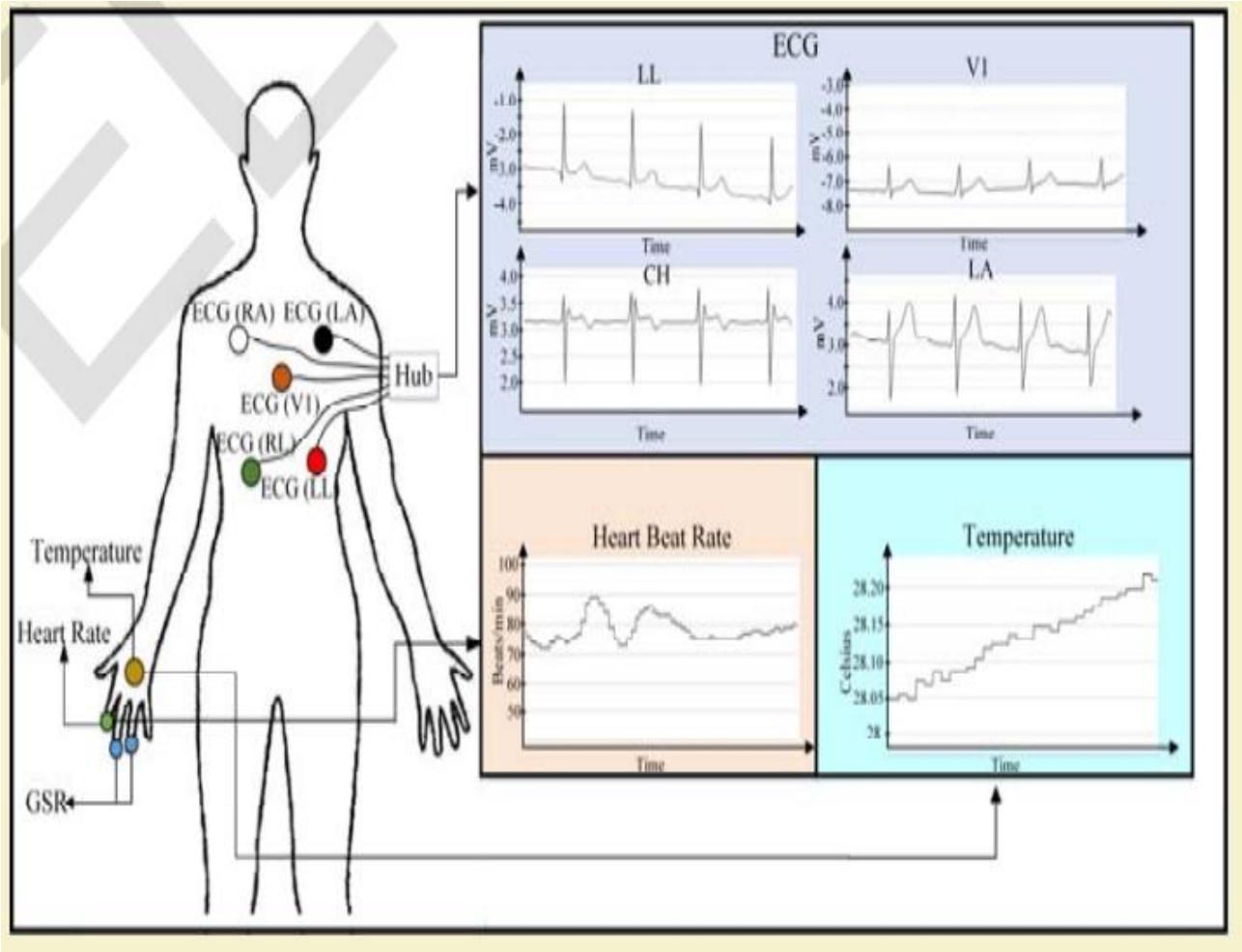
IoT Healthcare : Remote Healthcare

- Many people without ready access to effective healthcare
- Wireless IoT driven solutions bring healthcare to patients rather than bring patients to healthcare
- Securely capture a variety of medical data through IoT based sensors, analyze data with smart algorithms
- Wirelessly share data with health professionals for appropriate health recommendations



IoT Healthcare : Real-time Monitoring

- IoT-driven non-invasive monitoring
- Sensors to collect comprehensive physiological information
- Gateways and cloud-based analytics and storage of data
- Wirelessly send data to caregivers
- Lowers cost of healthcare



IoT Healthcare : Preventive care

- Fall detection for seniors
- Emergency situation detection and alert to family members
- Machine learning for health trend tracking and early anomaly detection

Advantages of Health Care IoT

- Real time
- Low Cost
- Easy Management
- Automatic Processing
- Easy record keeping
- Easy diagnosis

Risk of Healthcare IoT

- Loss of Connectivity
- Security
- Error

Vehicular IoT

Architecture of Vehicular IoT

Cloud

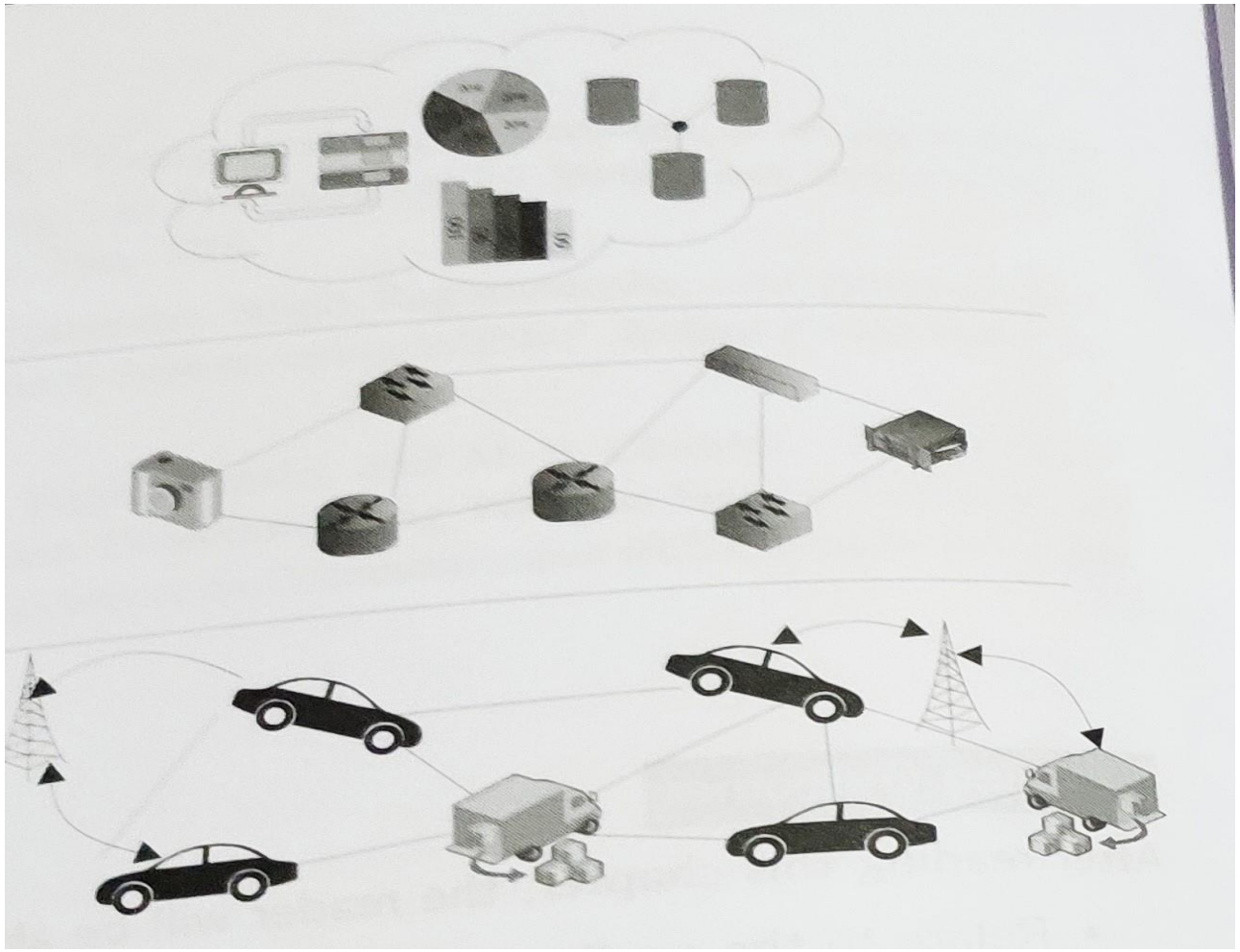
- High end Processing
- Heavy Analytics
- Long Term Storage
- Decision Making

Fog

- Low end Processing
- Small scale Analytics
- Short term storage
- Decision Making near the device

Device

- Vehicle internal environment sensing
- External environment sensing
- Data collection and sharing
- Event triggering



Vehicular IoT

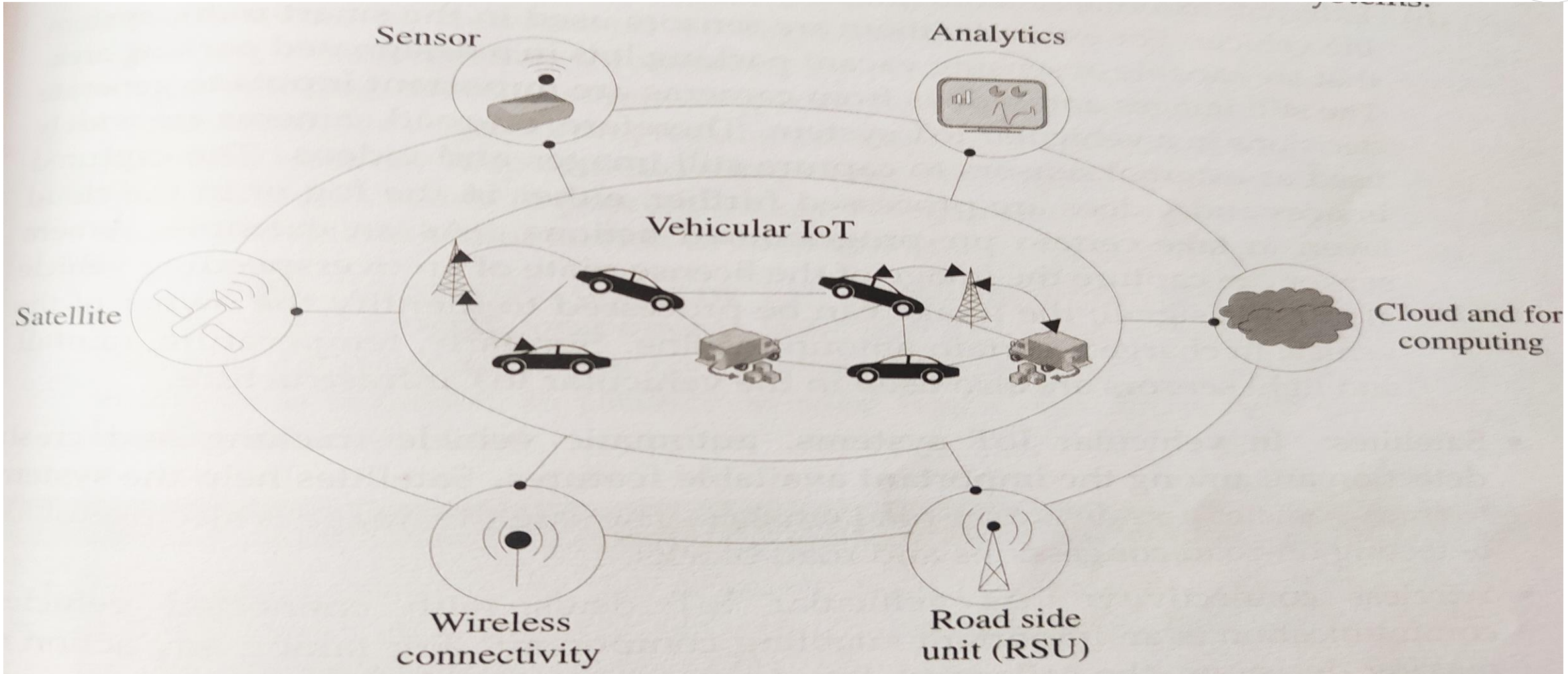


Figure 13.2 Components of vehicular IoT

Vehicular IoT

Advantages

- Easy tracking
- Fast Decision Making
- Connected vehicles
- Easy Management
- Safety
- Record

Agriculture IoT

Agriculture IoT

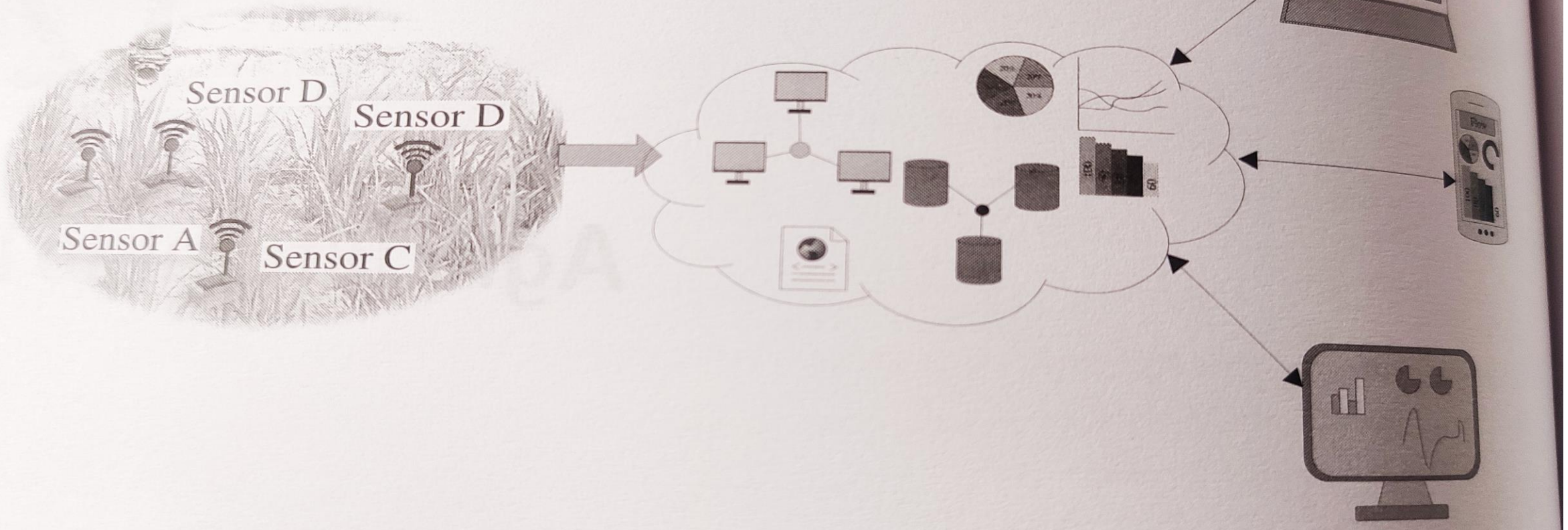


Figure 12.1 Architecture of agricultural IoT

Agriculture IoT

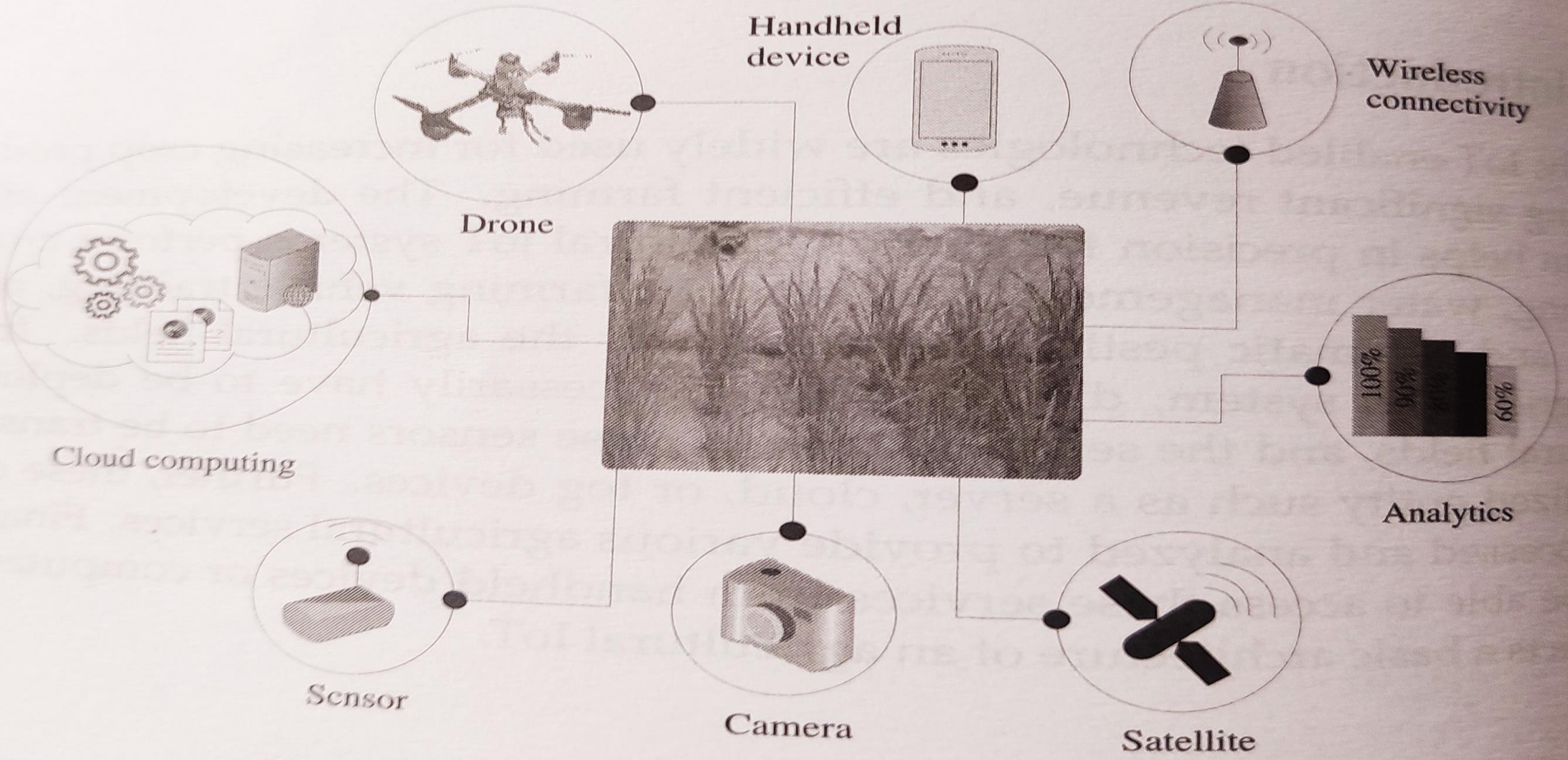


Figure 12.2 Components of agricultural IoT

Agriculture IoT

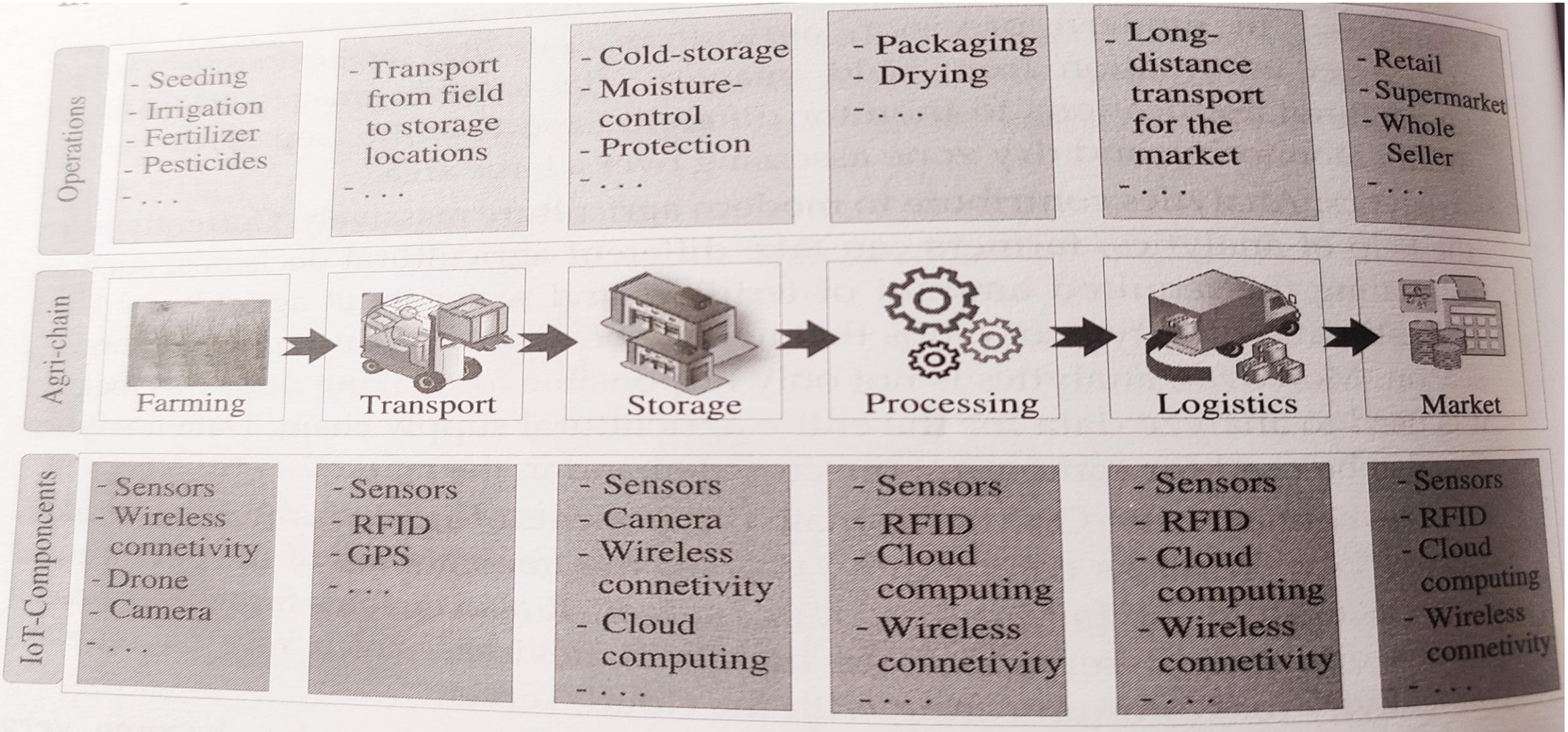


Figure 12.3 Use of IoT components in the agricultural chain

Agriculture IoT

Advantages

- Automatic seeding
- Efficient fertilizer and pesticide distribution
- Water Management
- Real time and Remote Monitoring
- Easy yield estimation
- Production overview

Agriculture IoT

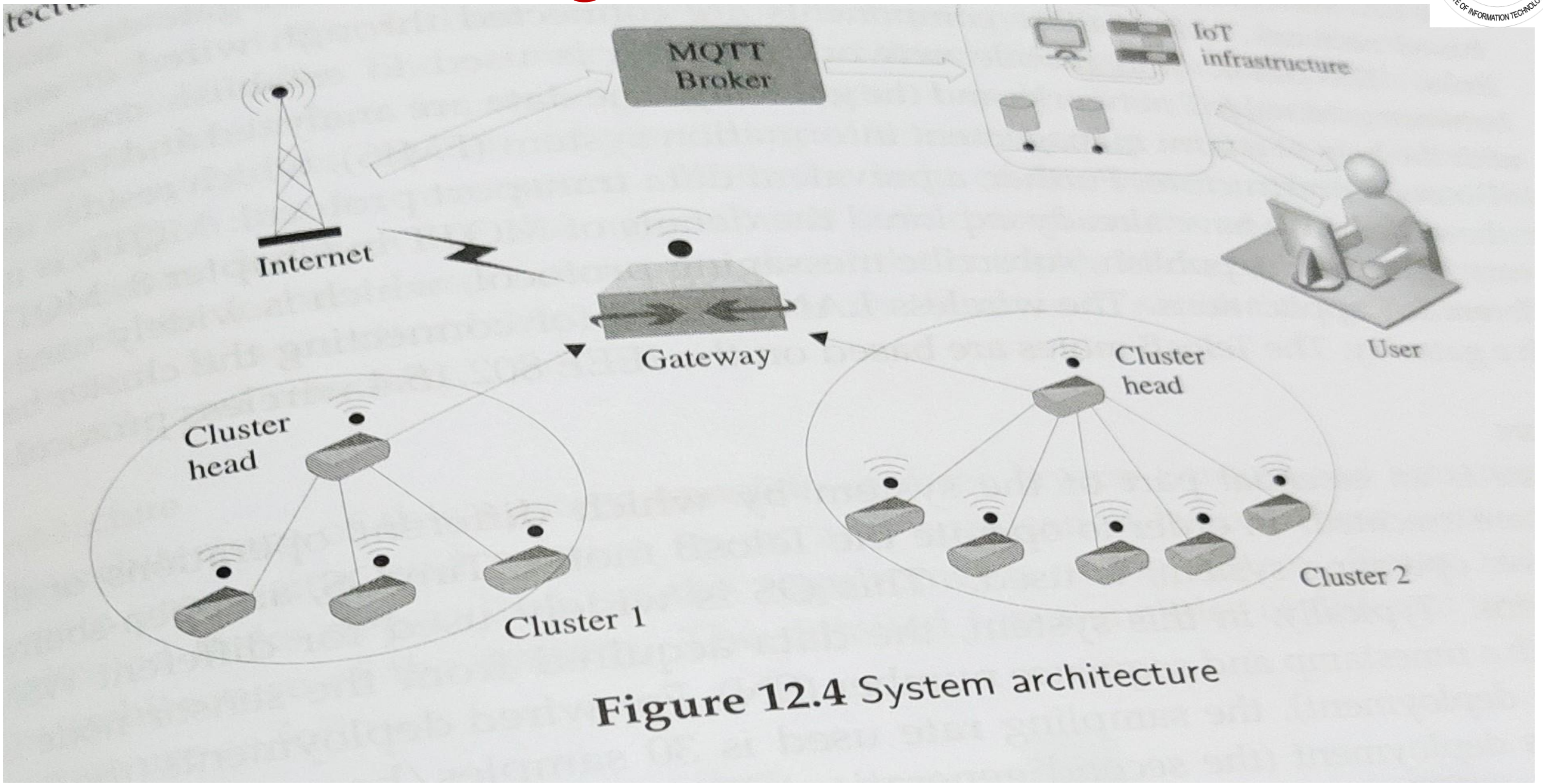


Figure 12.4 System architecture

Agriculture IoT

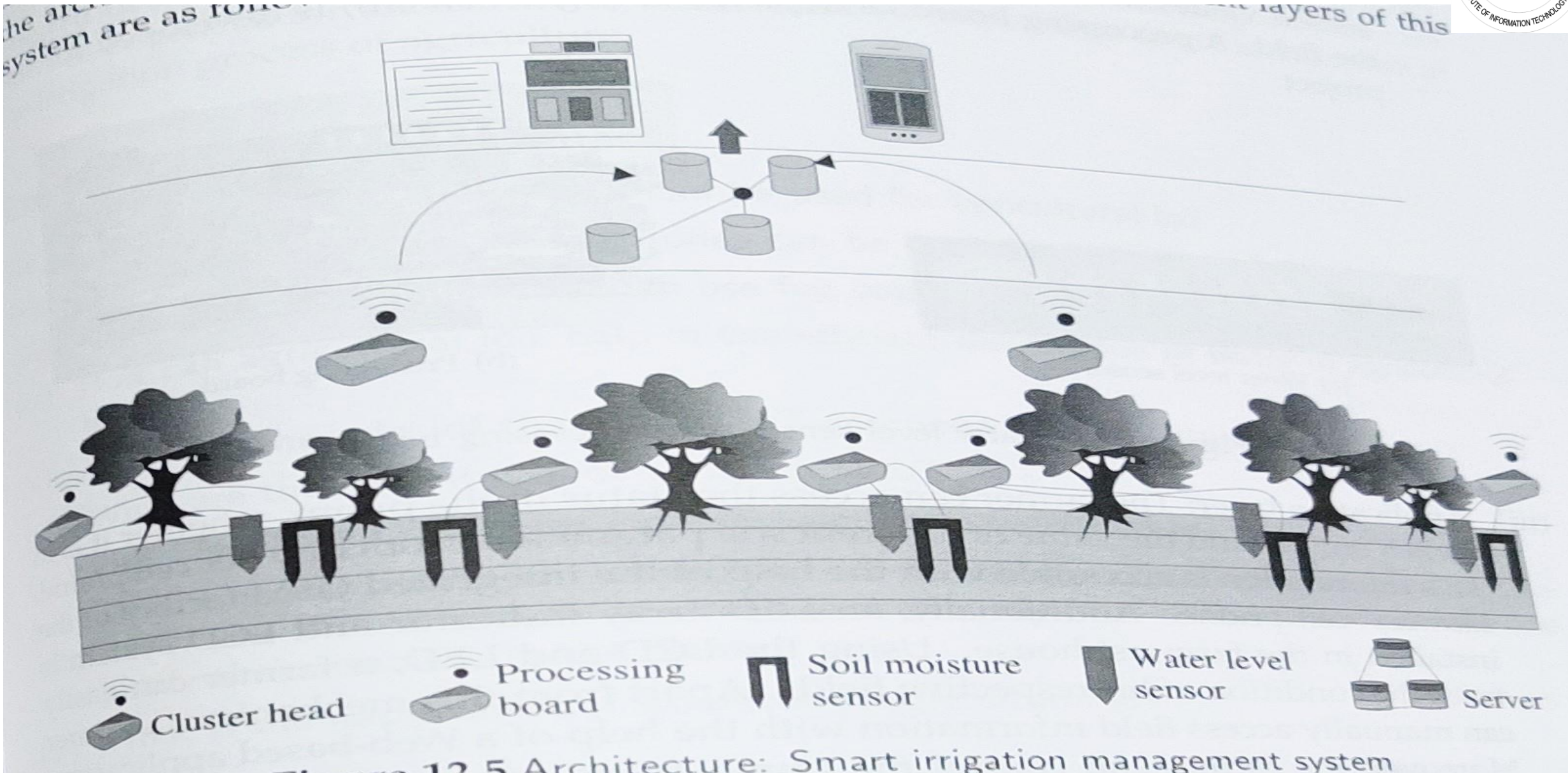


Figure 12.5 Architecture: Smart irrigation management system

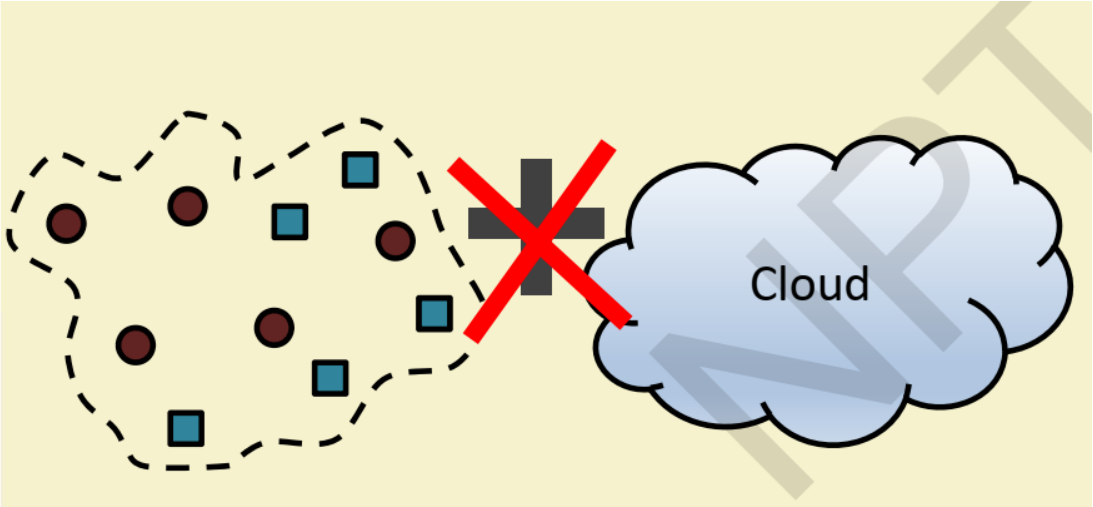
THANK YOU

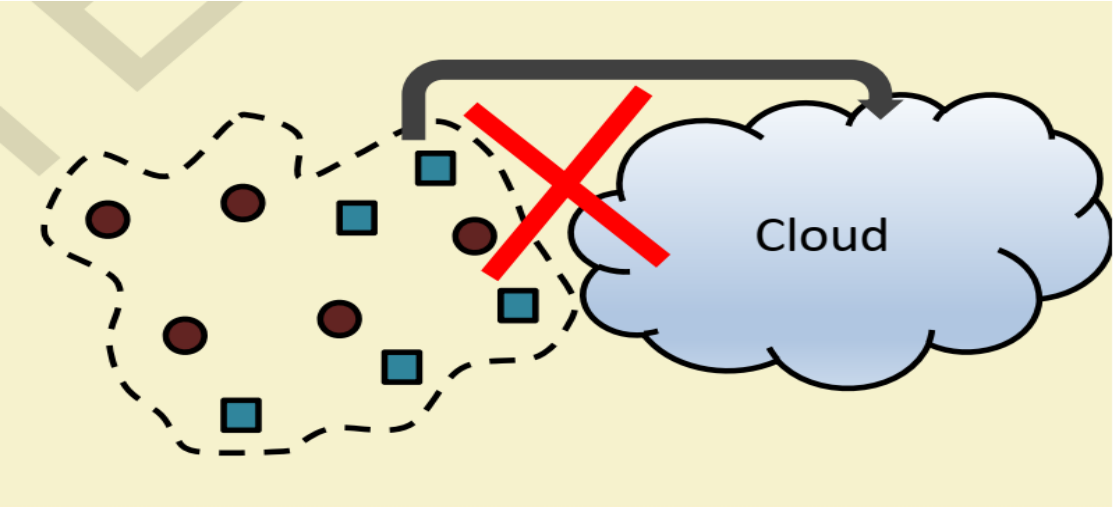
Sensor-Cloud

Introduction

- It is not a integration of sensors and cloud computing.

- It is not only “dumping the sensor data into cloud”

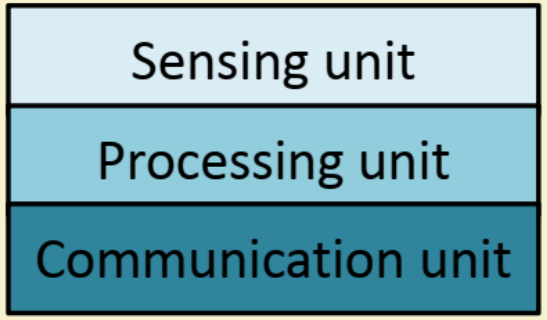




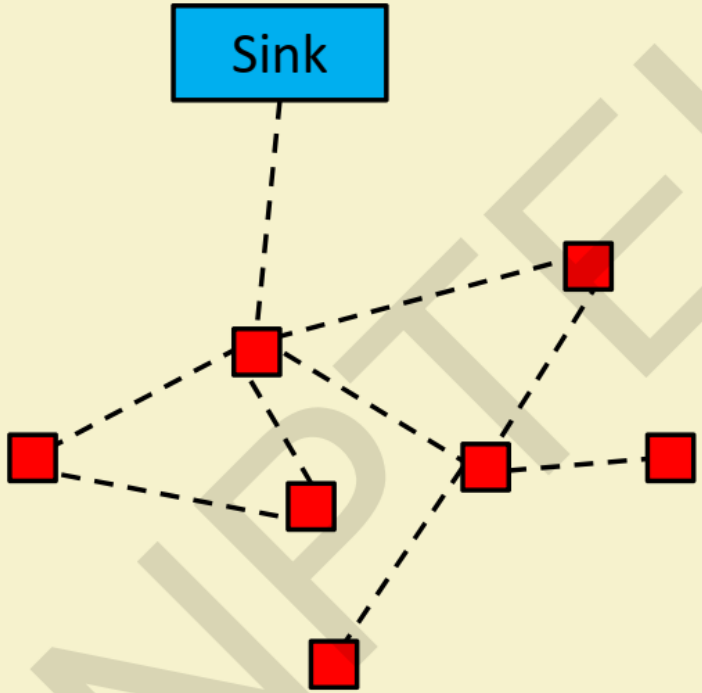
Wireless Sensor Networks (WSNs)

- Contain sensor nodes which sense some physical phenomena from the environment.
- Transmit the sensed data (through wireless communication) to a centralized unit, commonly known as Sink node.
- The communication between Sink node and other sensor nodes in the network may be single/multi-hop.
- Sink node further process data.

Wireless Sensor Networks (WSNs)



Major Components of a Sensor Node



Wireless Sensor Networks

Applications

- ✓ Target Tracking
- ✓ Wildlife Monitoring
- ✓ Healthcare
- ✓ Industrial Applications
- ✓ Smart Home
- ✓ Smart City
- ✓ Agriculture
- ✓ …

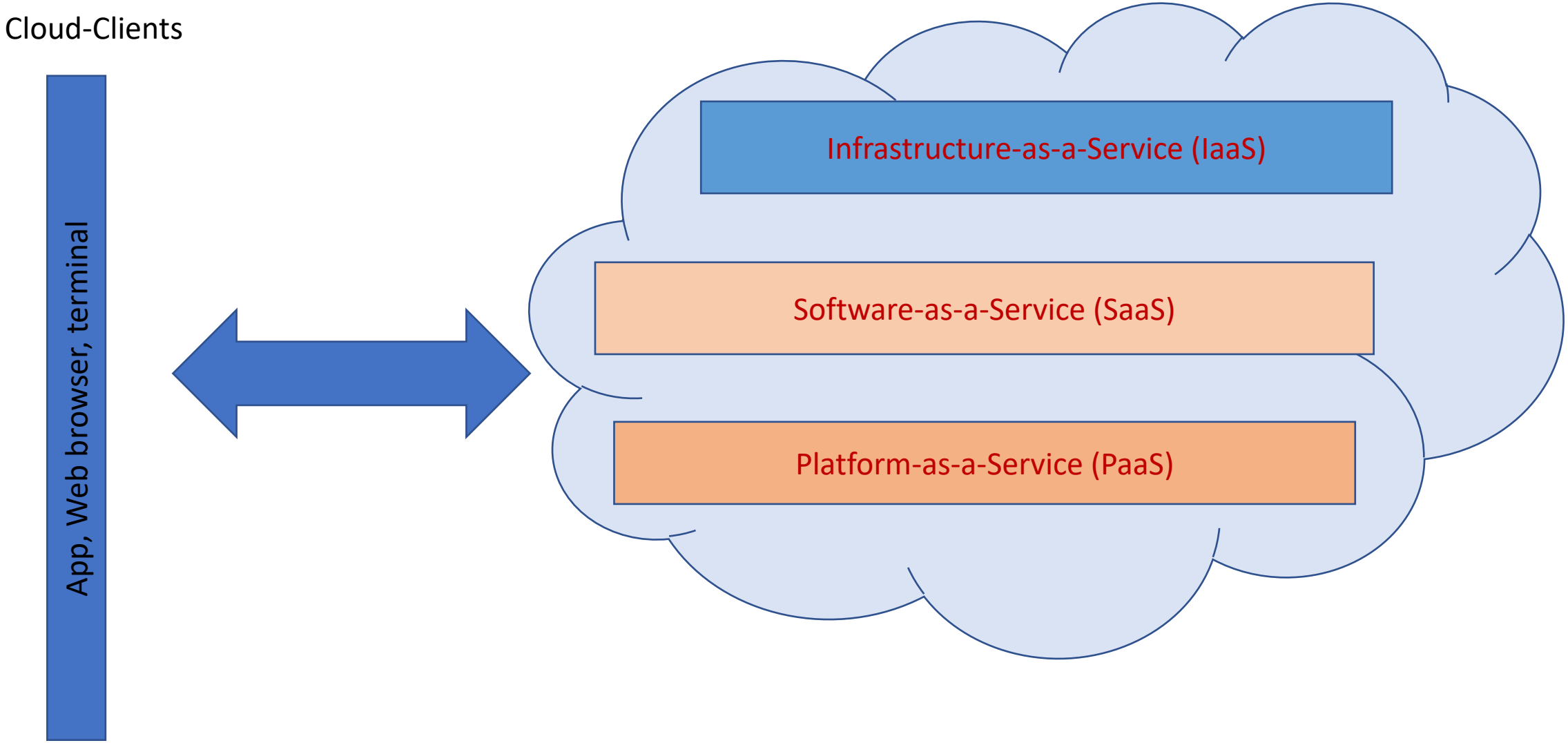
NPTEL

Cloud Computing

- An architecture which provides on-demand computing resources.

- Advantages
  - ✓Elasticity: Scaling up/down
  - ✓Pay-per-use: Payment for the resource as per requirement
  - ✓Self Service: Resource can be accessed by self

Cloud Computing: Services



Cloud Computing: Services

- Software-as-a-Service (SaaS)

✓ A third party provides a host application over internet

✓ Example: Microsoft Office 365

- Platform-as-a-Service (PaaS)

✓Provide a platform to develop and run applications

✓Example: Windows Azure

- Infrastructure-as-a-Service (IaaS)

✓Provide computing resources

✓Example: Storage space

Virtualization Concept

- One computer host appears as many computers-concept of Virtual Machine (VM)

- Improve IT throughput and costs by using physical resources as a pool from which virtual resources can be allocated.

- Benefit
  - ✓Sharing of resources: Same resource can be shared, in turn cost reduction
  - ✓Encapsulation: A complete computing environment
  - ✓Independence: Runs independently of underlying hardware
  - ✓Portability: VM Migration

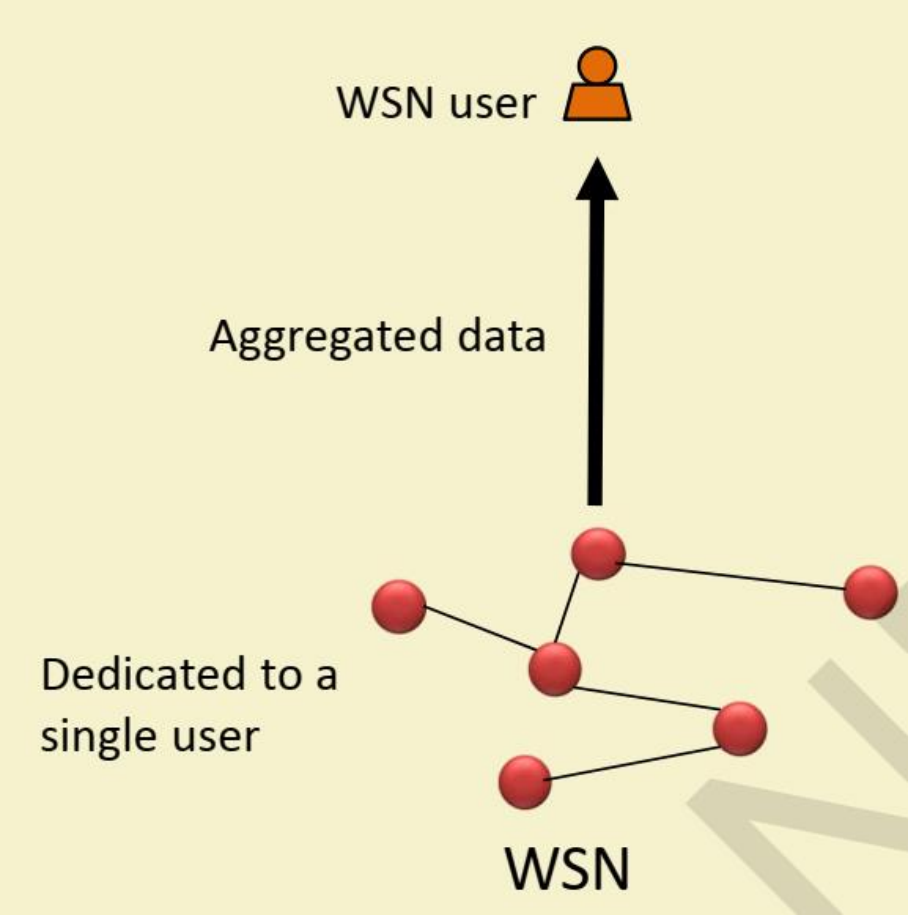
Limitations of WSNs

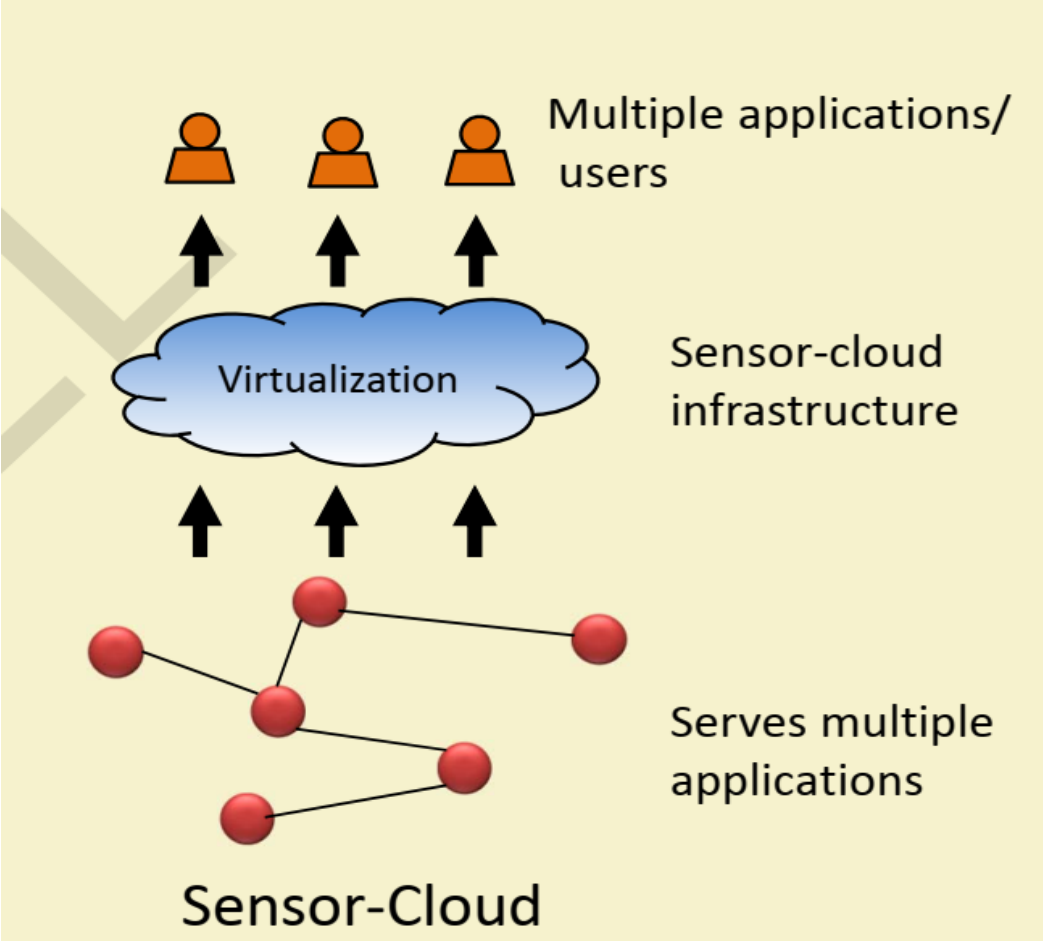
- Procurement
- Price
- Right vendor
- Types of sensor integrated with it
- Deployment
- Right way of deployment
- Right place of deployment
- Maintenance
- Post deployment maintenance
- Battery lifetime

Sensor-Cloud: Introduction

- Not only the integration of cloud computing and sensor networks, but sensor-cloud is more than that
- Concept of virtualization of sensor node
- Pay-per-use
- One sensor node/network appears as many
- A stratum between sensor nodes and end-users

Difference with WSN





Difference with WSN

Actors and Roles		
Attributes	**WSN**	**Sensor Cloud**
Ownership	WSN-user	Sensor-owner
Deployment	WSN-user	Sensor-owner
Redeployment	WSN-user	SCSP
Maintenances	WSN-user	SCSP
Overhead	WSN-user	SCSP
Usage	WSN-user	End-user

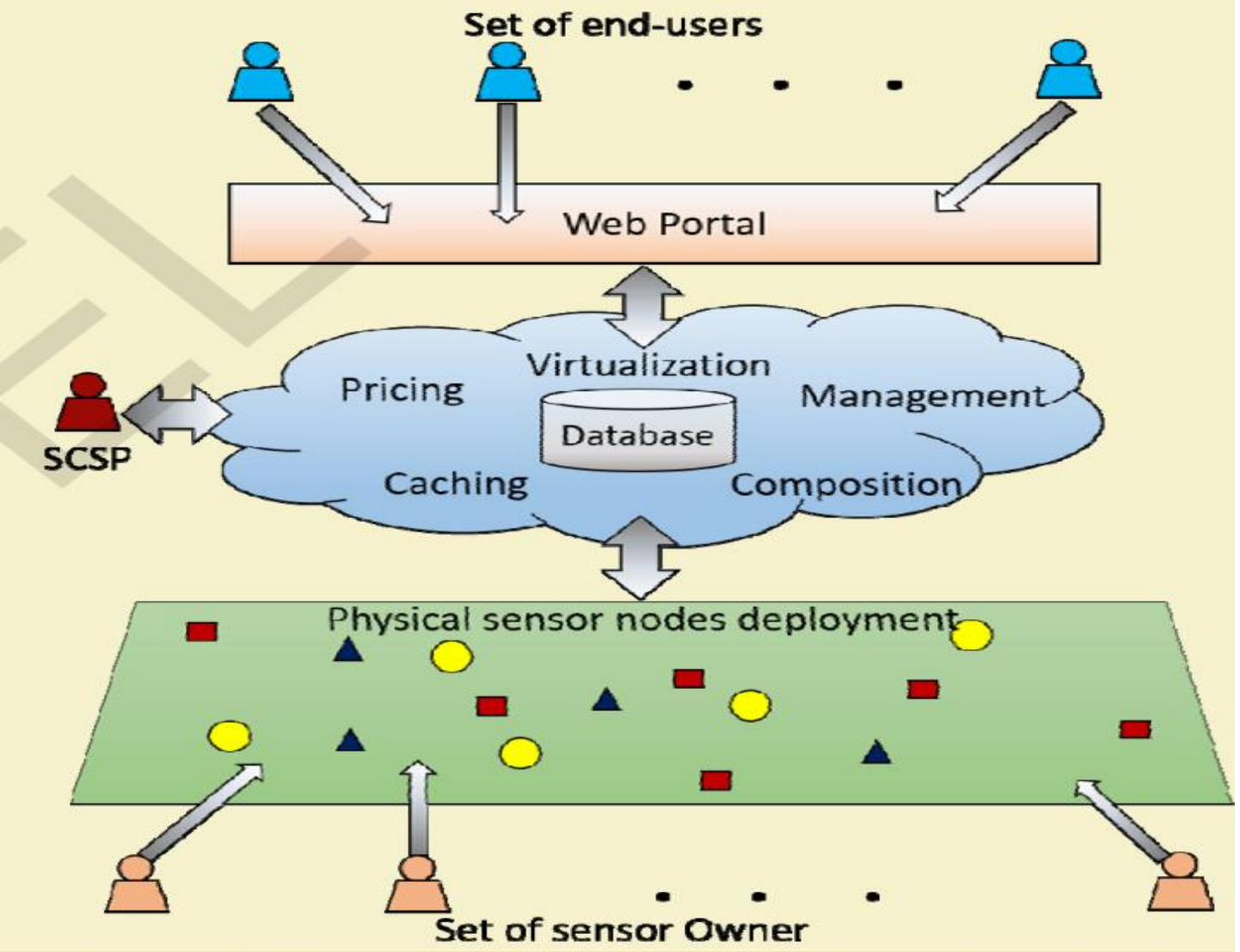
NPTEL

Actors in Sensor-cloud

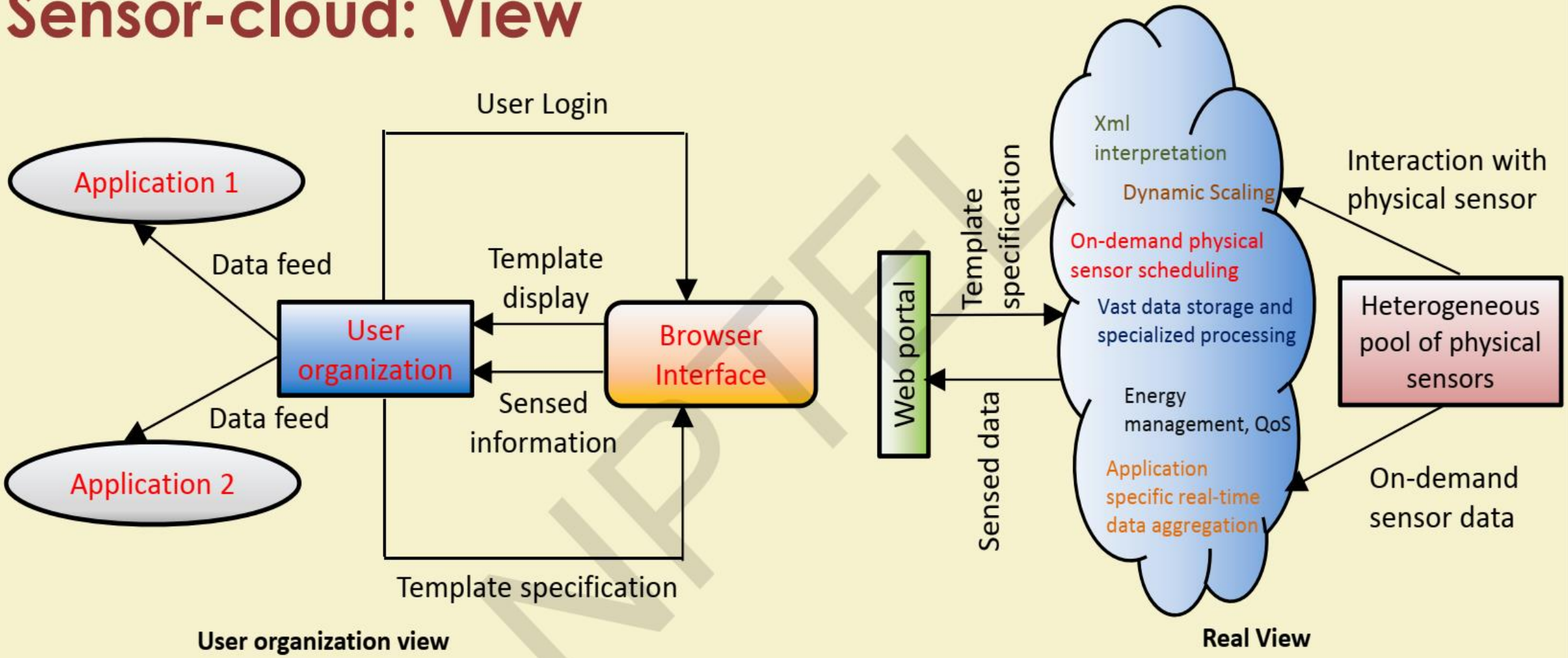
- End-users
  - ✓Enjoy Se-aaS through applications as per the requirements.
  - ✓Unknown about what and which physical sensor is/are allocated to serve the application
- Sensor-owner
  - ✓Plays a role from business perspective.
  - ✓They purchase physical sensor devices, deployed over different geographical locations, and lend these devices to the sensor-cloud
- Sensor-Cloud Service Provider (SCSP)
  - ✓A business actor.
  - ✓SCSP charges price from the end-users as per their usage of Se-aaS.

Sensor-cloud: Architecture

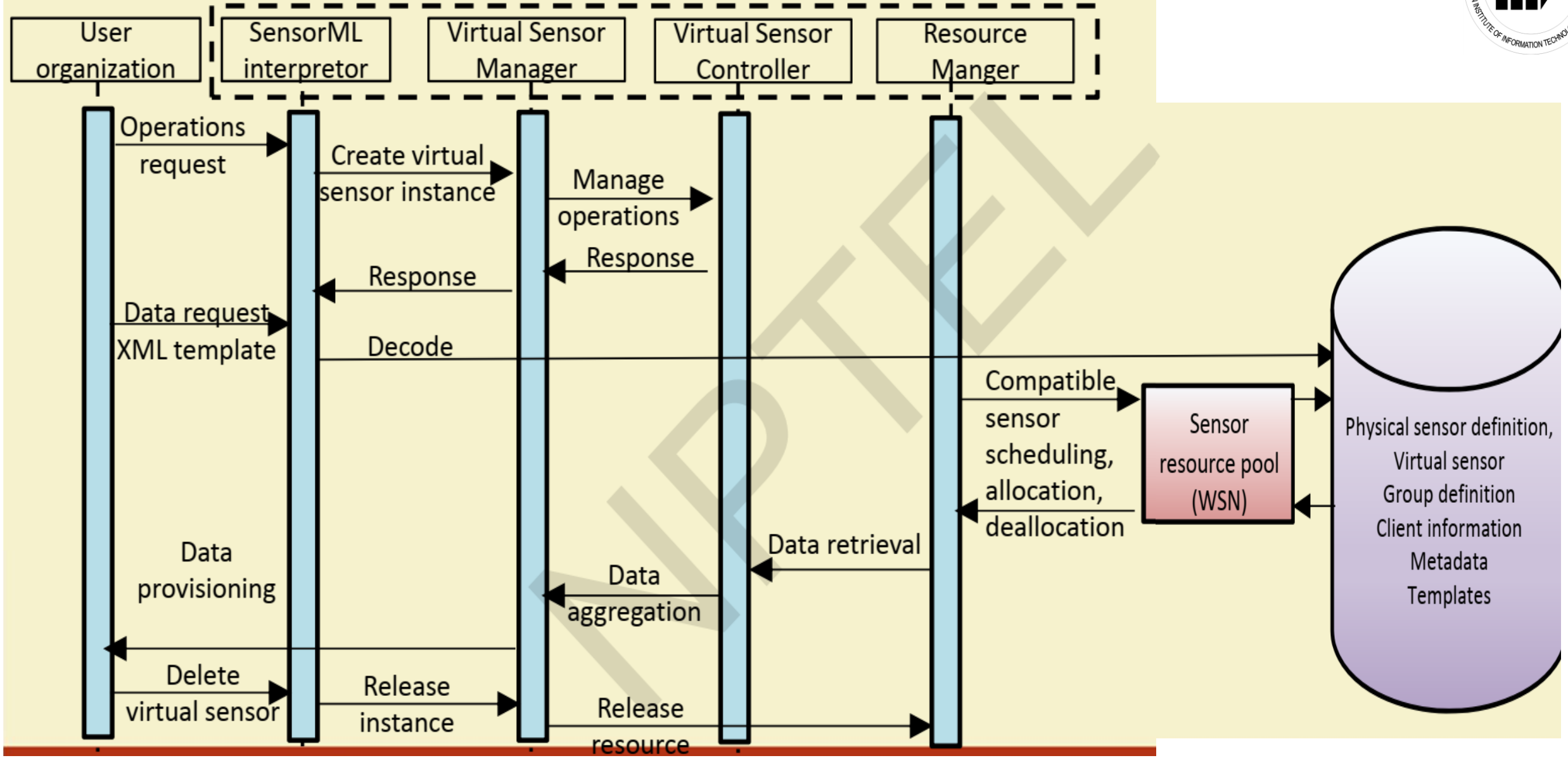
- End-users: Registered themselves, selects templates, and request for application(s)
- Sensor-owner: Deploy heterogeneous/ homogeneous physical sensor nodes over different geographical location
- SCSP: Plays managerial role



Sensor-cloud: View



Work Flow of Sensor-Cloud



THANK YOU

1. What is Raspberry Pi?

   Raspberry Pi is a microcomputer that we can connect with any keyboard, mouse or a monitor. Raspberry Pi is able to perform all tasks like creating word documents, spreadsheet, browsing, coding, games and much more. It is a tiny Linux computer that is used by many companies for performing all computer-based activities, learning and electronic projects. The Raspberry Pi uses a 32-bit ARM (Advanced RISC Machine) processor and was first developed by Raspberry Pi Foundation. The low cost makes it more popular among young people.

2. How does Raspberry Pi work?

   The memory card slot is used for inserting an SD card that acts as the hardware of Raspberry Pi. The USB port, HDMI port, and the audio/video port help us connect with a monitor, TV or any other device. This is how Raspberry Pi is capable of working anytime and anywhere. The processor gives the correct speed for running our computer programs all the time.

3. How is Raspberry Pi used in IoT?

   Raspberry Pi can be used as a platform to develop many Internet of Things project. It is simple to use Raspberry Pi because it uses Linux OS in a small card like a computer. It is also available in low cost. IoT, on the other hand, refers to a network of devices and software that help us to connect and exchange data. Raspberry Pi is easy to set up, so it is recommended for IoT.

4. What are the different components of Raspberry Pi Board?

   The Raspberry Pi board contains a 700 or 900 MHz processor with a minimum memory provision of 128 MB. It has an additional slot for memory card too. There is a graphics set up, USB port for connecting keyboard or mouse. Raspberry Pi comes along with an audio or video output option to connect your monitor. There is an HDMI port too for connecting with TV.

5. What are GPIO Pins used in Raspberry Pi Board?

   GPIO is the acronym for General Purpose Input Output Pin. They are more like switches on the board that gives an output voltage when high and give no voltage when turned to low. This is used in the Raspberry Pi boards to make an interface between the Raspberry Pi and all the components of the board. This enables multiple interactions and makes internal properties of devices easily available on board.

6. Can Raspberry Pi be used as an server?

   Yes, like we use Raspberry Pi for the desktop we can use it for the server as well. Raspberry Pi allows us to utilise it like a Web server that can help us create a simple site or even store data in the cloud. This can be accessed at any time. We can develop new templates without paying any monthly hosting fee. Raspberry Pi is thus an affordable

web server too. This is very suitable for small business and for people who want to learn easy web languages.

7. List the advantages and disadvantages of Raspberry Pi.

   Advantages of using Raspberry Pi

   - Small sized yet equals a supercomputer
   - The web traffic is less when it is used as a server
   - Very cost effective

   Disadvantages of using Raspberry Pi

   - Limitations in the OS used
   - Some complicated tasks may take a long time.

8. What is the language used by Raspberry Pi?

   Raspberry Pi uses Python as its official programming language. Python is one of the most user-friendly programming language used. It is also preferred by many companies for system development. Raspberry Pi helps us to quickly release our projects with Python. Raspberry Pi is preloaded with Python which has comprehensive syntax.

9. How is Raspberry Pi different from Arduino?

   Raspberry Pi uses Linux OS and is a general purpose microcomputer. It is capable of running multiple programs at a time, while the Arduino is a simple microcomputer that is capable of running one program only.

10. What is NOOBS software?

    NOOBS or New Out Of The Box Software is used for initializing Raspberry Pi for the first time. This is the easiest way possible to install Raspberry Pi anywhere. It requires no additional access for network or any imaging software. To set up Raspberry Pi, we need the NOOBS zip file which is to be downloaded. After that we can insert an SD card, connect Monitor, keyboard or mouse and start using Raspberry Pi.

Data Analytics in IoT

What is Data Analytics

- Data analytics (DA) is the process of examining data sets in order to draw conclusions about the information they contain, increasingly with the aid of specialized systems and software.

- Data analytics technologies and techniques are widely used in commercial industries to enable organizations to make more-informed business decisions and by scientists and researchers to verify or disprove scientific models, theories and hypotheses.

Types of Data Analysis

Two types of analysis.

- Qualitative Analysis
  - ✓Deals with the analysis of data that is categorical in nature.

- Quantitative Analysis
  - ✓ Quantitative analysis refers to the process by which numerical data is analyzed

Qualitative Analysis

- Data is not described through numerical values.
- Described by some sort of descriptive context such as text.
- Data can be gathered by many methods such as interviews, videos and audio recordings, field notes.
- Data needs to be interpreted.
- The grouping of data into identifiable themes.
- Qualitative analysis can be summarized by three basic principles (Seidel, 1998):
  - ✓ Notice things
  - ✓ Collect things
  - ✓ Think about things

Quantitative Analysis

- Quantitative analysis refers to the process by which numerical data is analysed.

- Involves descriptive statistics such as mean, media, standard deviation.

- The following are often involved with quantitative analysis:
  - ✓ Statistical models
  - ✓ Analysis of variables
  - ✓ Data dispersion
  - ✓ Analysis of relationships between variables
  - ✓ Contingence and correlation
  - ✓ Regression analysis
  - ✓ Statistical significance
  - ✓ Precision
  - ✓ Error limits

Comparison

Qualitative Data	Quantitative Data
Data is observed	Data is measured
Involves descriptions	Involves numbers
Emphasis is on quality	Emphasis is on quantity
Examples are color, smell, taste, etc	Examples are volume, weight, etc

Advantages

- Allows for the identification of important (and often mission-critical) trends.
- Helps businesses identify performance problems that require some sort of action.
- Can be viewed in a visual manner, which leads to faster and better decisions.
- Better awareness regarding the habits of potential customers.
- It can provide a company with an edge over their competitors

Popular Tools for IoT Application

- K-means
- Decision tree (DT)
- Random Forest (RF)
- K-nearest neighbor (KNN)
- Density based special clustering of Application with noise (DBSCAN)

K-nearest neighbor (KNN) Algorithm

1. Select a value of k, where k indicates the number of nearest sample points necessary for the application.

2. Compute the distance between the given data point to all the available training data points.

3. Sort the distances in ascending order.

4. Consider the kth nearest distances and identify the corresponding class of data points.

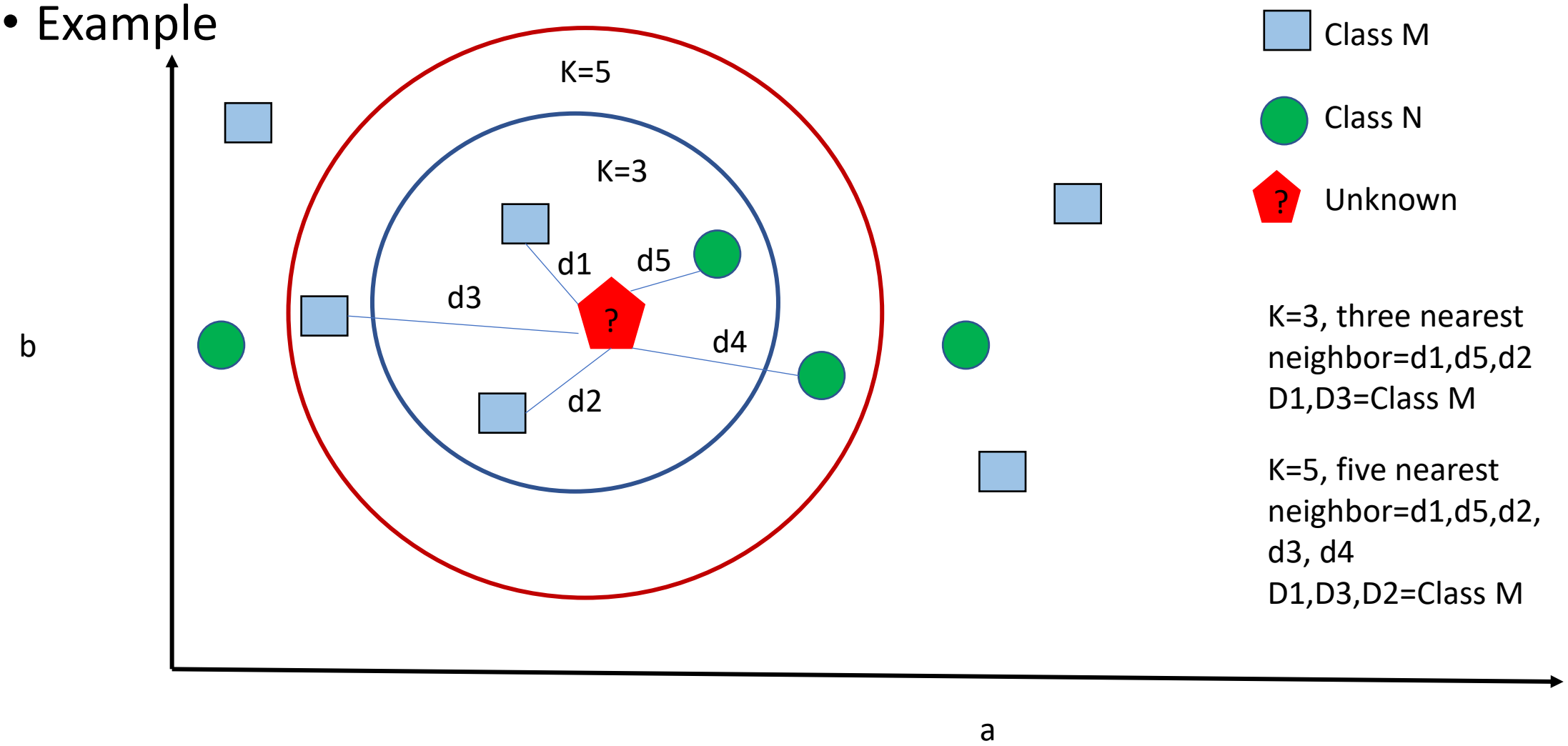
5. Identify the majority of the class of those k-nearest neighbor data points as the class of unknown data points.

K-nearest neighbor (KNN) Algorithm

Advantages	Disadvantages
Easily implementable	Noise sensitive
Easy handling of measuring data	Needs a large memory space
Do not learn during the period of training, therefore is faster compared to other ML Algorithm	Does not work well for large and high dimension data set

K-nearest neighbor (KNN) Algorithm

- Example



K=3, three nearest neighbor=d1,d5,d2
D1,D3=Class M

K=5, five nearest neighbor=d1,d5,d2, d3, d4
D1,D3,D2=Class M

THANK YOU

Basics of Networking

Networking

- **Connected entity with specific application**

- **Linking of computers and communication network devices (Switches, routers, and wireless access points), which interconnect through a network(Internet/Intranet) and are separated by unique device identifiers (Internet protocol, IP address, MAC Address)**

- **Network devices may be connected by a single path or through multiple paths for sending and receiving data.**

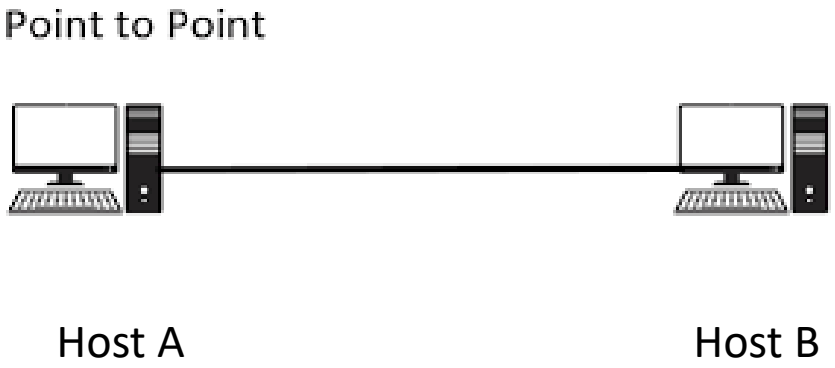
Network Types

- Type of connection
  - ✓It depends on the way a host communicates with other hosts or other computer networks.
  - ✓It is two types (point-to-point and point-to-multipoint)
- Physical topology
  - ✓It depends on the communication paths between the hosts are connected.
  - ✓It is four types(Star, Mesh, Bus, Ring)
- Reach of network
  - ✓It depends on network reachability.
  - ✓It is four types(PAN,LAN,MAN,WAN)

Connection types

- Point-to-point

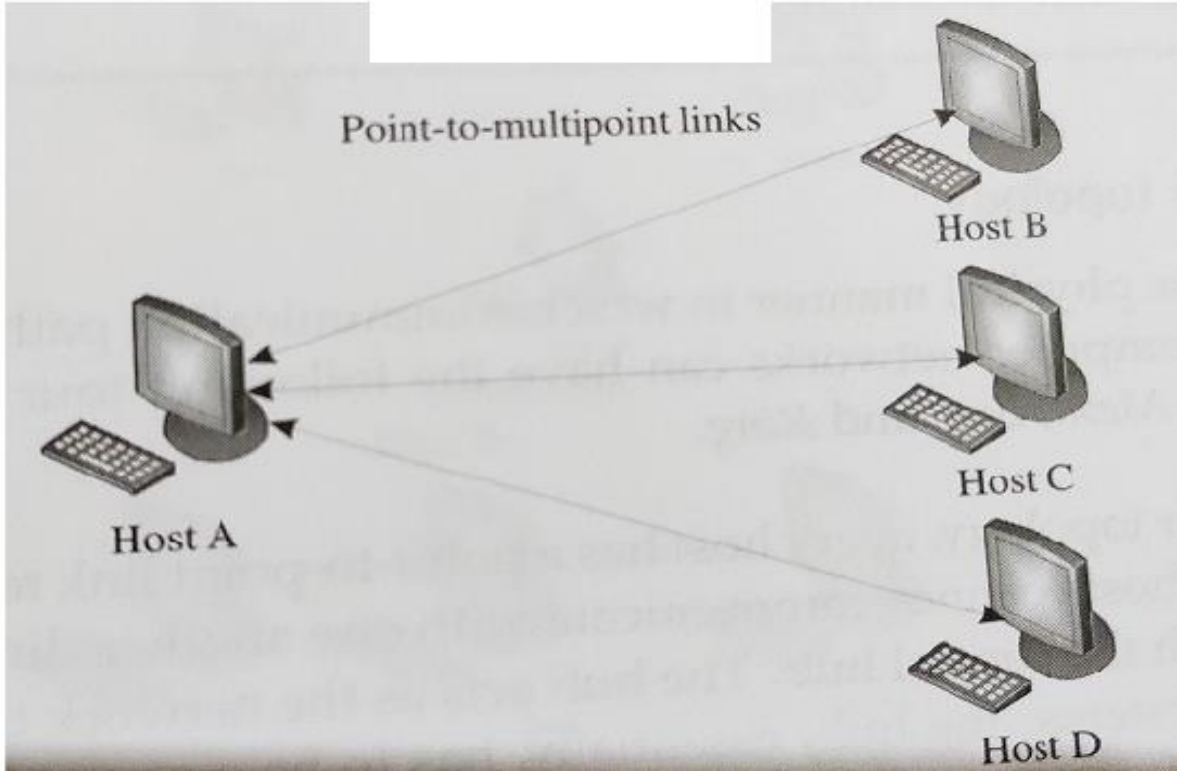
  - ✓It establishes direct connections between two hosts.
  - ✓Example : Remote control for an air conditioner, television
  - ✓Here whole channel is dedicated among devices.
  - ✓It works over duplex links.
  - ✓It is useful for synchronous and asynchronous systems.
  - ✓Widely used in optical networks.



Connection types

Point-to-Multipoint

- ✓More than two hosts share the same link
- ✓Widely used in wireless networks and IP telephony
- ✓Channel is shared between various hosts either spatially (FDMA)or temporally(TDMA).



Physical Topology

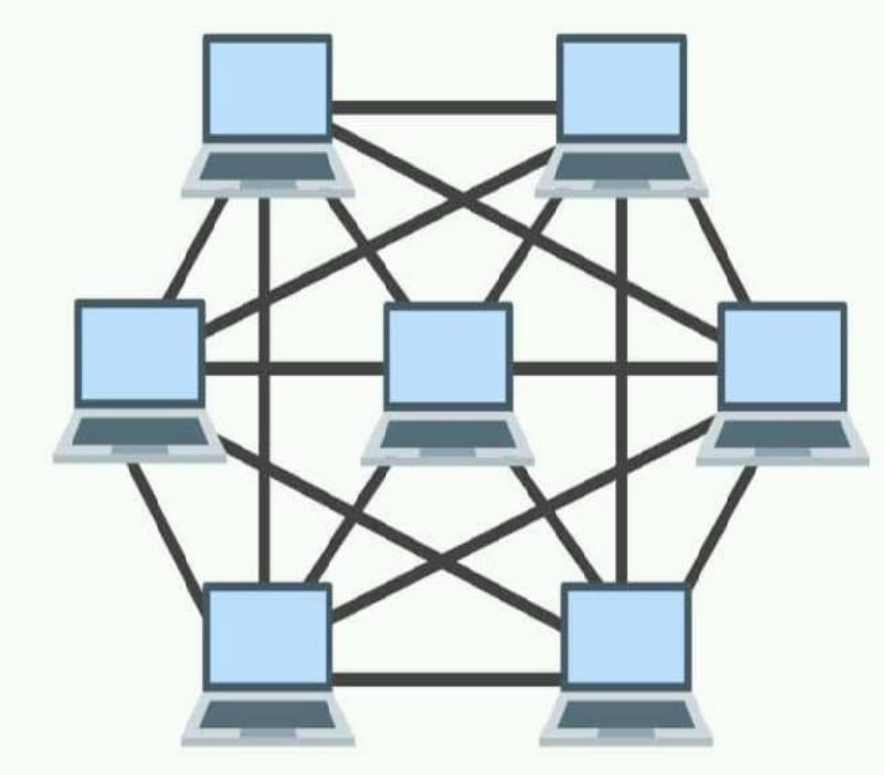
Star

- ✓Every host has a point-to-point link to a central controller or hub.
- ✓A host can not directly communicate with another host
- ✓The hub acts as the network traffic exchange
- ✓Cheaper and easier to set up
- ✓Suffers with single point of failure

Physical Topology

Mesh

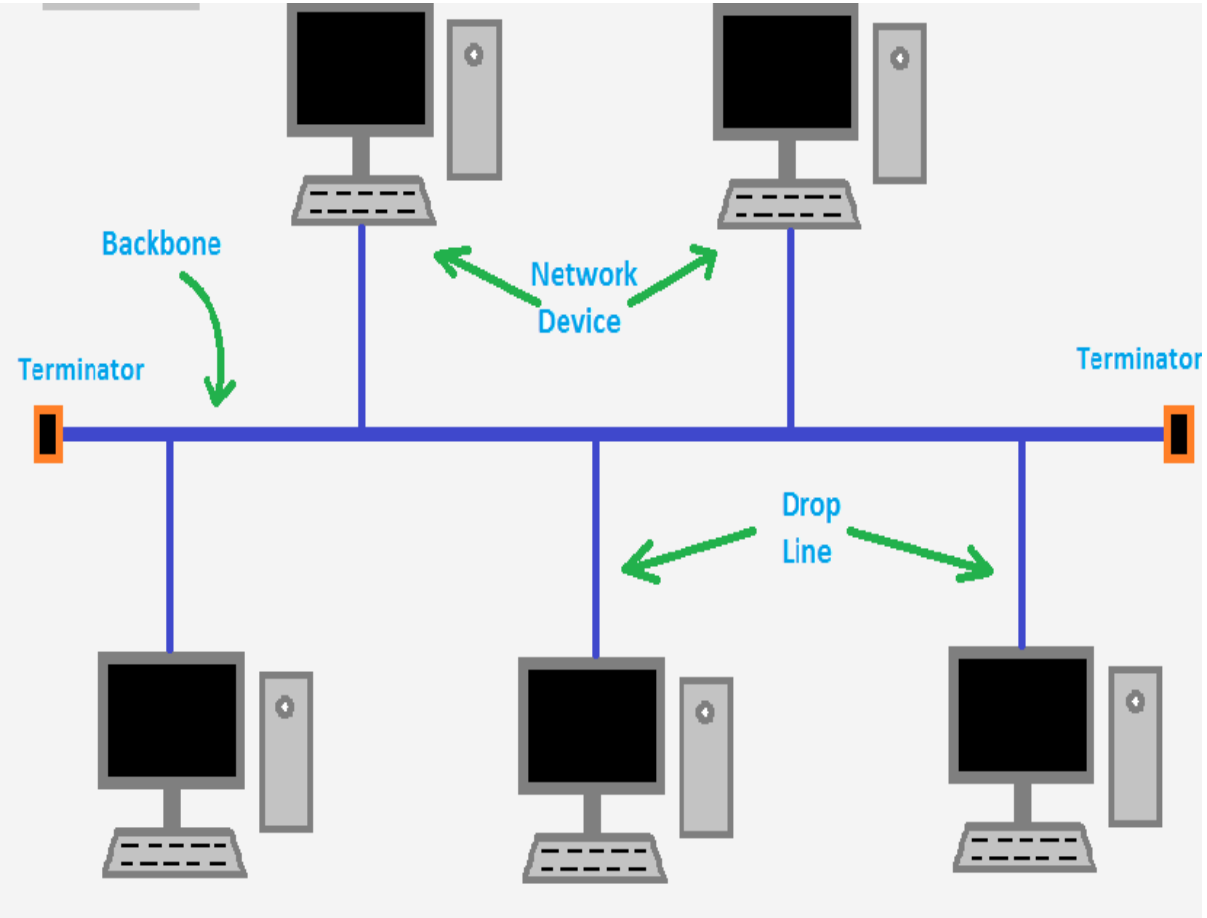
- ✓Every host is connected to every other host using a dedicated point-to-point link.
- ✓It has n(n-1)/2 dedicated full duplex links between the hosts, where n is the total number of hosts present in the network.
- ✓It is a expensive topology with respect to number of links
- ✓It is robustness and resilience system
- ✓It supports high security and privacy among the nodes
- ✓It reduces data loads on the network



Physical Topology

Bus

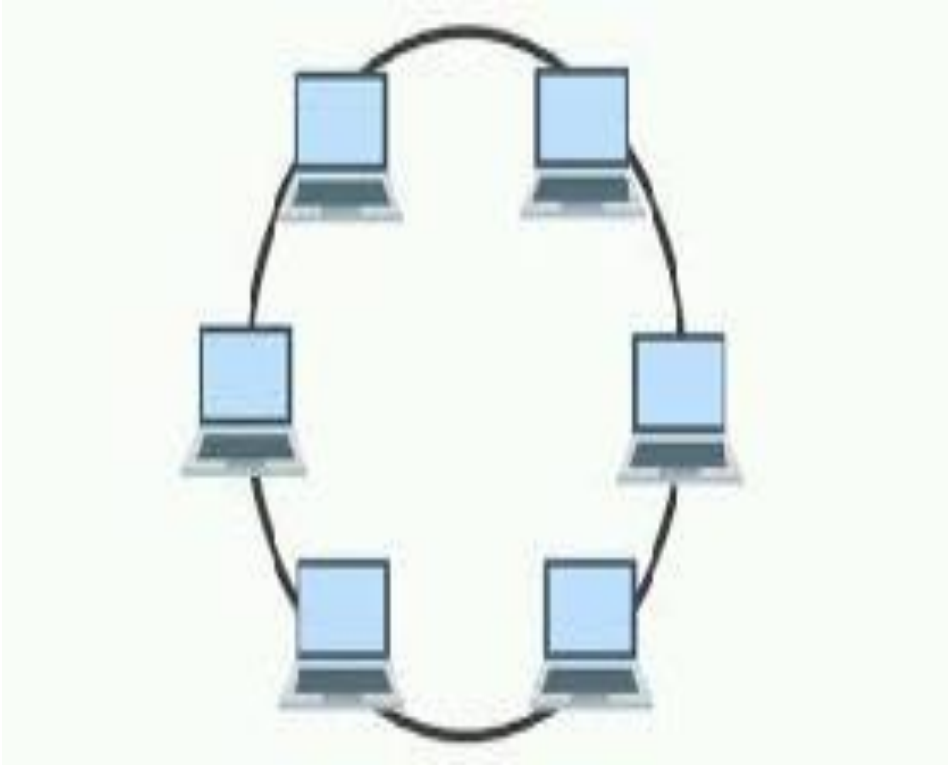
- ✓It follows the point-to-multipoint connection.
- ✓Ease of installation
- ✓Cheap Network
- ✓Signal loss occurs
- ✓Simple cabling procedure
- ✓Multiple drop lines and taps are used to connect the hosts to the bus.
- ✓Difficulty in fault localization within the network



Physical Topology

Ring

- ✓It uses point-to-point connection among the hosts
- ✓Each host have a dedicated point-to-point connection with its two immediate neighboring hosts on either side of it through repeaters at each host.
- ✓The repeaters at each host capture the incoming signal intended for other hosts, regenerates the bit stream and passes it into the next repeater
- ✓Fault identification and set up of the ring is simple and straightforward
- ✓High probability of single point of failure



Physical Topology

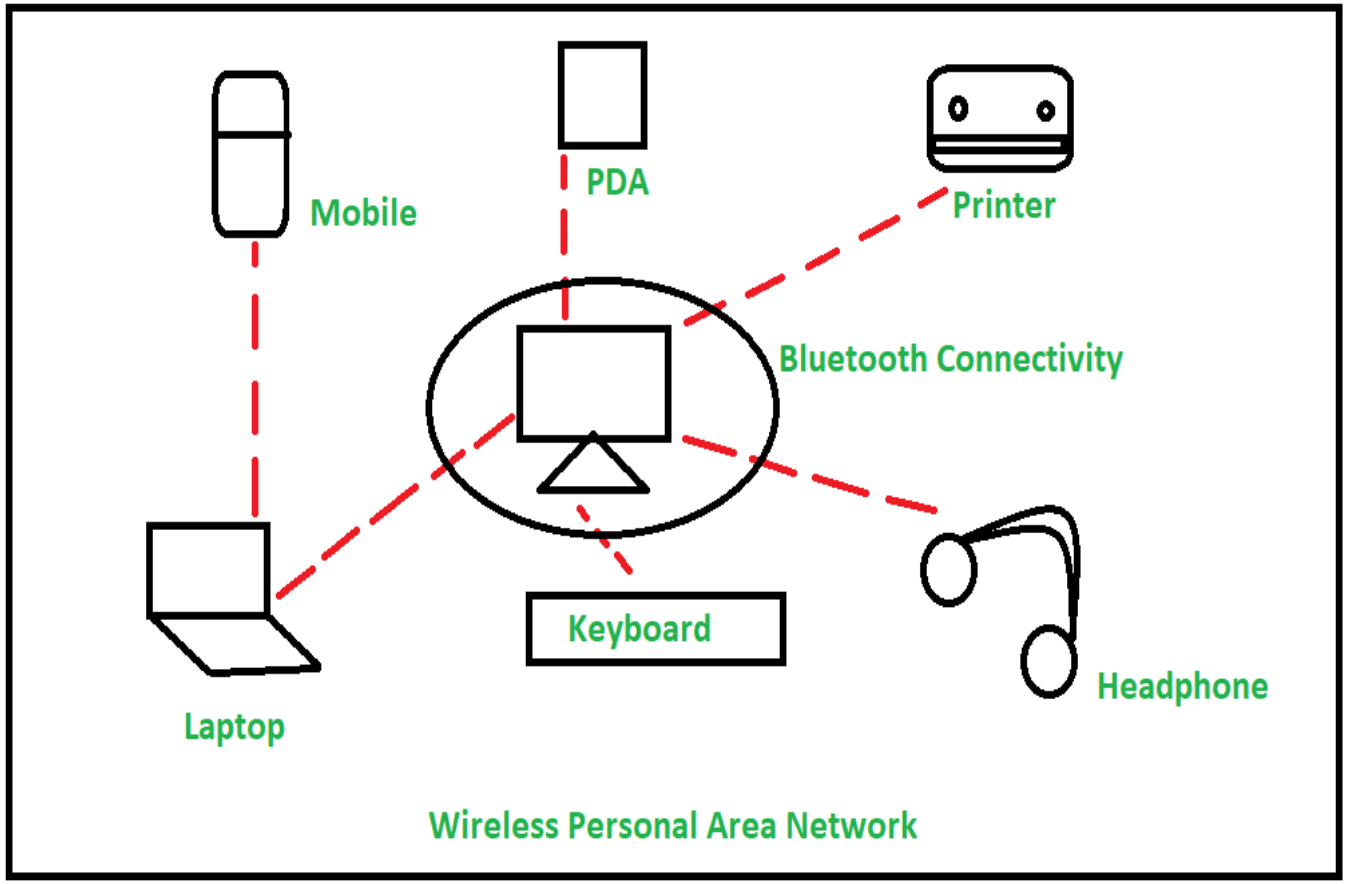
Network Topology comparison

Si. No.	Topology	Feature	Advantage	Disadvantage
1	Star	Point-to-point	Cheap, ease of installation, ease of fault identification	Single point of failure, traffic visible to network entities
2	Mesh	Point-to-point	Resilient against single point of failures, scalable, traffic privacy and security ensured	Costly, Complex connections
3	Bus	Point-to-Multipoint	Ease of installation, cheap	Length of backbone cable limited, number of hosts limited, hard to localize faults
4	Ring	Point-to-point	Ease of installation, cheap, ease of fault identification	Prone to single point of failure

Network Reachability

Personal Area Networks(PAN)

- ✓PAN are restricted to individual usage.
- ✓Example : wireless headphones, wireless speakers, laptops, smartphones, wireless keyboard, wireless mouse, printer within a house.
- ✓It supports wireless networks which make use of low range and low power technologies.
- ✓Reachability lies in the range of few centimeters to few meters



Network Reachability

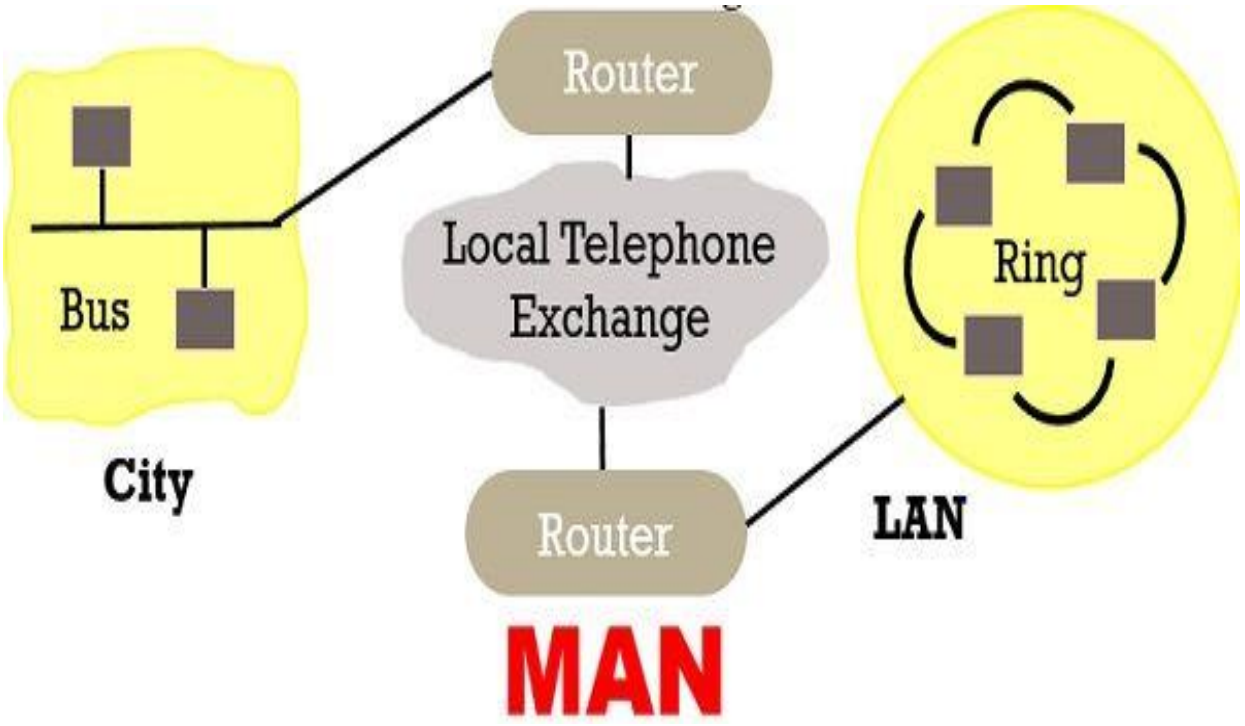
Local Area Networks(LAN)

- ✓A collection of hosts linked to a single network through wired or wireless connections
- ✓It is restricted to buildings, organizations, campuses
- ✓Data access rates within the LAN ranges from 100Mbps to 1000Mbps
- ✓High fault tolerance levels

Network Reachability

Metropolitan Area Networks (MAN)

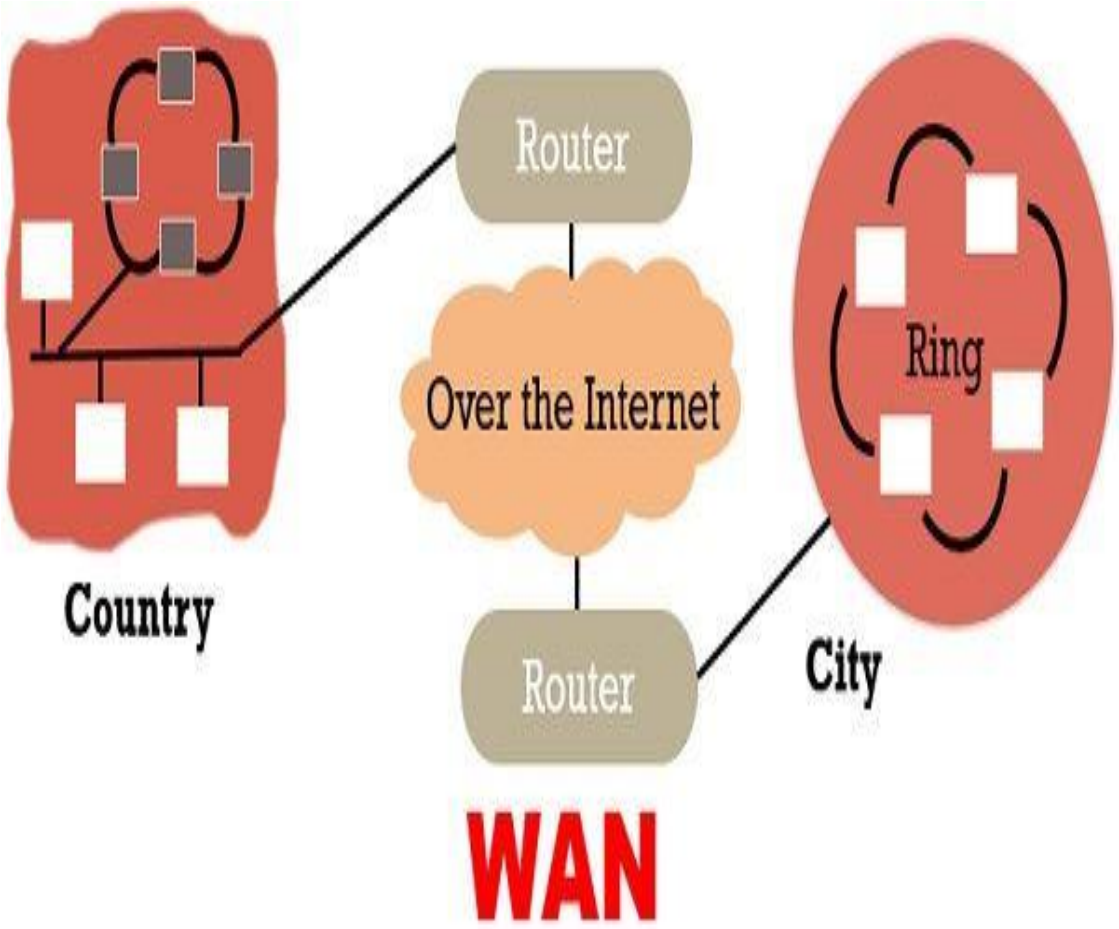
- ✓Reachability of a MAN lies between LAN and WAN
- ✓Widely used by various organization or building within a given geographic location or city
- ✓Example: Internet Service Provider (ISP) supplying internet connectivity to various organizations within a city
- ✓Cost effective that means a individual can not owned this.
- ✓Networking components are modems and cables
- ✓It has moderate fault tolerance level



Network Reachability

Wide Area Networks (WAN)

- ✓Connect to diverse geographical locations
- ✓Restricted within the boundaries of a state or country
- ✓Data rate of WAN is in the order of a fraction of LAN's Data rate
- ✓WANs are connected to LAN or MAN by using public switched telephone networks (PSTNs) or satellite based links
- ✓Transmission range is high compared to PAN, LAN, MAN.
- ✓Maintenance is very costly.
- ✓Fault tolerance of WAN is low compared to LAN.
- ✓More prone to noise during transmission



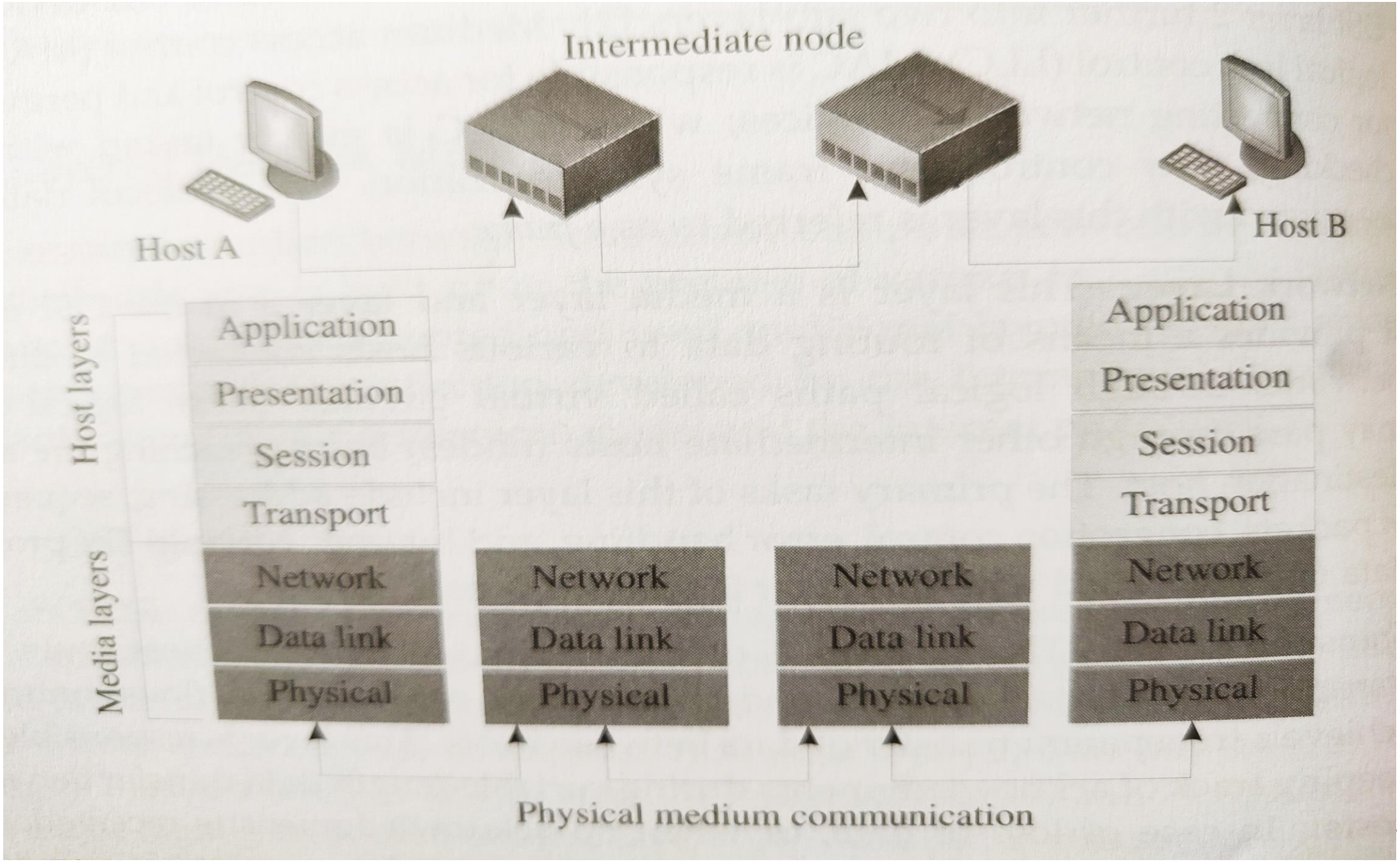
Comparison of PAN, LAN, MAN, WAN

BASIS OF COMPARISON	PAN	LAN	MAN	WAN
Expands to	Personal Area Network	Local Area Network	Metropolitan Area Network	Wide Area Network
Meaning	A network that connects a group of personnel in a home.	A network that connects a group of computers in a small geographical area.	It covers relatively large region such as cities, towns.	It spans large locality and connects countries together. Example Internet.
Ownership of Network	Private	Private	Private or Public	Private or Public
Design and maintenance	Easy	Easy	Difficult	Difficult
Propagation Delay	Short	Short	Moderate	Long
Speed	High	High	Moderate	Low
Fault Tolerance	More Tolerant	More Tolerant	Less Tolerant	Less Tolerant
Congestion	Less	Less	More	More
Used for	Home	College, School, Hospital.	Small towns, City.	Country/Continent.
Allows	Single pair of devices to communicate.	Single pair of devices to communicate.	Multiple computers can simultaneously interact.	A huge group of computers communicate at the same time.

Layered Network Model

ISO-OSI reference model

- It is a conceptual model maintained by International Organization of Standardization.
- It divides any network communication system into seven layers
- Seven layers are
  - ✓ Physical layer
  - ✓ Datalink layer
  - ✓ Network layer
  - ✓ Transport layer
  - ✓ Session layer
  - ✓ Presentation layer
  - ✓ Application layer


Intermediate node
Host A
Host B
Host layers
Media layers
Application
Presentation
Session
Transport
Network
Data link
Physical
Network
Data link
Physical
Network
Data link
Physical
Application
Presentation
Session
Transport
Network
Data link
Physical
Physical medium communication

ISO-OSI reference model

Physical Layer

- It is media layer
- It is responsible for taking care of the electrical and mechanical operations of the host (signal generation, signal transfer, voltages, layout of the cable, physical port layout, line impedance, signal loss)
- This layer is responsible for topological layout of the network(star, bus, ring, mesh), communication mode (simplex, duplex) and bit rate control operations.
- The protocol data unit is Symbol.

ISO-OSI reference model

Data Link Layer

- This is media layer
- This layer is mainly used for establishment and termination of the connection between two hosts and detection and correction of errors during the communication between two or more devices.
- This layer is divided into two sub layers and they are LLC (Logical Link Control) and MAC (Media access control). LLC is responsible for error checking, flow control, frame synchronization. MAC is responsible for access control and permissions for connecting network devices.
- The protocol data unit is frame.

ISO-OSI reference model

Network Layer

- ✓This is a media layer.
- ✓It provides routing data to various hosts connected to different networks through logical paths called virtual circuits.
- ✓Various tasks of this layer includes addressing, sequencing of packets, congestion control, error handling, Internetworking.
- ✓The data unit is packet.

ISO-OSI reference model

Transport Layer

- This is host layer.
- This layer is responsible for end to end error recovery and flow control to achieve a transparent transfer of data between hosts and keeping track of acknowledgements during variable length data transfer between hosts.
- The protocol data unit is segment or datagram.

ISO-OSI reference model

Session Layer

- This is host layer.
- This layer is responsible for establishing, controlling, terminating of communication between hosts.
- Protocols used for this layer is remote procedure call, remote sessions.
- Protocol data unit is data.

ISO-OSI reference model

Presentation Layer

- This is host layer.
- This is responsible for data format conversion and encryption.
- It is also called syntax layer.
- The data unit is called data.

ISO-OSI reference model

Application layer

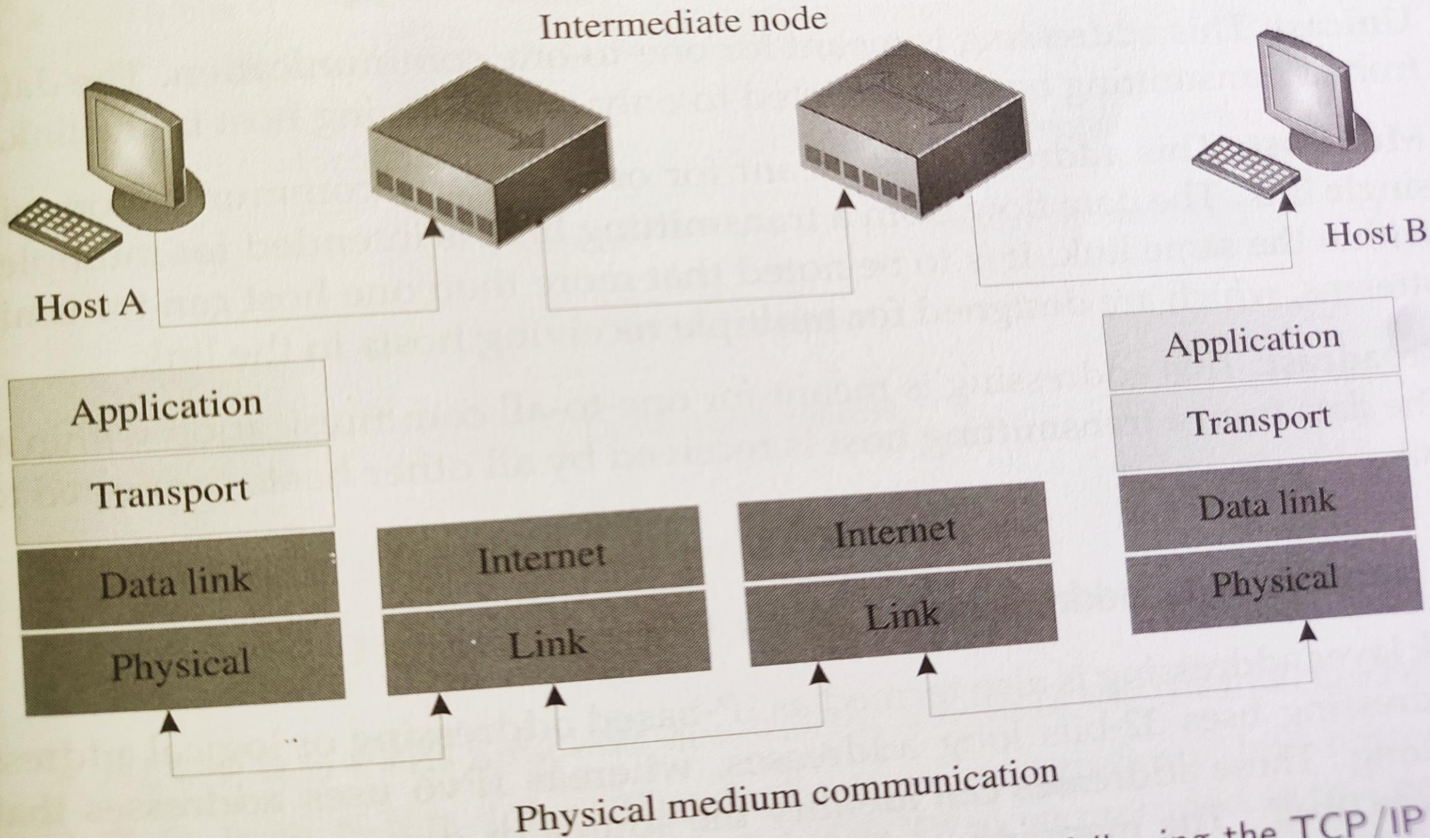
- This is host layer.
- It is used by end user through software APIs (Application Program Interfaces)(FTP, HTTP, e-mails) and terminals.
- It deals with user authentication, identification of communication hosts, quality of service and privacy.
- The protocol data unit is data.

Summary of OSI layers and their features

Layer	Name	Location	PDU(Protocol data unit)	Function	Example
1	Physical	Media	Symbol	Communication over physical medium	Ethernet, FDDI
2	Data link	Media	Frame	Reliability of communication over physical medium	IEEE802.5,IEEE 802.3,PPP,HDLC
3	Network	Media	Packet	Structuring of data and routing between multiple nodes	IP
4	Transport	Host	Segment	Reliability of communication over networks or between hosts	TCP,UDP
5	Session	Host	Data	Establishment, management and termination of remote sessions	RPC
6	Presentation	Host	Data	Syntactic conversion of data and encryption	Encryption,MPEG
7	Application	Host	Data	User identification, authentication, privacy, quality of service	SNMP,WWW,HTTP,FTP,Telnet

Internet Protocol suite

- It is conceptual model.
- It has four layers
- They are Link layer, Internet layer, Transport layer, Application layer
- This is commonly known as TCP/IP protocol suite.
- This is also called Department of Defense (DoD) model.


Intermediate node
Host A
Host B
Application
Transport
Data link
Physical
Internet
Link
Internet
Link
Application
Transport
Data link
Physical
Physical medium communication

Internet Protocol suite

Link Layer

- This is base layer of TCP/IP protocol suite.
- It is also called network interface layer.
- This is synchronous with physical and data link layer of OSI layer.
- It transmits TCP/IP packets over physical media.
- It is independent of medium in use, frame format, network access.
- Technology used : Ethernet, Wireless LAN,ATM(Asynchronous transfer mode)

Internet Protocol suite

Internet layer

- It is synchronous to network layer of OSI model
- It is responsible for addressing, address translation, data packaging, data disassembly and assembly, routing, packet delivery tracking operations.
- Protocols used in this layer is ARP(Address resolution protocol),IP(Internet protocol),ICMP(Internet control message protocol) and IGMP(Internet group management protocol)
- This is built on IPv4 and IPv6.

Internet Protocol suite

Transport layer

- It is synchronous with transport layer of OSI model
- Its function includes error control, flow control, congestion control, segmentation and addressing in end to end manner.
- It is independent of underlying network.
- Protocols used :TCP(Transmission control protocol), UDP(user datagram protocol).
- It provides connection oriented and connection less services between two or more hosts and network devices.

Internet Protocol suite

Application layer

- Functionalities of this layer is synchronous with collective functionalities of session, presentation, and application layer of OSI layer.
- It enables end user to access the services of underlying layers and define the protocols for the transfer of data.
- Protocols used in this layer is: HTTP(Hyper text transfer protocol), FTP(File transfer protocol), SMTP(simple mail transfer protocol), DNS(domain name system), RIP(Routing information protocol), SNMP(simple network management protocol)

Summary of TCP/IP layers and their features

Layer	Name	Location	PDU(Protocol data unit)	Function	Example
1	Link	Media	Frame	Transmission of data over physical medium	Ethernet, Wireless LAN, ATM
3	Internet	Media	Packet	Structuring of data and routing between multiple nodes	IP,ARP,ICMP, IGMP
4	Transport	Host	Segment	Reliability of communication over networks or between hosts	TCP,UDP
7	Application	Host	Data	User identification, authentication, privacy, quality of service, etc.	SNMP,WWW, HTTP,FTP,RIP, DNS,SMTP

Addressing

Addressing mechanism is divided into two parts

- Link layer addressing
- Network layer addressing

Data link layer addressing

- Data link layer address is also known as media access control (MAC) address of devices.
- It is 48 bit hardware address provided by device manufacturers.
- First 24 bit is organizational identifiers and last 24 bit is network interface controller identifiers.
- These addresses are unique globally.
- It is three types
    - ✓Unicast(one-to-one communication)
    - ✓Multicast(one-to-many communication)
    - ✓broadcast(one-to-all communication)

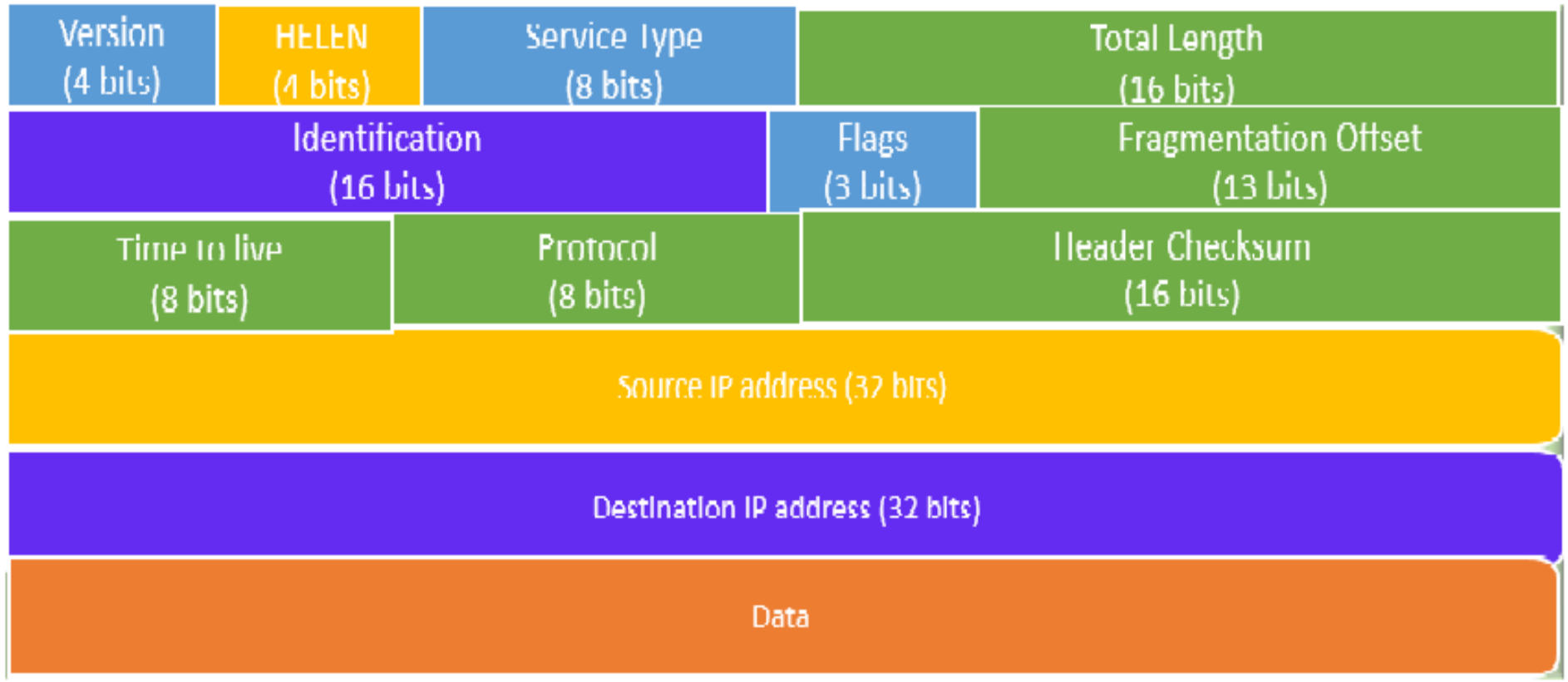
Network layer Addressing

- It is also known as IP based addressing or logical addressing.
- IPv4(32 bits long addresses), IPv6(128 bits long addresses).
- The mapping (device/host logical address to its hardware address) is done by ARP(Address resolution protocol).

IPv4

- IPv4 is an IP version widely used to identify devices on a network .
- It was the first version of IP deployed ARPANET in 1983.
- It uses a 32-bit address scheme to store 2^32 addresses.
- It is considered the primary Internet Protocol and carries 94% of Internet traffic.

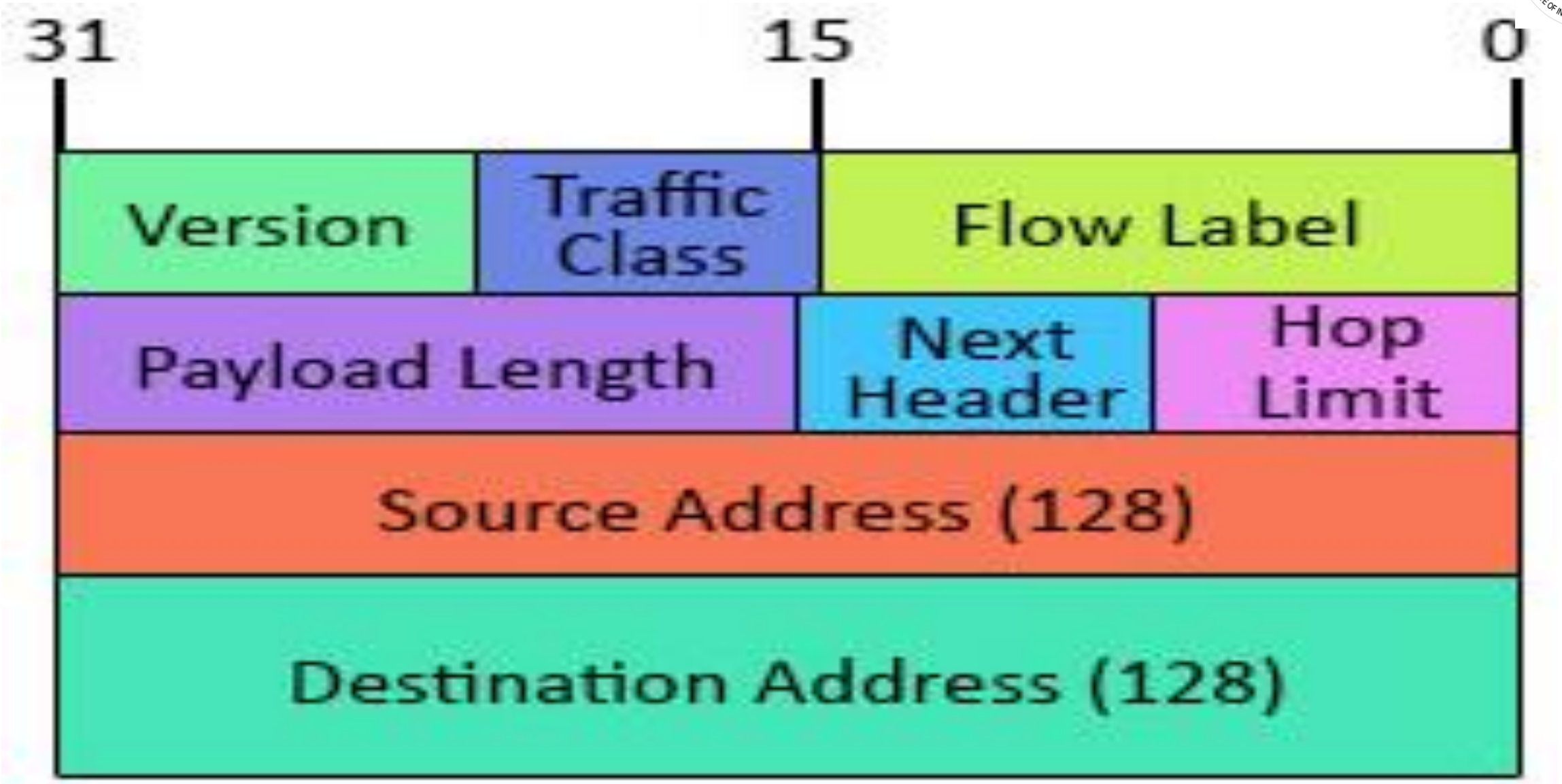
IPv4


Version
(4 bits)
HELEN
(4 bits)
Service Type
(8 bits)
Total Length
(16 bits)
Identification
(16 bits)
Flags
(3 bits)
Fragmentation Offset
(13 bits)
Time to live
(8 bits)
Protocol
(8 bits)
Header Checksum
(16 bits)
Source IP address (32 bits)
Destination IP address (32 bits)
Data

IPv6

- IPv6 is the most recent version of the Internet Protocol.
- This new IP address version is being deployed to fulfill the need for more Internet addresses.
- It was aimed to resolve issues that are associated with IPv4.
- With 128-bit address space, it allows 340 undecillion unique address space.
- IPv6 is also called IPng (Internet Protocol next generation).

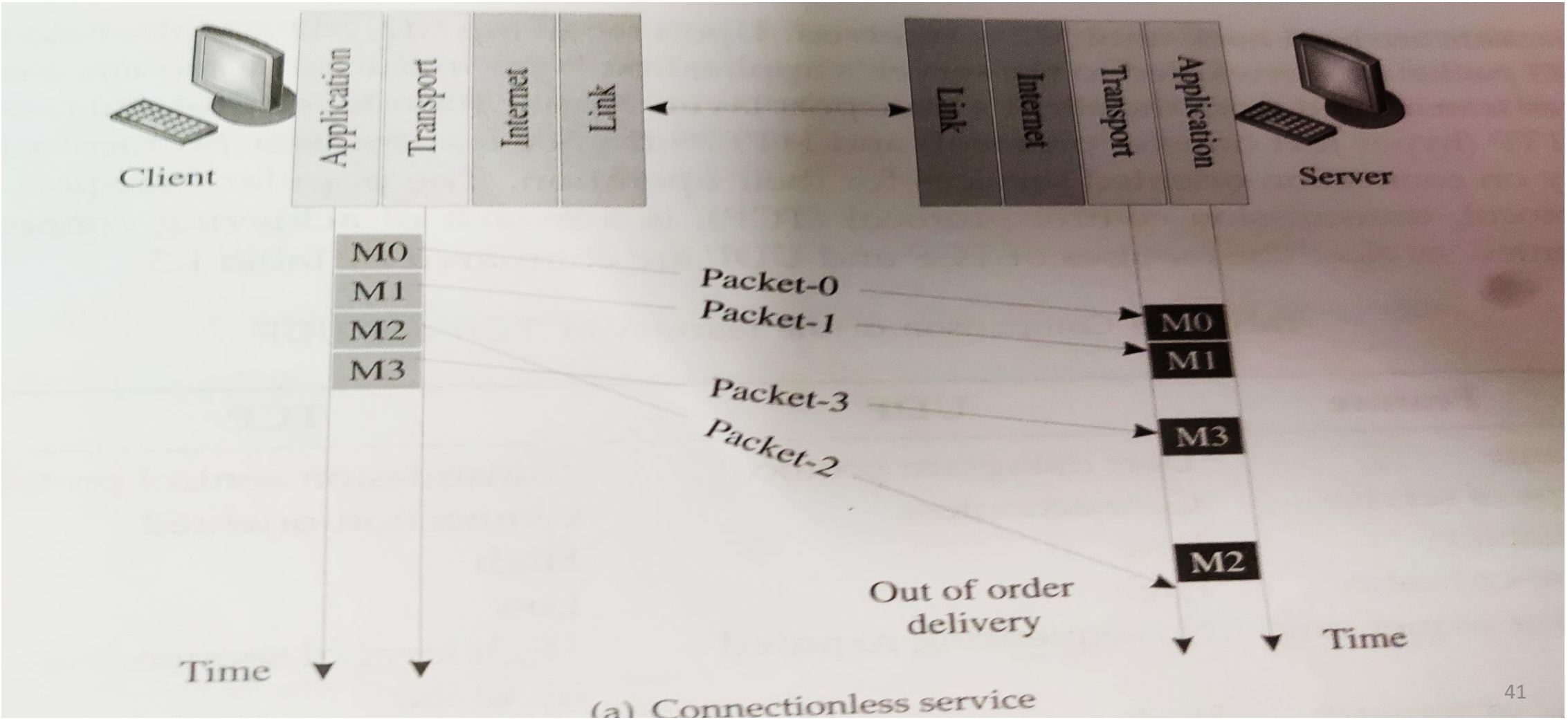
IPv6


31
15
0
Version
Traffic Class
Flow Label
Payload Length
Next Header
Hop Limit
Source Address (128)
Destination Address (128)

Comparison of IPv4 and IPv6

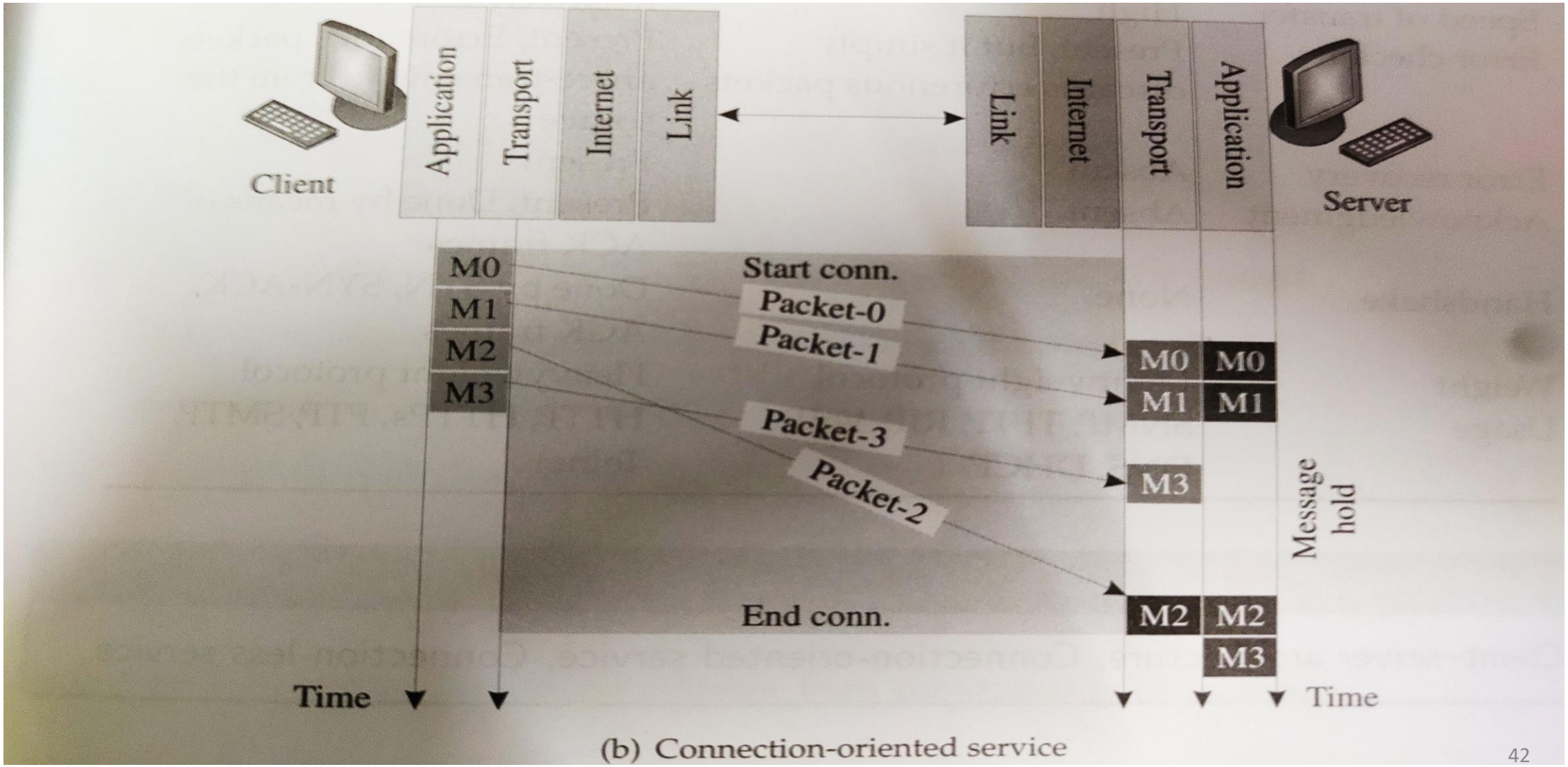
- IPv4 is 32-Bit IP address whereas IPv6 is a 128-Bit IP address.
- IPv4 is a numeric addressing method whereas IPv6 is an alphanumeric addressing method.
- IPv4 binary bits are separated by a dot(.) whereas IPv6 binary bits are separated by a colon(:).
- IPv4 offers 12 header fields whereas IPv6 offers 8 header fields.
- IPv4 supports broadcast whereas IPv6 doesn’t support broadcast.
- IPv4 has checksum fields while IPv6 doesn’t have checksum fields
- IPv4 supports VLSM (Variable Length Subnet Mask) whereas IPv6 doesn’t support VLSM.
- IPv4 uses ARP (Address Resolution Protocol) to map to MAC address whereas IPv6 uses NDP (Neighbour Discovery Protocol) to map to MAC address.

Connectionless services



(a) Connectionless service

Connection-oriented services



(b) Connection-oriented service

Connection oriented vs connection less services

.NO	Connection-oriented Service	Connection-less Service
1.	Example: Telephone system.	Example: Postal system.
2.	It is preferred by long and steady communication.	It is preferred by bursty communication.
3.	It is feasible.	It is not feasible.
4.	Congestion is not possible.	Congestion is possible.
5.	It gives the guarantee of reliability.	It does not give the guarantee of reliability.
6.	Packets follow the same route.	Packets do not follow the same route.
7.	It requires a bandwidth of high range.	It requires a bandwidth of low range.

Comparison of the features of TCP and UDP

Si. No	Feature	UDP	TCP
1	Name	User Datagram Protocol	Transmission control Protocol
2	Type of service	Connectionless	Connection-oriented
3	Reliability	Low	High
4	Time-criticality	High	Low
5	Packet sequencing	No sequencing required	High level of sequencing involved
6	Speed of transfer	High	Relatively low
7	Error checking	Present, but it simply discards erroneous packets	Present, erroneous packets are re-transmitted from the source
8	Error recovery	Absent	Present
9	Acknowledgment	Absent	Present, Done by acknowledgement frame
10	Handshake	None	Done by SYN, SYN-ACK, ACK frames
11	Weight	Lightweight protocol	Heavy weight protocol
12	Usage	RIP, VoIP, DNS, DHCP	HTTP, FTP, SMTP, Telnet

Thank You

Unit-1

Introduction to IoT

Networking

- **Connected entity with specific application**

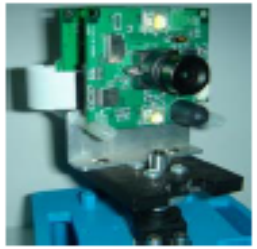
- **Linking of computers and communication network devices (Switches, routers, and wireless access points), which interconnect through a network(Internet/Intranet) and are separated by unique device identifiers (Internet protocol, IP address, MAC Address)**

- **Network devices may be connected by a single path or through multiple paths for sending and receiving data.**

Wireless Sensor

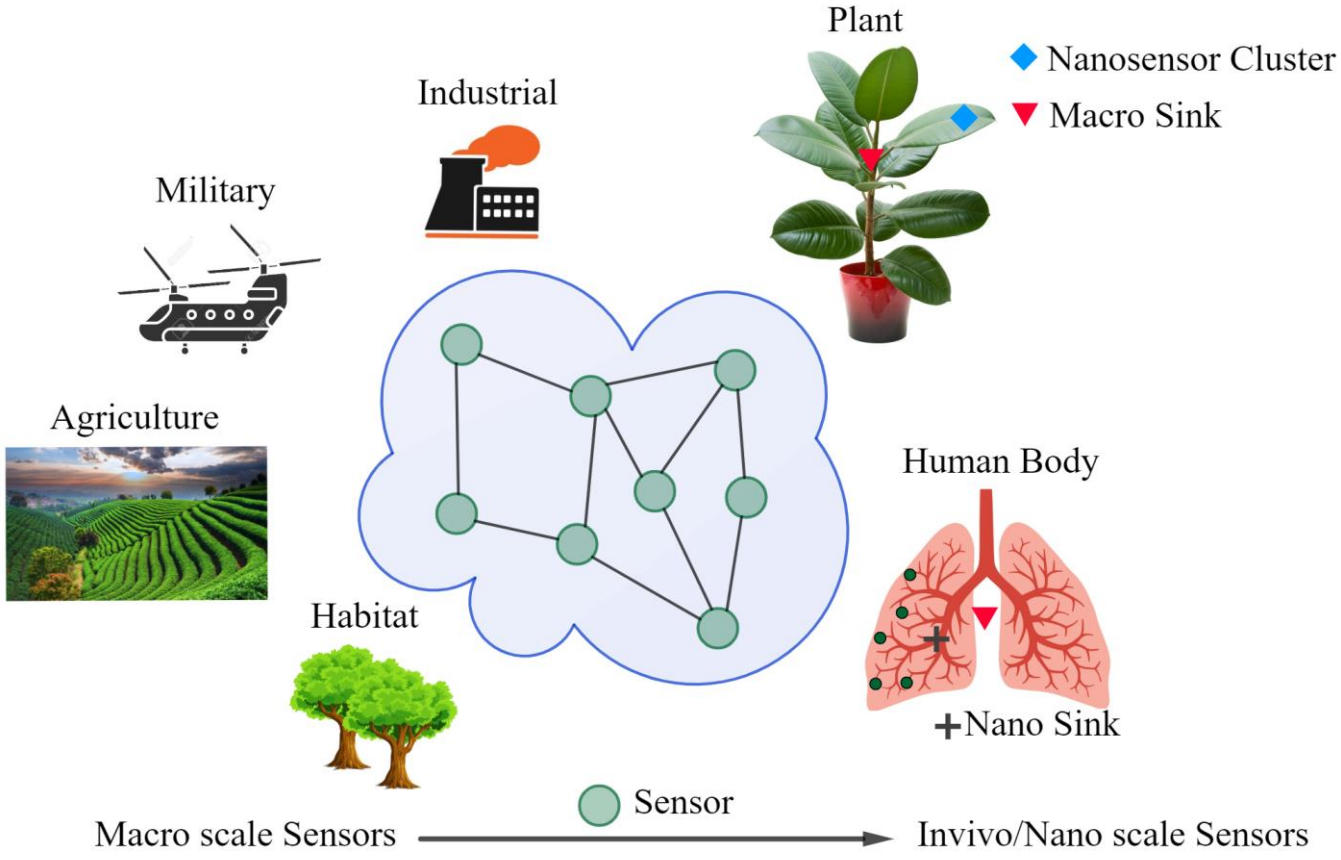
Computation
In-network Processing:
Fusion, Estimation,
Filtering, Aggregation

Communication
(Wireless)
Transmission/Reception:
Broadcasting, Routing,
Dissemination



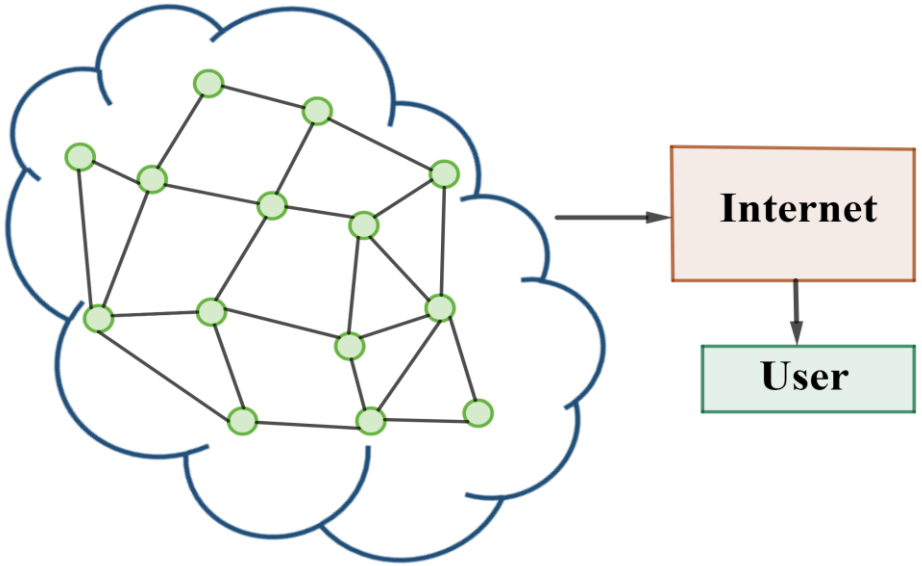
Control
(Sensing / Actuation)
Data Sensing & Collection:
temperature, humidity,
pressure, light, velocity,
sound, image

Evolution of Wireless Sensor Networks

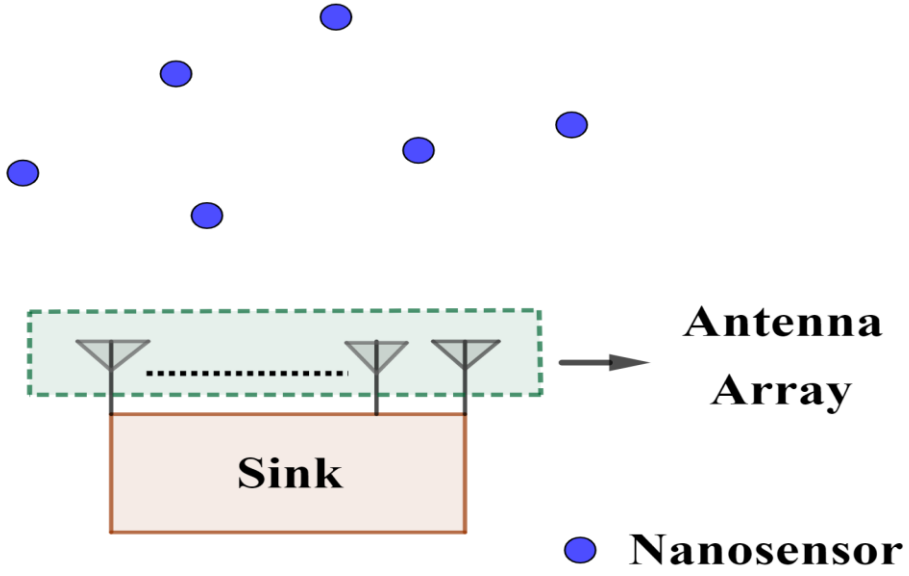


Application and Evolution of WSN

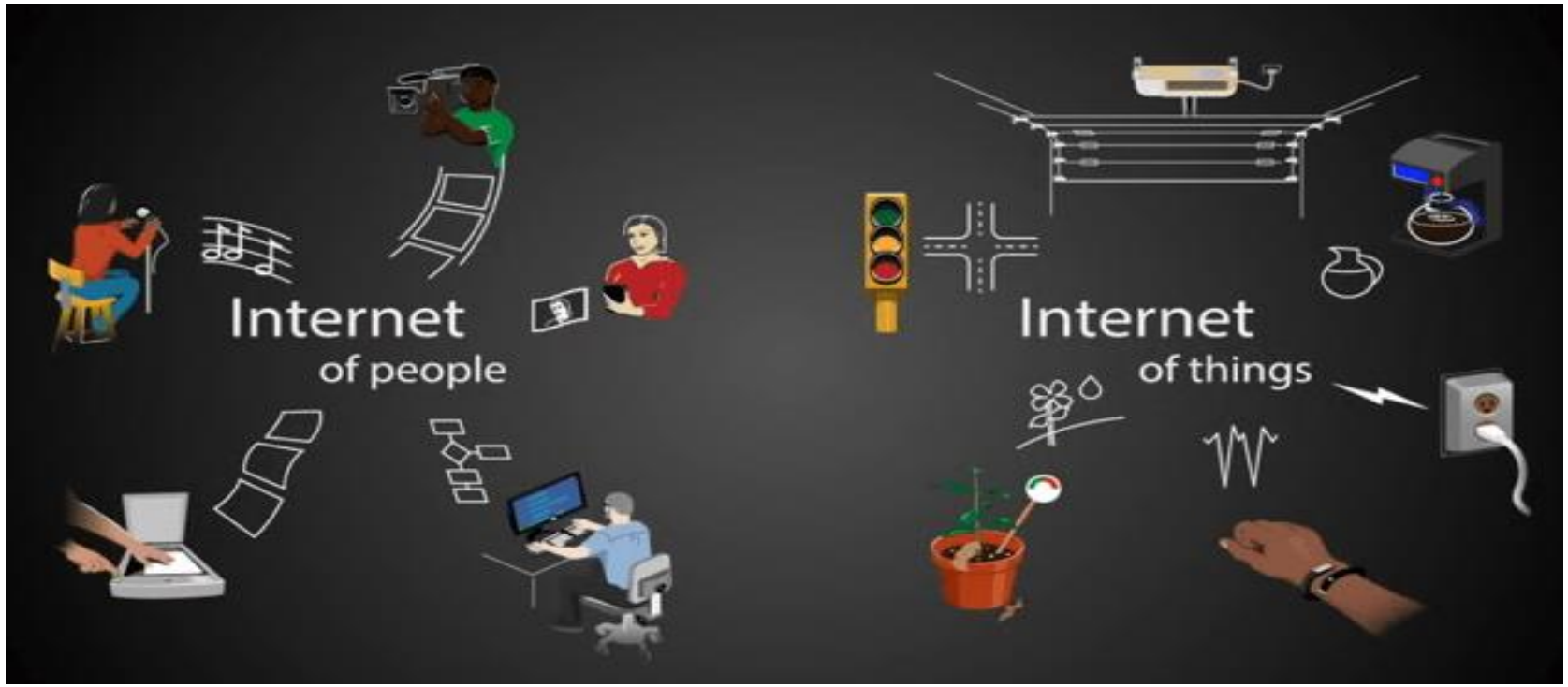
Wireless Sensor Networks Use Case



Scenario 1 – Macro WSN

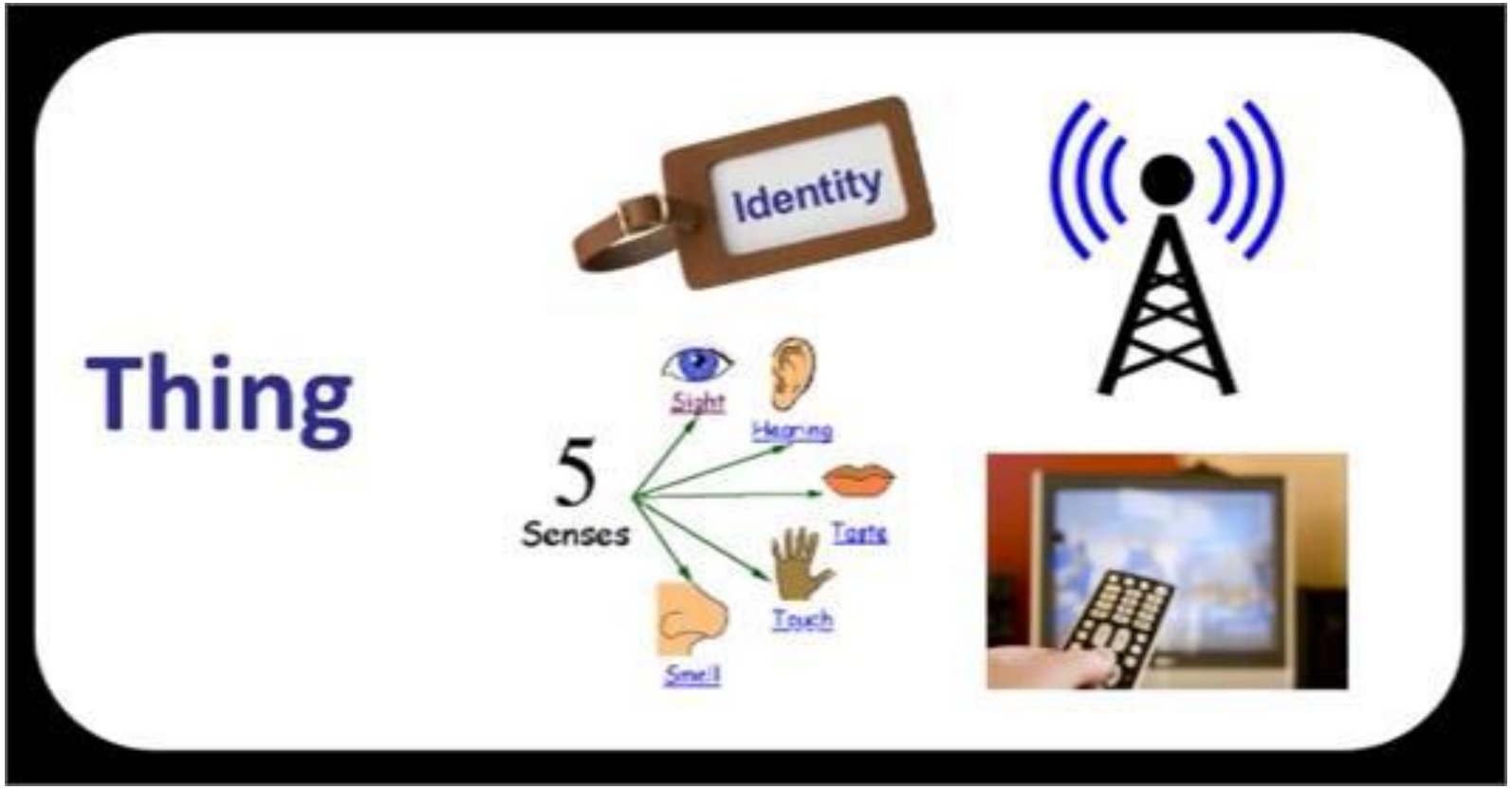


Scenario 2 – Nano WSN



- **Internet-**
  - **Connectivity among the people**
  - **Become part of life**
- **New Internet- Connecting things**
- **Things + Sense and Communicate**

Thing ????



Ask Google : Where is my keys?
: Where are my kids?

What is IoT?

- It stands for Internet of things.
- "Things", in the IoT sense, can refer to a wide variety of devices.
- It is basically a network
- Things can communicate with each other using **internet** as means of communication between them.
- All the things are IP protocol enabled in order to have this concept possible.

Definition of IoT

- The Internet of Things (IoT) is the network of physical objects that contain embedded technology to communicate and sense or interact with their internal states or the external environment.

Characteristics

- Efficient, scalable and associated architecture
- Unambiguous naming and addressing
- Abundance of sleeping nodes, mobile and non-IP devices
- Intermittent connectivity

How to Build IoT

- To build connected devices : need three different pieces.
    1. a device that can connect,
    2. a network connection and
    3. an application
- Wireless radios allow the devices to connect to the Internet and to each other.
- For short range
    - Wi-Fi, Bluetooth, Zigbee and Z-Wave, just to name a few.
- For longer range,
    - 2G / 3G and now 4G (LTE).
- In addition, a new breed of low-power, long-range wireless networks (LPWAN- Low Power Wide Area Network).

Who Care IoT?

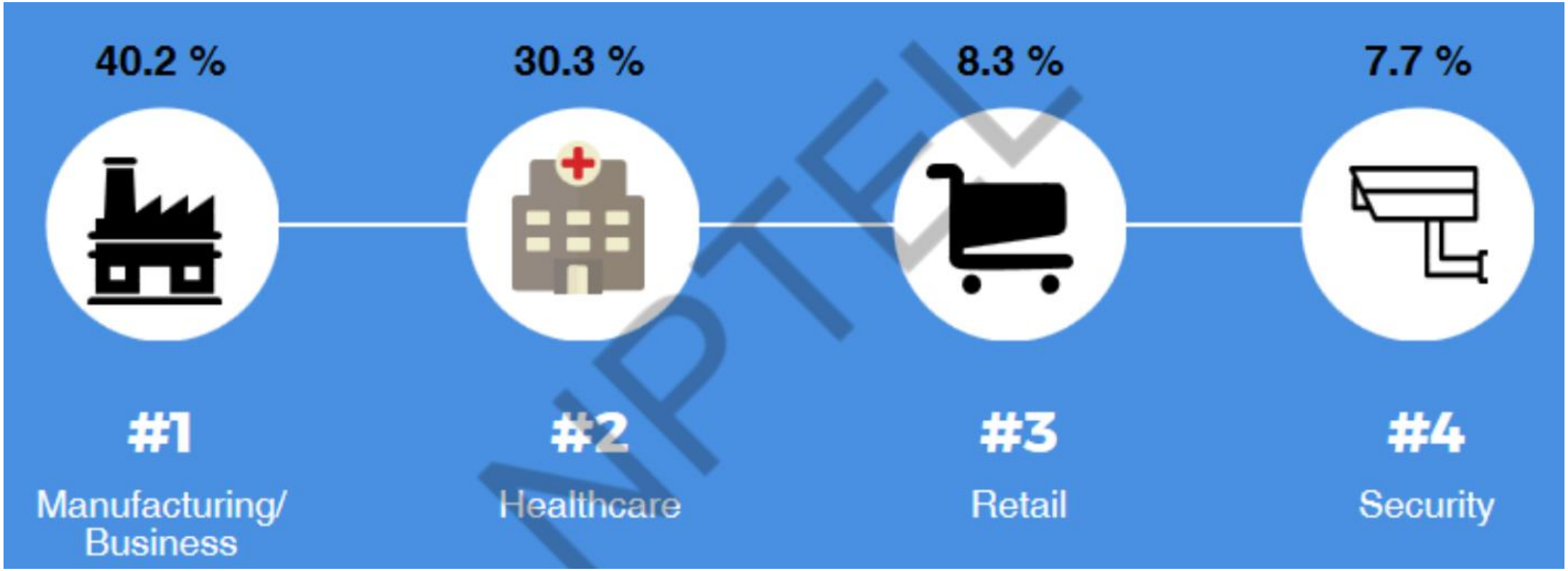
- At this point, the easier question might be who *isn't* working on an IoT product.

- Big names like Samsung, LG, Apple, Google, IBM Lowe's and Philips are all working on connected devices, as are many smaller companies and start-ups.

Modern Day IoT Applications

- Smart Parking
- Structural health
- Noise Urban Maps
- Smartphone Detection
- Traffic Congestion
- Smart Lighting
- Waste Management
- Smart Roads
- River Floods
- Supply Chain Control
- NFC Payment
- Intelligent Shopping Applications
- Smart Product
- Radiation Levels
- Smart Grid
- Tank level
- Photovoltaic Installations
- Water Flow
- Silos Stock Calculation
- Perimeter Access Control
- Liquid Presence
- Forest Fire Detection
- Air Pollution
- Snow Level Monitoring
- Landslide and Avalanche Prevention
- Earthquake Early Detection
- Water Leakages
- Explosive and Hazardous Gases

IoT Market Share



IoT Market Share

- Business/Manufacturing
  - Real-time analytics of supply chains and equipment, robotic machinery.
- Healthcare
  - Portable health monitoring, electronic record keeping, pharmaceutical safeguards.
- Retail
  - Inventory tracking, smartphone purchasing, anonymous analytics of consumer choices.
- Security
  - Biometric and facial recognition locks, remote sensors.

Origin of Terminology

- In the 2000s, we are heading into a new era of ubiquity, where the “users” of the Internet will be counted in billions and where humans may become the minority as generators and receivers of traffic.

- Instead, most of the traffic will flow between devices and all kinds of “things”, thereby creating a much wider and more complex Internet of Things.

- The title of the report was “Internet of Things”

- Discussed the possibility of internet connected M2M connectivity networks, extending to common household devices

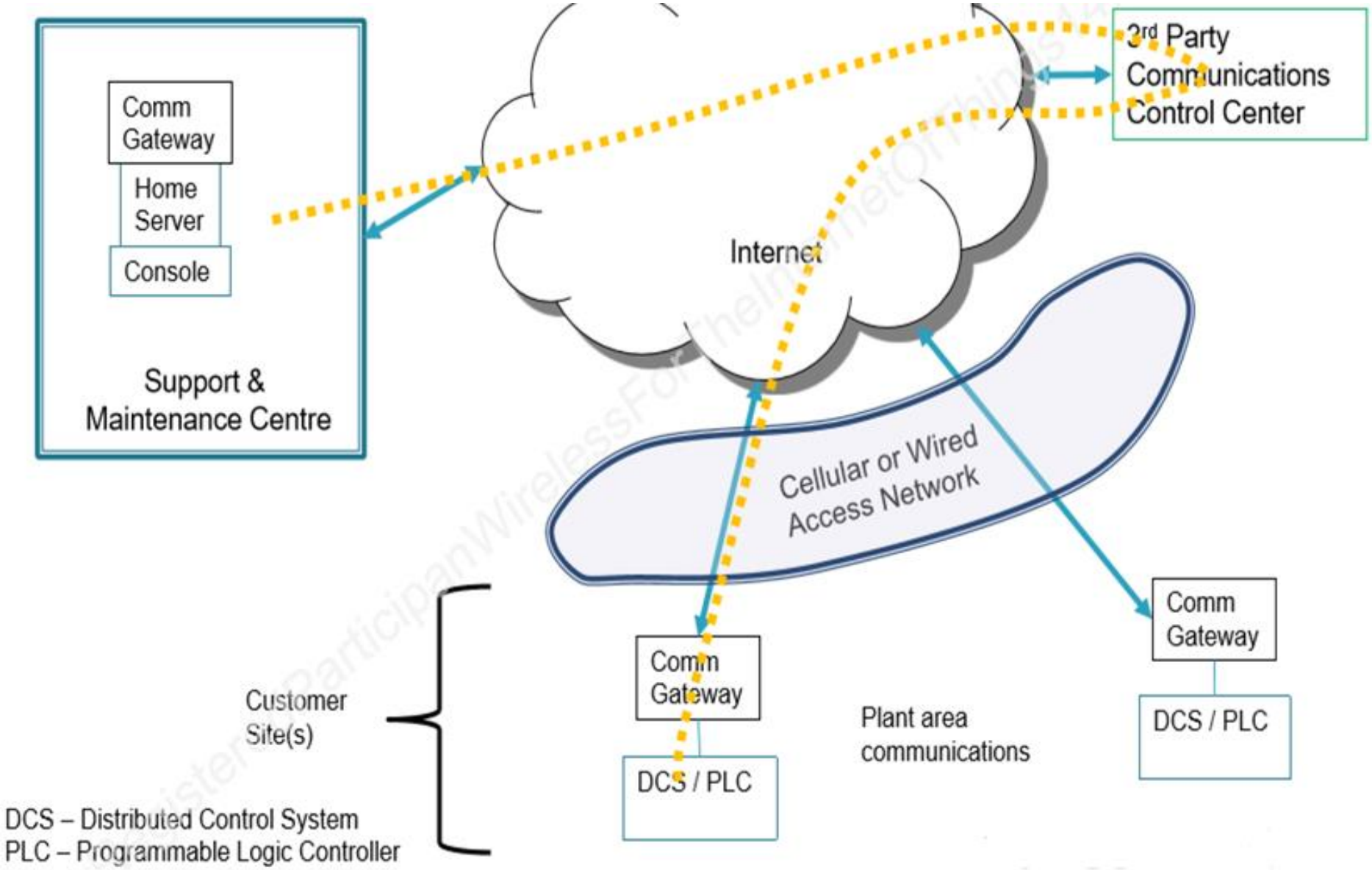
- Some areas identified as IoT enablers:
  RFID, Nanotechnology, Sensors, Smart Networks.

IoT Example Connected Support

- The main idea is you are attached to something and you are monitoring its behaviour.

- Down we have industrial applications and we have Distributed Control Systems (DCS) made up of Programmable Logic Controller (PLC).

- Typically in this model devices can speak to each other and there is some sort of communication between the gateways that will leave the local area.


Comm Gateway
Home Server
Console
Support & Maintenance Centre
Internet
3rd Party Communications Control Center
Cellular or Wired Access Network
Comm Gateway
DCS / PLC
Comm Gateway
DCS / PLC
Customer Site(s)
Plant area communications
DCS – Distributed Control System
PLC – Programmable Logic Controller

CONTD…

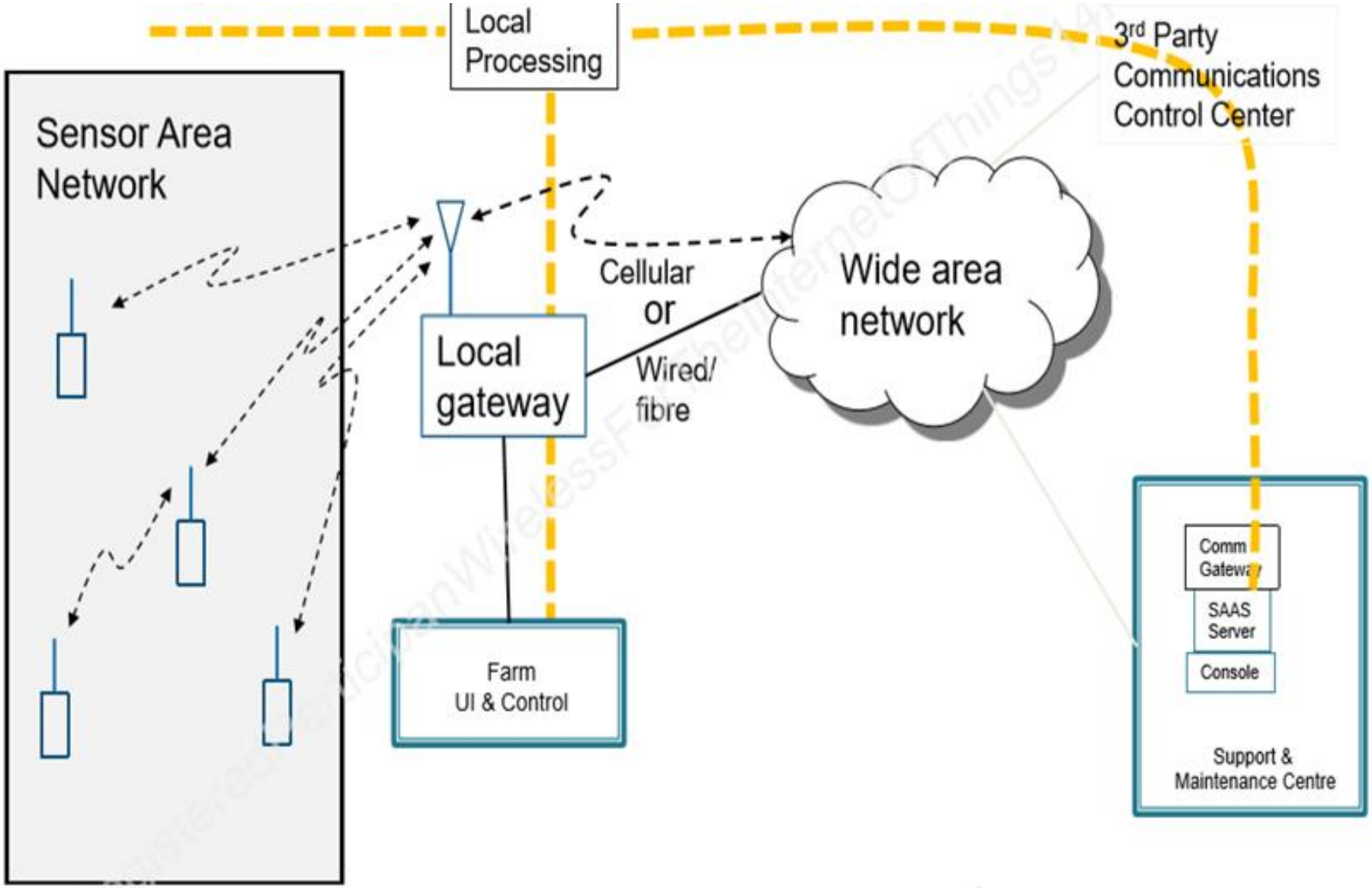
- Communication gateways are connected to internet.
- Connected by
  - cellular or
  - wired access network.
- Wired connections has some drawbacks so wireless connections are preferred.
- Often we go to nearby equipment and then hops to wide area wireless network and ultimately go into internet or private internet.
- 3rd party Communications Control Centre uses MVNO (mobile virtual network operator),
  - Provides access for you and your equipment globally to cellular network.

CONTD…

- An MVNO enters into a business agreement with a mobile network operator to obtain bulk access to network services at wholesale rates, then sets retail prices independently.
- An MVNO may use its own customer service, billing support systems, marketing, and sales personnel, or it could employ the services of a Mobile Virtual Network Enabler (MVNE).
- As there can be multiple customers globally , we can have a support and maintenance centre for our self and customers may also have their support and maintenance system.
- So the customers are basically connected to the 3rd party Communication Control Centre and support and maintenance centre.

IoT Example - Smart Agriculture

- A sensor area network,
  - sensors are connected in mesh and can talk to each other through local gateway.
- Local gateway may speak cellular or it might be wired/Fibre.
- We have Farm UI and Control of the gateway and
- Information goes for some local processing and there will be some remote processing.
- Using LPWAN technology we don't require the local gateway as we can directly connect the sensors to wide area network
  - but it can create a problem because now we need a communication line between support and maintenance centre and Farm UI and Control.



UI: User Interface

CONTD…

- The data which is being gathered needs to come back to somebody who makes decision (Farm UI & Control).
- The whole point behind IoT concept is to collect data, process it and change (optimize) something.
- Local storage and some remote storage of data is required.
  - So we could actually go through the wide area networks.

Summary

- Internet technology connecting devices, machines and tools to the internet by means of wireless technologies.
- Over 9 billion ‘Things’ connected to the Internet, as of now.
- ‘Things’ connected to the Internet are projected to cross 20 billion in the near future.
- Unification of technologies such as low-power embedded systems, cloud computing, big-data, machine learning, and networking.

Thank You

Introduction to 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 (UIDs) and the ability to transfer data over a network without requiring human-to-human or human-to-computer interaction.

- A ***thing*** in the IoT can be a person with a heart monitor implant, a farm animal with a biochip transponder, an automobile that has built-in sensors to alert the driver when tire pressure is low or any other natural or man-made object that can be assigned an IP address and is able to transfer data over a network.

- IoT is a sensor network of billions of *smart devices* that connect people, systems and other applications to collect and share data.

- An IoT system consists of web-enabled smart devices that use embedded processors, sensors and communication hardware to collect, send and act on data they acquire from their environments.

- IoT devices share the sensor data they collect by connecting to an IoT gateway or other edge device where data is either sent to the cloud to be analysed or analysed locally.

Introduction to IoT

- IoT is a concept of connecting any device with an on and off switch to the Internet (and/or to eac other). This includes everything from cell phones, coffee makers, washing machines, headphones, lamps, wearable devices and almost anything else you can think of. This also applies to components of machines, for example a jet engine of an airplane or the drill of an oil rig.

- The IoT is a giant network of connected "things" (which also includes people). The relationship will be between people-people, people-things, and things-things.

- The dominant *consumer IoT device*, worldwide, is the smart TV. Between 25-35% cent of consumers worldwide own a television that can connect to the Internet, according to a Deloitte research. However, other areas of the IoT market are growing rapidly.

- Organizations in a *variety of industries* are using IoT to operate more efficiently, better understand customers to deliver enhanced customer service, improve decision-making and increase the value of the business.

- In mathematical language IoT can be defined as

$$IoT = \text{Sensor} + \text{Network} + \text{Data} + \text{Services}$$

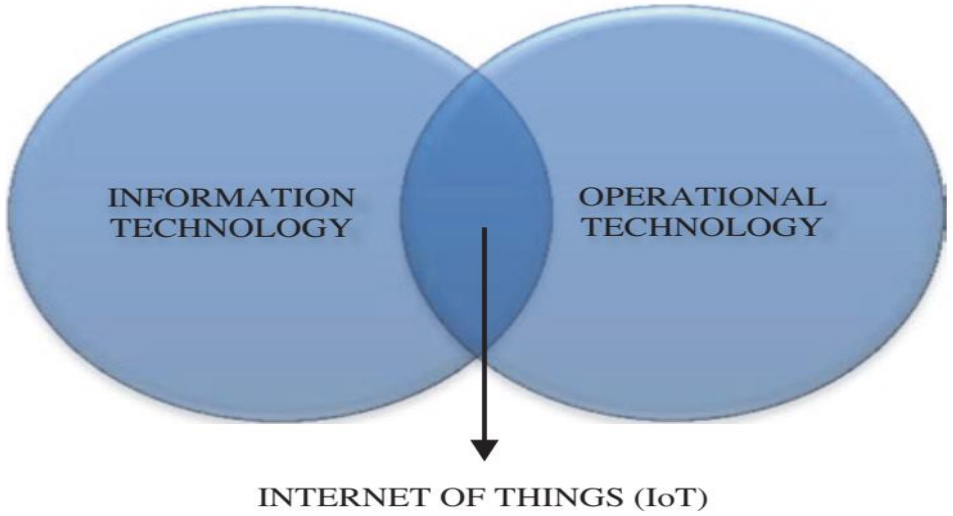
Introduction to IoT

- IoT can be explained by a Venn diagram where two different sets namely Information Technology (IT) and Operational Technology (OT) unite to form Internet of Things.

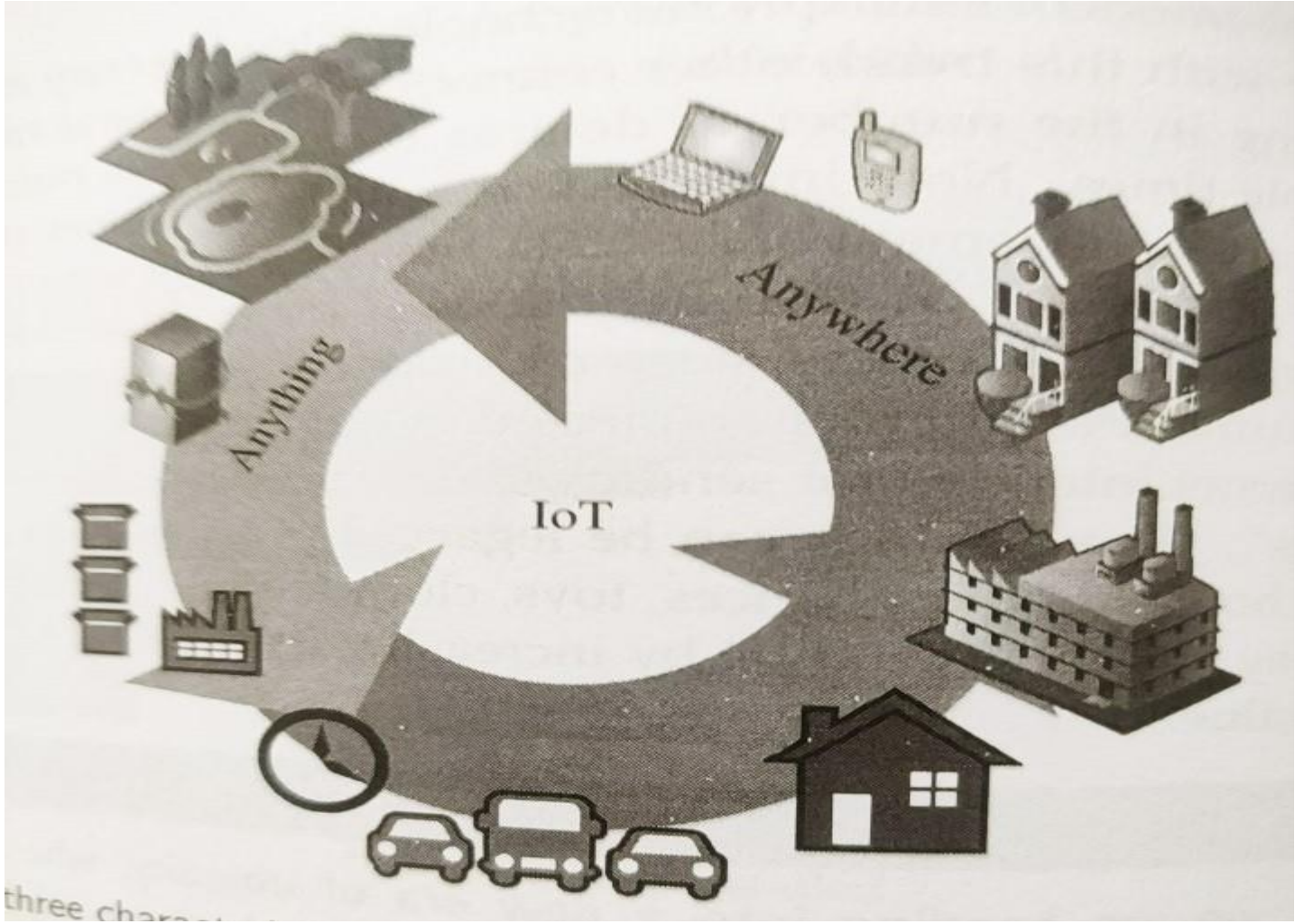
- The IT domain consists of ‘things ‘like servers, databases and applications. These ‘things’ run on the network and are controlled by IT. IT assists secure connectivity of the data and gadgets for smooth flow within the vicinity of an organization.

- The OT is generally concerned with the industrial work and contains ‘things’ like sensors and devices connected to the machines or some other equipment. It supervises devices and processes on physical systems.

.



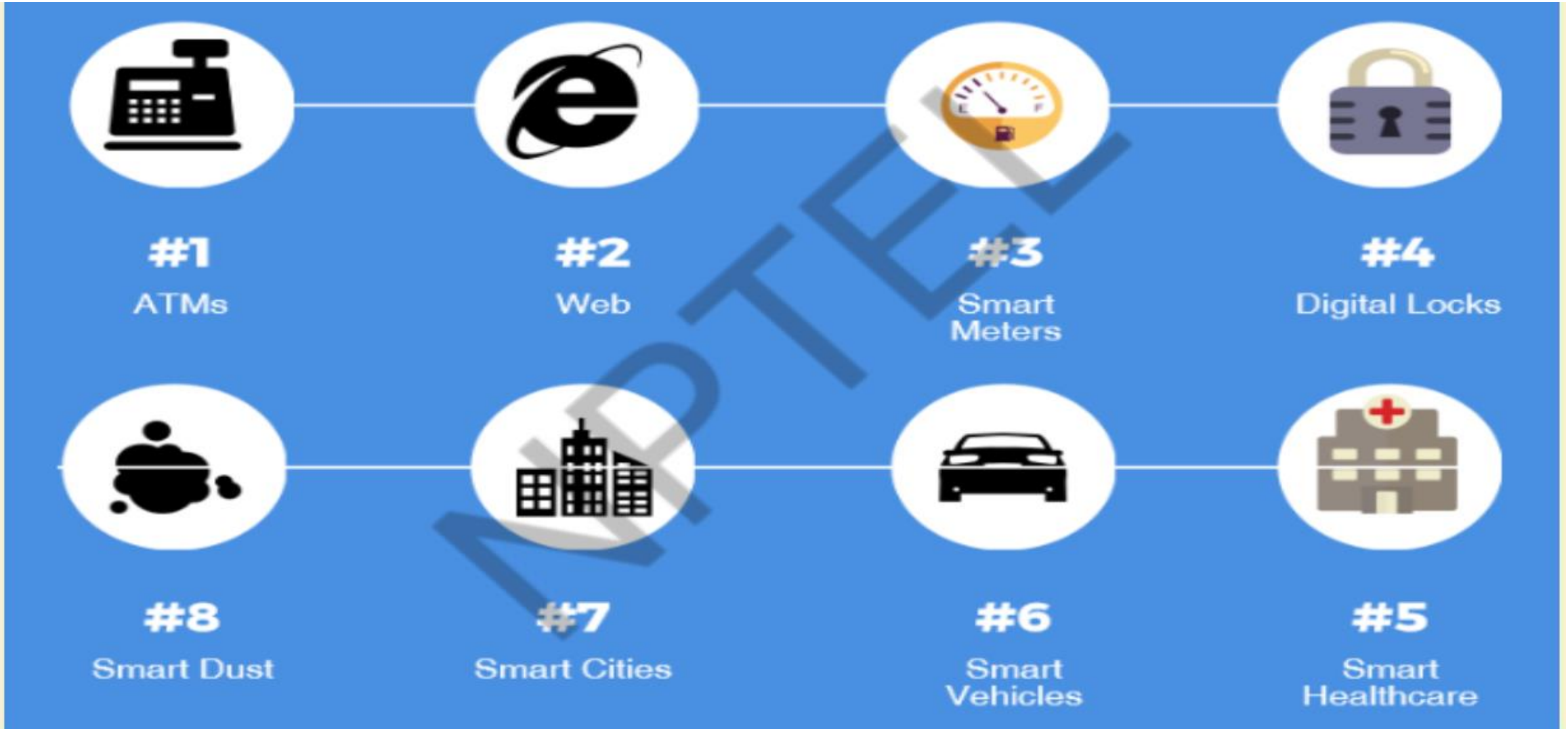
Characteristics feature of IoT



- Any time
- Any where
- Anything

- This feature highlights the robustness and dynamic nature of IoT.

Evolution of IoT



Evolution of IoT

- ATM (Automated teller machine)
  - ✓ These ubiquitous money dispensers went online for the first time way back in 1974.
  - ✓ The cash distribution machine is linked to the user's bank account.
  - ✓ It dispenses cash upon verification of the identity of user and their account through a special coded card.
  - ✓ Availability of financial transactions even when banks are closed.

- WEB
  - ✓ World Wide Web made its debut in 1991 to revolutionize computing and communications.
  - ✓ It is a global information sharing and communication platform.

- SMART METERS
  - ✓ The first power meters to communicate remotely with the grid were installed in the early 2000s.
  - ✓ These are capable of communicating remotely with the power grid.
  - ✓ They enabled remote monitoring of subscriber's power usage and eased the process of billing and power allocation from grids.

Evolution of IoT

- DIGITAL LOCKS
  - ✓ Smartphones can be used to lock and unlock doors remotely, and business owners can change key codes rapidly to grant or restrict access to employees and guests.
  - ✓ It can be considered as an attempt to connected home automation system.

- SMART HEALTHCARE
  - ✓ Healthcare devices connected to hospitals, doctors and relatives to alert them of medical emergencies and take preventive measures.
  - ✓ The devices may be simple wearable appliances, monitoring the heart rate and pulses of the wearer, and the medical devices that monitors in the hospitals.
  - ✓ These systems makes the availability of medical records and test results much faster, cheaper and convenient for both patients and hospital authorities.

- SMART VEHICLES
  - ✓ Vehicles self-diagnose themselves and alert owners about system failures.
  - ✓ They communicate to the Internet, or with other vehicles, or sensors and actuators contained within it.

Evolution of IoT

- SMART CITIES
  - ✓ City-wide infrastructure communicating amongst themselves for unified and synchronized operations and information dissemination.
  - ✓ This is a city wide implementation of smart sensing, monitoring, and actuation system.

- SMART DUST
  - ✓ Microscopic computers (smaller than a grain of sand) can be sprayed or injected almost anywhere to measure chemicals in the soil or to diagnose problems in the human body

- SMART FACTORIES
  - ✓ They can monitor plant processes, assembly lines, distribution lines, and manage factory floors.
  - ✓ The reduction in mishaps due to human errors in judgement or unoptimized process is drastically reduced.

- UAVs(Unnamed aerial vehicles)
  - ✓ It is a public domain solutions tasked with application ranges from agriculture, surveys, surveillance, deliveries, stock maintenance, asset management and other tasks.

Evolution of IoT

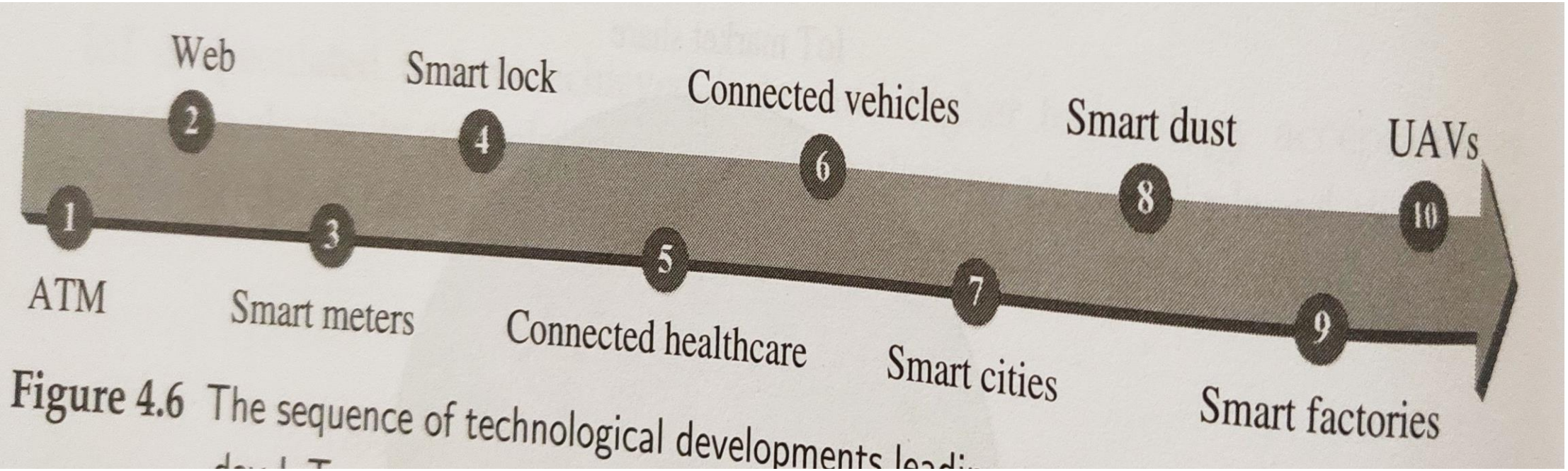
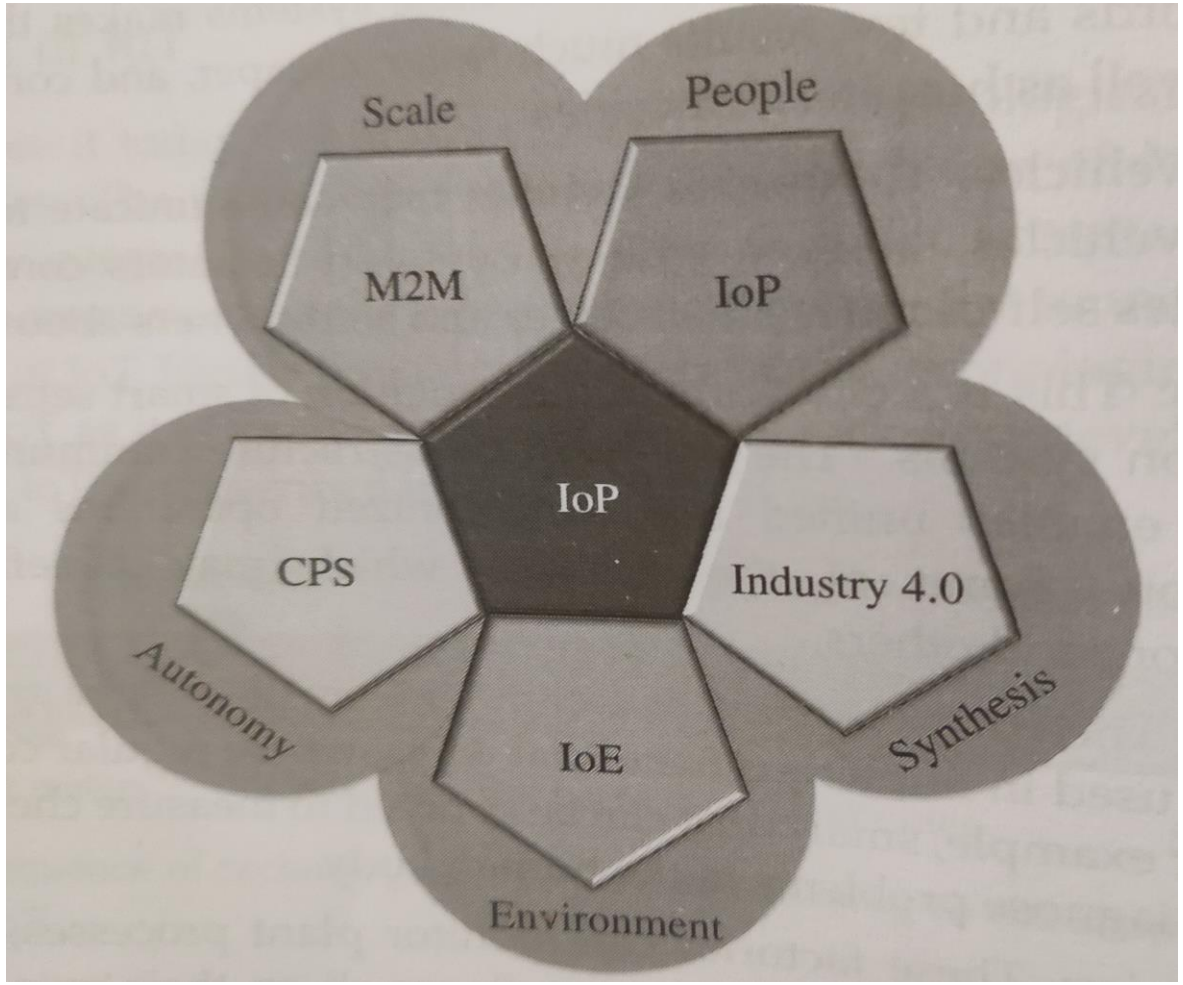


Figure 4.6 The sequence of technological developments leadi

Interdependence and reach of IoT over various application domains and networking paradigm



Interdependence and reach of IoT over various application domains and networking paradigm

M2M

- This signifies a system of connected machines and devices which can talk among themselves without human intervention.

- The communication between the machine can be for updating machine status, collaboratives task completion, overall knowledge of the systems and the environments and others.

Interdependence and reach of IoT over various application domains and networking paradigm

CPS

- It is a closed control loop starting from sensing, processing, and finally to actuation using a feedback mechanisms.

- It helps in maintaining the state of the environment through the feedback control loop, which ensures that until the desired state is attained, the system keeps on actuating and sensing.
- Humans are simple supervisory role and ground level operations are automated.

Interdependence and reach of IoT over various application domains and networking paradigm

IOE

- It minimizes and reversing the ill effects of the permeations of Internet based technologies on the environments.

- The major focus area includes smart and sustainable farming, sustainable and energy efficient habitats, enhancing the energy efficiency of the systems and processes.

Interdependence and reach of IoT over various application domains and networking paradigm

Industry 4.0

- It includes digitization of manufacturing industries.
- It puts forward the concept of smart factories where machines can talk to one another without human involvement.
- It translates to better resource and workforce management, optimization of production time and resources, and better keep up and lifetimes of industrial systems.

Interdependence and reach of IoT over various application domains and networking paradigm

IoP

- A new technological movement on the Internet which aims to decentralize online social interactions, payments, transactions and other task while maintaining the confidentiality and privacy of users data
- A famous site for IoP is Bitcoin.

Baseline Technologies

A number of technologies that are very closely related to IoT include

- ✓ Machine-to-Machine (M2M) communications
- ✓ Cyber-Physical-Systems (CPS)
- ✓ Web-of-Things (WoT)

IoT vs. M2M

- M2M refers to communications and interactions between machines and devices.
- Such interactions can occur via a cloud computing infrastructure (e.g., devices exchanging information through a cloud infrastructure).
- M2M offers the means for managing devices and devices interaction, while also collecting machine and/or sensor data.
- M2M is a term introduced by telecommunication services providers and, pays emphasis on machines interactions via one or more telecom/communication networks (e.g., 3G, 4G, 5G, satellite, public networks)

IoT vs. M2M

- **M2M is part of the IoT, while M2M standards have a prominent place in the IoT standards landscape.**
- However, IoT has a broader scope than M2M, since it comprises a broader range of interactions, including interactions between devices/things, things and people, things with applications and people with applications.
- It also enables the composition of workflows comprising all of the above interactions.
- IoT includes the notion of internet connectivity (which is provided in most of the networks outlined above), but is not necessarily focused on the use of telecom networks.

IoT vs. CPS

- CPS is a digital twin.
- Digital twin is a *virtual system-model* relation.
- A system includes a physical system or equipment or a piece of machinery.
- Model represents a mathematical model or representation of physical systems behavior or operation.
- In CPS, digital twin allows for the comparison of the physical systems output, performance, and health.
- Based on feedback from the digital twin, a physical system can easily given corrective direction/commands to obtain the desirable outputs.

IoT vs. CPS

- IOT does not compulsory need digital twin system.
- IoT puts more focus on networking but not on control.
- Some of the constituent sub system of IoT may include feedback and control.
- CPS may be considered as one subdomain of IoT.

IoT vs. WoT

- From a developer's perspective, the WoT enables access and control over IoT resources and applications using mainstream web technologies (such as HTML 5.0, JavaScript, Ajax, PHP, Ruby n' Rails etc.).

- The approach to building WoT is therefore based on RESTful principles and REST APIs, which enable both developers and deployers to benefit from the popularity and maturity of web technologies.

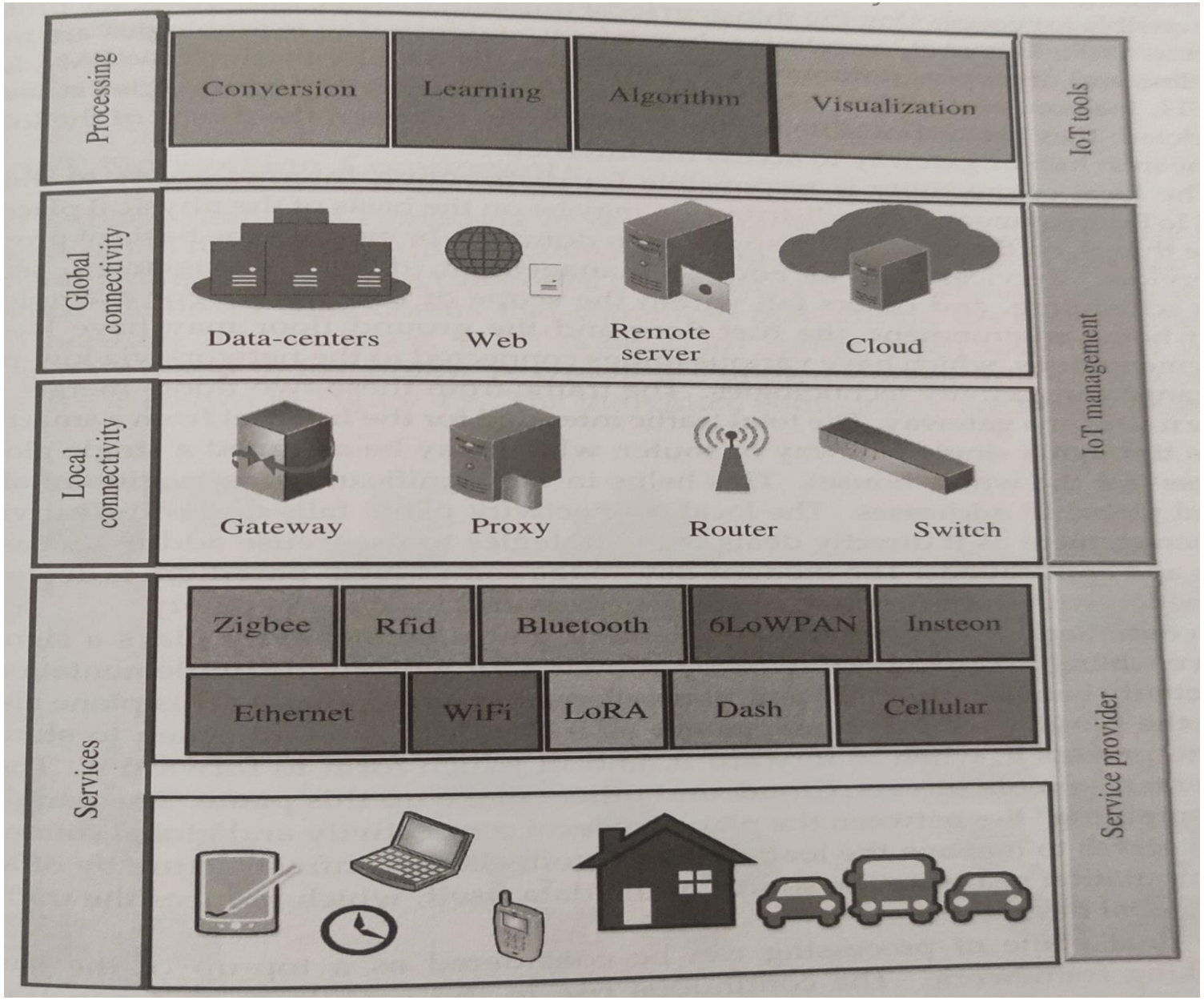
- Still, building the WoT has various scalability, security etc. challenges, especially as part of a roadmap towards a global WoT.

IoT vs. WoT

- While IoT is about creating a network of objects, things, people, systems and applications, WoT tries to integrate them to the Web.

- Technically speaking, WoT can be thought as a flavour/option of an application layer added over the IoT's network layer. However, the scope of IoT applications is broader and includes systems that are not accessible through the web (e.g., conventional WSN and RFID systems).

Enabling IoT and complex interdependence of technolog



Enabling IoT and complex interdependence of technologies

- IoT paradigm is divided into *four* planes.
- They are

  ✓Services

  ✓Local connectivity

  ✓Global connectivity

  ✓Processing

Enabling IoT and complex interdependence of technologies

Services

- It falls under the purview of service providers.
- It is composed of two parts.

1. Things or devices (Example:- wearables, computers, smartphones, household appliances, smart glasses, etc.)
2. Low power connectivity(IEEE802.15.4 protocol,RFID,Bluetooth,6LowPAN, etc.)

Enabling IoT and complex interdependence of technologies

Local connectivity

- It is responsible for distributing Internet access to multiple local IoT deployments.
- It handles address management, device management, security, sleep scheduling.

Global connectivity

- Allowing worldwide implementation and connectivity between things, users, controllers, and applications.
- It decides how and when to store data, when to process it, when to forward it, and in which form to forward it.
- Example:-Data centre, remote server, cloud

Enabling IoT and complex interdependence of technologies

Processing

- It includes intelligence, conversation, learning, algorithms, visualization and analysis of the information with respect to the application.
- Example:-Bigdata, machine learning

IoT Networking Components

- The components of IoT network includes

  - ✓IoT node
  - ✓IoT router
  - ✓IoT LAN
  - ✓IoT WAN
  - ✓IoT Gateway
  - ✓IoT Proxy

IoT Networking Components

IoT node

- These are the networking devices within the IoT LAN.
- Each IoT node contains a sensor, a processor, and a radio.
- A IoT node may be connected to another IoT node inside a LAN directly or by a common gateway of that LAN.
- A IoT node may be connected to outside LAN through gateways and proxies.

IoT Networking Components

IoT router

- It is a networking equipment responsible for routing of packets between various IoT entities in the network.
- It keeps traffic flowing correctly within the network
- A router can be repurposed as a gateway by enhancing its functionalities.

IoT Networking Components

IoT LAN

- LAN enables local connectivity within the purview of a single gateway.
- LAN consist of short range connectivity technology.
- It may or may not connected to the Internet.
- It is localized within a building or an organization.

IoT Networking Components

IoT WAN

- It connects to various LANs.
- They are organizationally and geographically wide with their operational range laying between a few kilometers to hundreds of kilometers.
- It is connected to Internet.
- It enables Internet access to the segments they are connecting.

IoT Networking Components

IoT Gateway

- It is a router connecting the IoT LAN to a IoT WAN or the Internet.
- It can implement several LAN and WAN.
- It forwards packets between LAN and WANs.

IoT Networking Components

IoT Proxy

- It lies in the application layer
- It performs application layer functionalities between IoT node and other entities present in the network.
- It provides security to the network entities.
- It helps to extend the addressing range of its network.
- It contains the feature of firewalls, packet filters, security and routing operations.

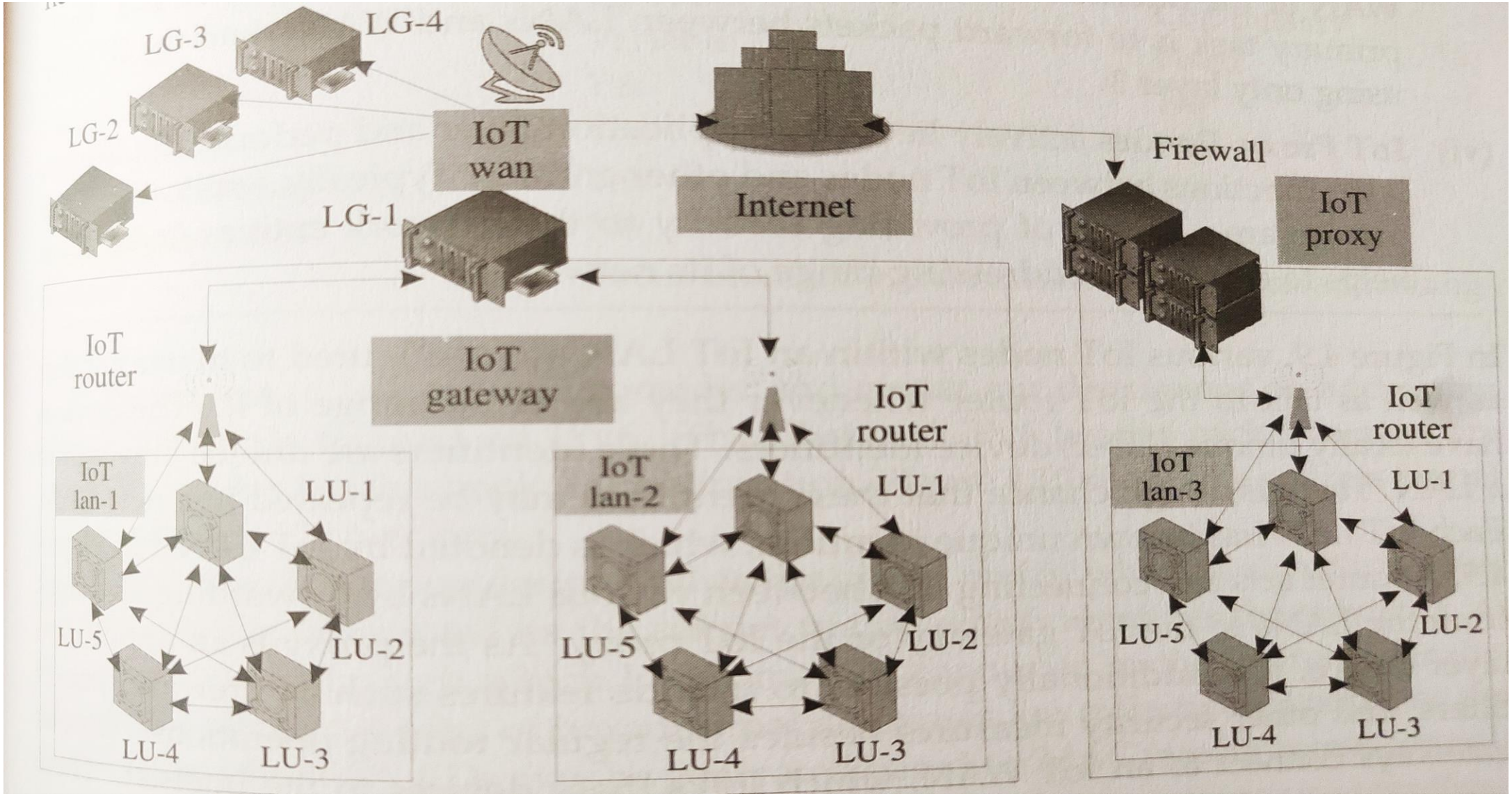


Fig 1:IoT Network ecosystem highlighting the various networking components (from IoT node to Internet)

Description about the IOT ecosystem in Fig:1

- This figure contains *three* IoT LANs having unique identifier IoT LAN-*x*.
- *Five* IoT node (having id locally unique(LU-*x*) is used to form a IoT LAN.
- Each IoT node have unique identifier within its LAN.
- Each IoT node can communicate with each other or with the IoT router.
- Each IoT router can forwards the packets from IoT LAN to IoT gateway or IoT proxy.
- Each IoT gateway have unique identifier LG-*x*(Local gateway-x).
- Two or more IoT gateway are connected to form a IoT WAN.
- IoT WAN is connected to Internet.
- Then all IoT nodes can access the Internet.
- At the place of IoT gateway IoT proxy can be used which also connected to Internet for data exchange.

Addressing strategies in IoT

- IPv6 is used for IoT addressing.
- It has three components.
  - ✓ *Global prefix*
  - ✓ *Subnet prefix*
  - ✓ *Interface identifiers*

Global prefix

- It is globally unique.
- First three blocks of the address is called global prefix.

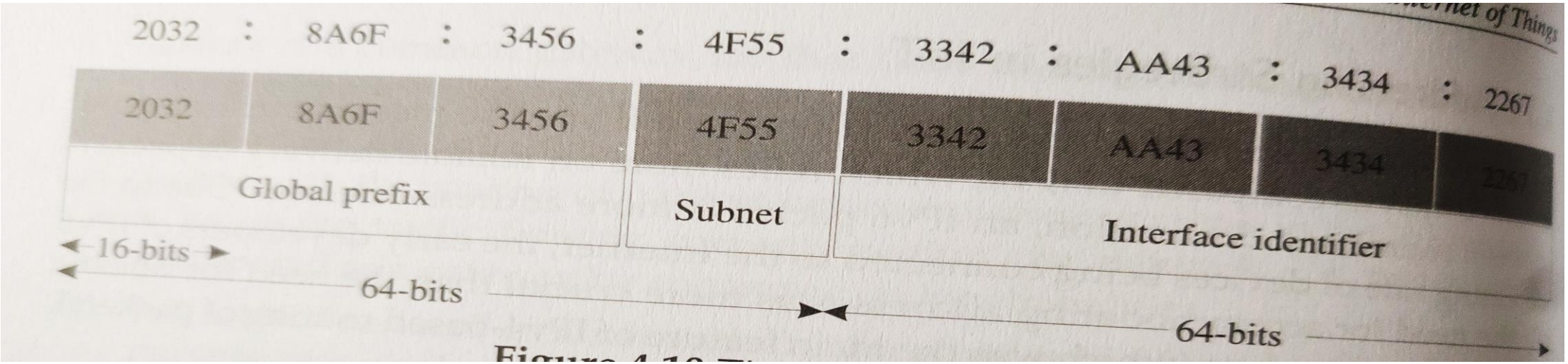
Subnet prefix

- It identifies the subnet of an interface/gateway through which LANs may be connected to the Internet.

Interface identifiers

- The last four blocks (64 bits) of hexadecimal addresses are called interface identifiers.
- IIDs may be generated based on MAC (media access control) identifiers of devices/nodes or using pseudo-random number generator algorithms.

The IPv6 address format

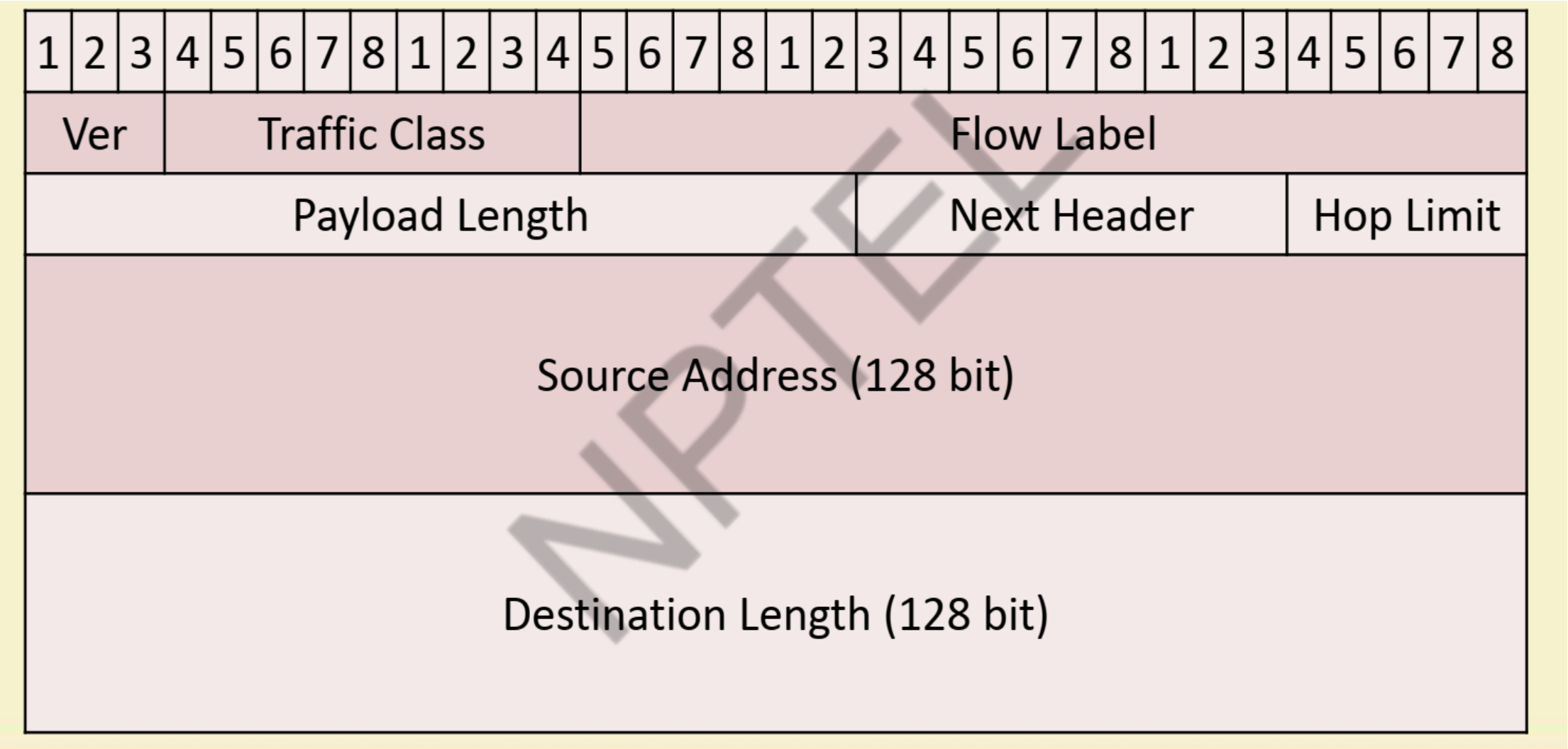


Example:

IPv6 address :- 1034:7B6F:1345:4E44:1234:AAAA:5B78:3421

Global prefix:-1034:7B6F:1345
Subnet:-4E44
Interface identifiers:-1234:AAAA:5B78:3421

IPv6 Header format



NPTEL

Features of IPv6

- The IPv6 header structure is more simpler as it mainly focuses on the addressing part of the source and destination.
- It is concerned more with addressing than with reliability of data delivery.

Difference between IPv4 and IPv6

Si. No	Feature	IPv4	IPv6
1	Developed	IETF 1974	IETF1998
2	Address Length	32	128
3	Number of addresses	2^{32}	2^{128}
4	Notation	Dotted decimal	Hexadecimal
5	Dynamic allocation of addresses	DHCP	DHCPv6, SLAAC
6	IP Security	Optional	Compulsory
7	Header size	Variable	Fixed
8	Header checksum	Yes	No
9	Header options	Yes	No
10	Broadcast Address	Yes	No
11	Multicast Address	No	Yes
12	Feature	Focus on reliable transmission	Focus on addressing

IPv6

IPv6 addresses can be divided into seven separate address types based on how these addresses are used or where they are deployed.

1. Global unicast (GUA)
2. Multicast
3. Link local(LL)
4. Unique local(ULA)
5. Loop back
6. Unspecified
7. Solicited-node Multicast

IPv6

1.Global Unicast(GUA)

- These addresses are assigned to single IOT entities/interface.
- They enable the entities to transmit traffic to and from Internet.
- Normally these addresses are assigned to IoT Gateway, Proxies or WANs

2. Multicast

- These addresses enable transmission of messages from a single networked entities to multiple destination entities simultaneously.

3.Link local(LL)

- The operational domain of these addresses are valid within a LAN.
- These addresses may be repeated in other LAN.
- All the addresses are unique within a LAN.

4.Unique local(ULA)

- These addresses are not routed over the Internet.
- These addresses may be repeated in other LAN.
- All the addresses are unique within a LAN.

IPv6

5. Loop Back

- It is also known as local host address.
- These addresses are used by developers and network tester for diagnostics and system checks.

6.Unspecified

- All the bits in the IPv6 are set to zero
- Destination addresses are not specified.

7.Solicited node multicast

- It is a multi cast address based on IPv6 address of an IoT node or entity.

Address management Class

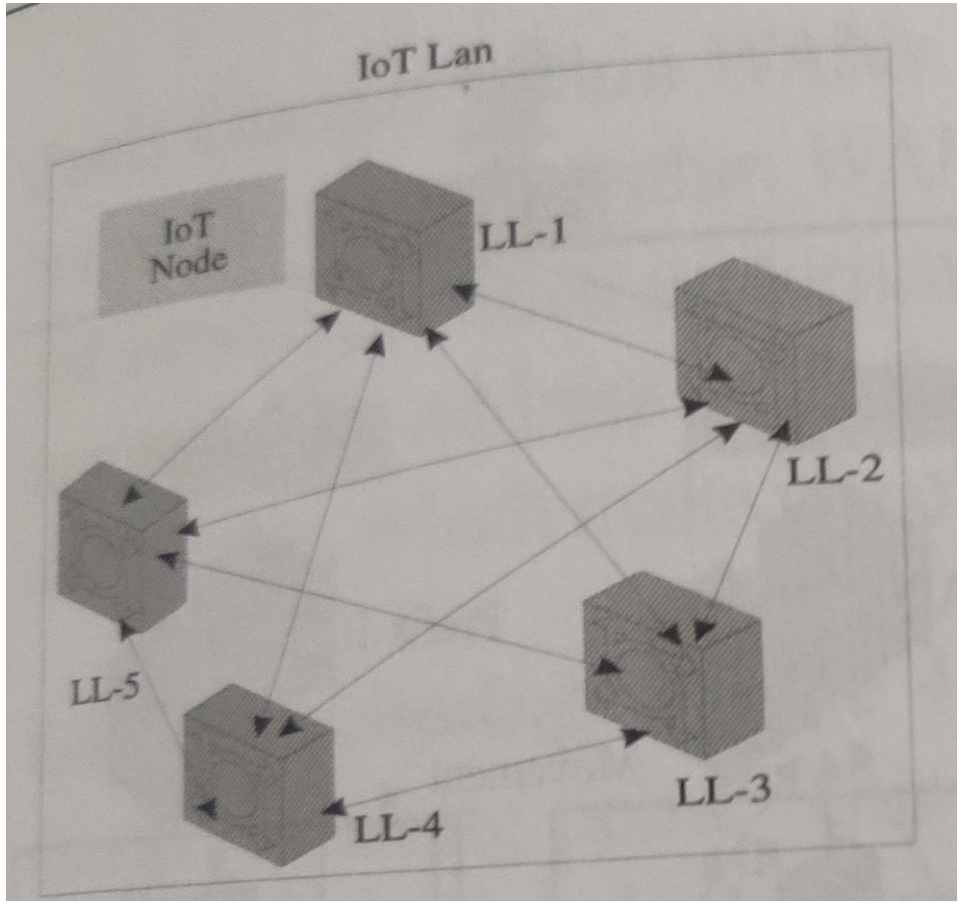
The addressing strategies in IoT are broadly classified into seven classes. These classes are

- Class 1
- Class 2
- Class 3
- Class 4
- Class 5
- Class 6
- Class 7

Address management Class

Class 1:

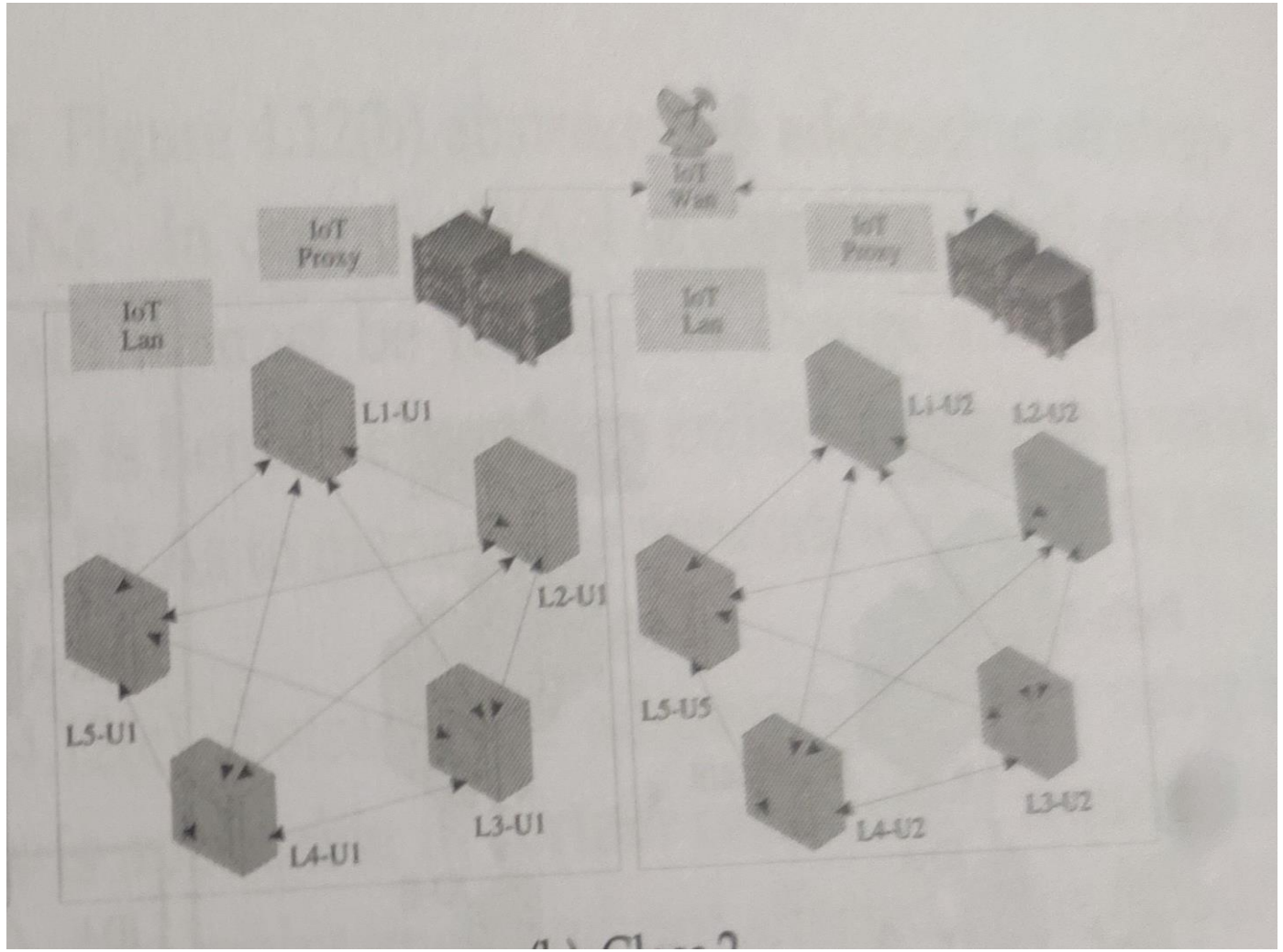
- Communication between IoT nodes are restricted within the LAN only.
- This is a isolated class.
- IoT nodes are identified by their LL addresses.
- The IoT node within the LAN may follow mesh topology



Address management Class

Class 2:

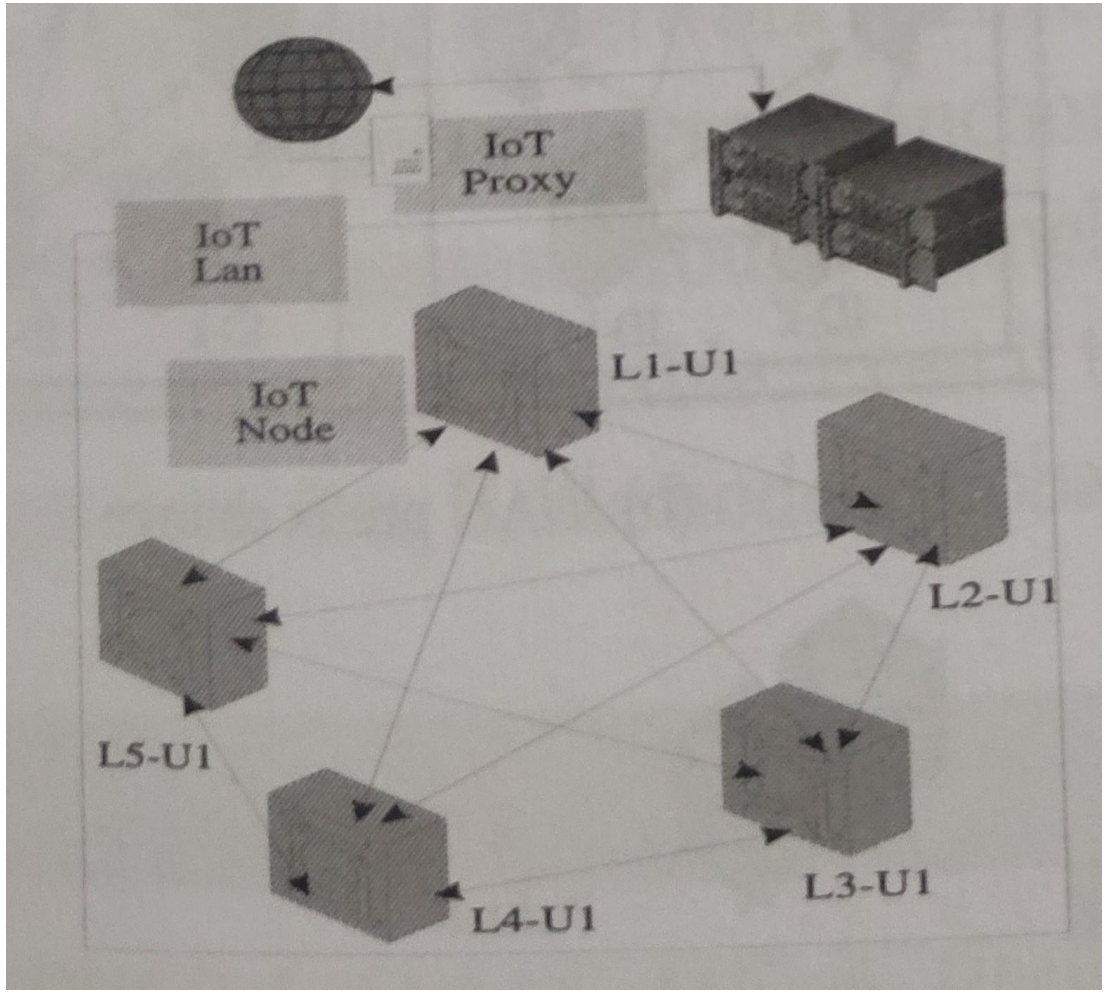
- ULA and GUA are used for addressing class 2 IoT nodes.
- L1-L5 are LL addresses of locally unique IoT nodes within the LANs.
- U1,U2 are the unique addresses of the two gateways.
- These gateways establishes a WAN and may or may not connected to the Internet.



Address management Class

Class 3:

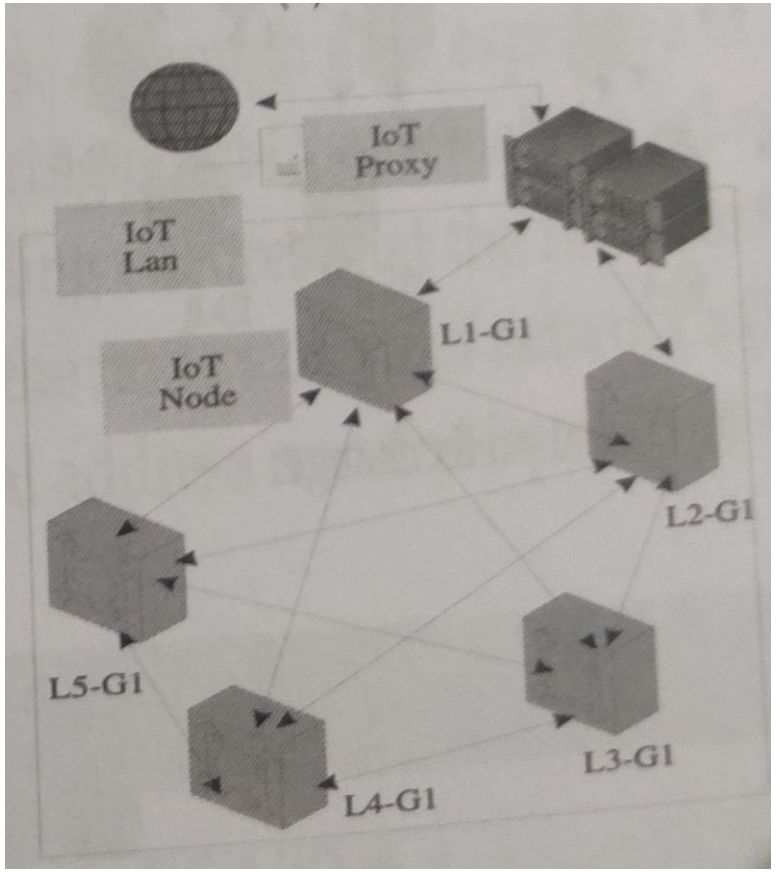
- IoT LAN is connected to an IoT proxy.
- IoT proxy performs a host of functions ranging from address allocation, address management to provide security to the network
- IoT proxy uses ULA address(L*x*-U*x* *pair*).



Address management Class

Class 4:

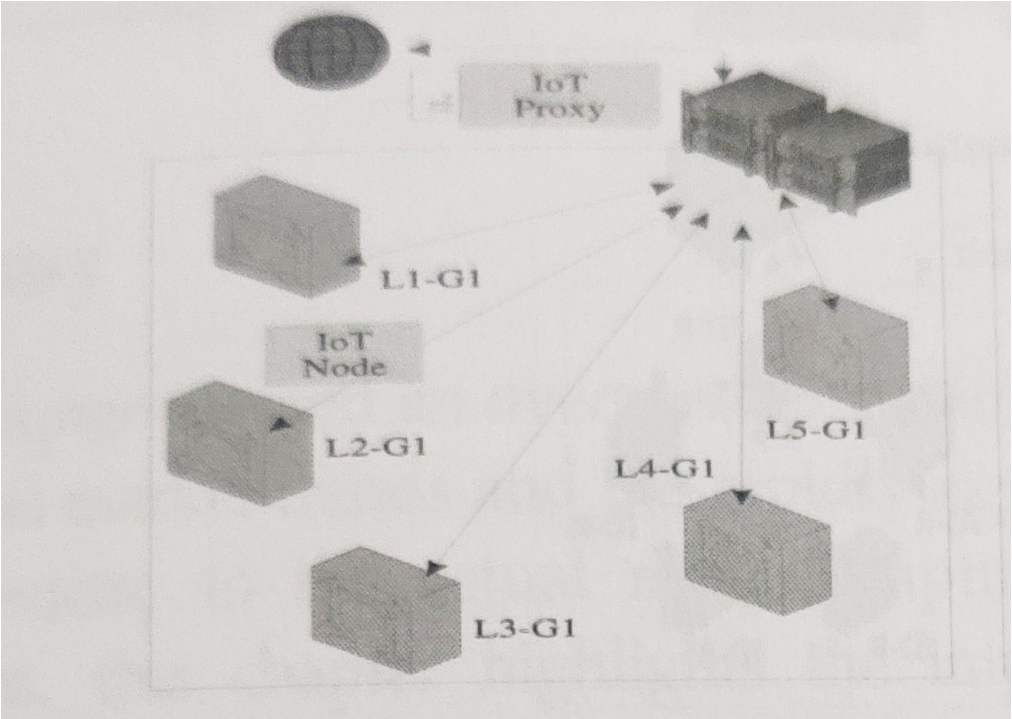
- IoT proxy acts as a gateway between the IoT LAN and Internet.
- It provides GUA to the IoT nodes within the IoT LAN.
- A globally unique prefix is allocated to this gateway, which is used with the individual device identifiers to extend global Internet connectivity to the IoT nodes
- IoT gateway enables local communication between the nodes without the need for packets to be routed through the Internet.
- IoT nodes within the gateway can talk to one another directly without always involving the gateways.
- A proxy beyond the gateway enables global communication through the Internet.



Address management Class

Class 5:

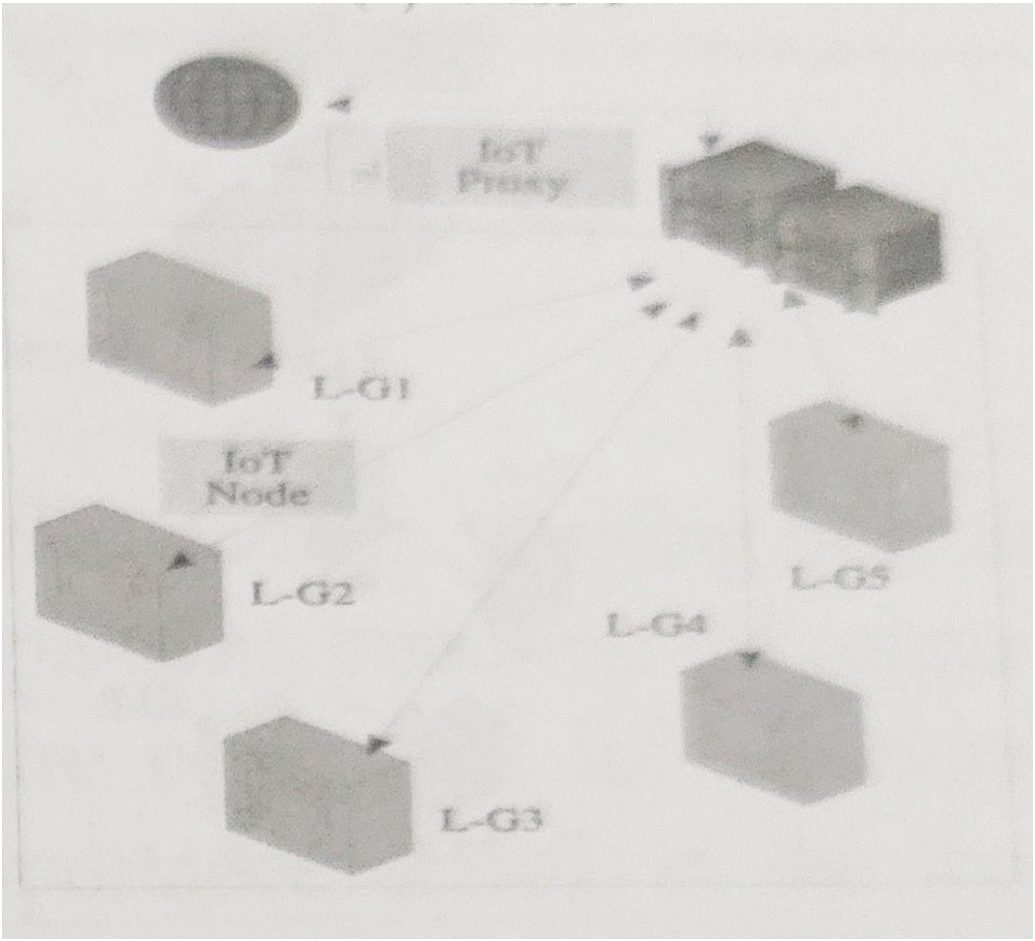
- Functionally similar to class 4.
- It follows star topology with the LAN gateway as the centre of the star.
- All the communication from the IoT nodes under the gateway has to go through the gateway.
- A proxy beyond the gate way enables global communication through the Internet.
- The IoT nodes within the gateways operational purview have the same GUA.



Address management Class

Class 6:

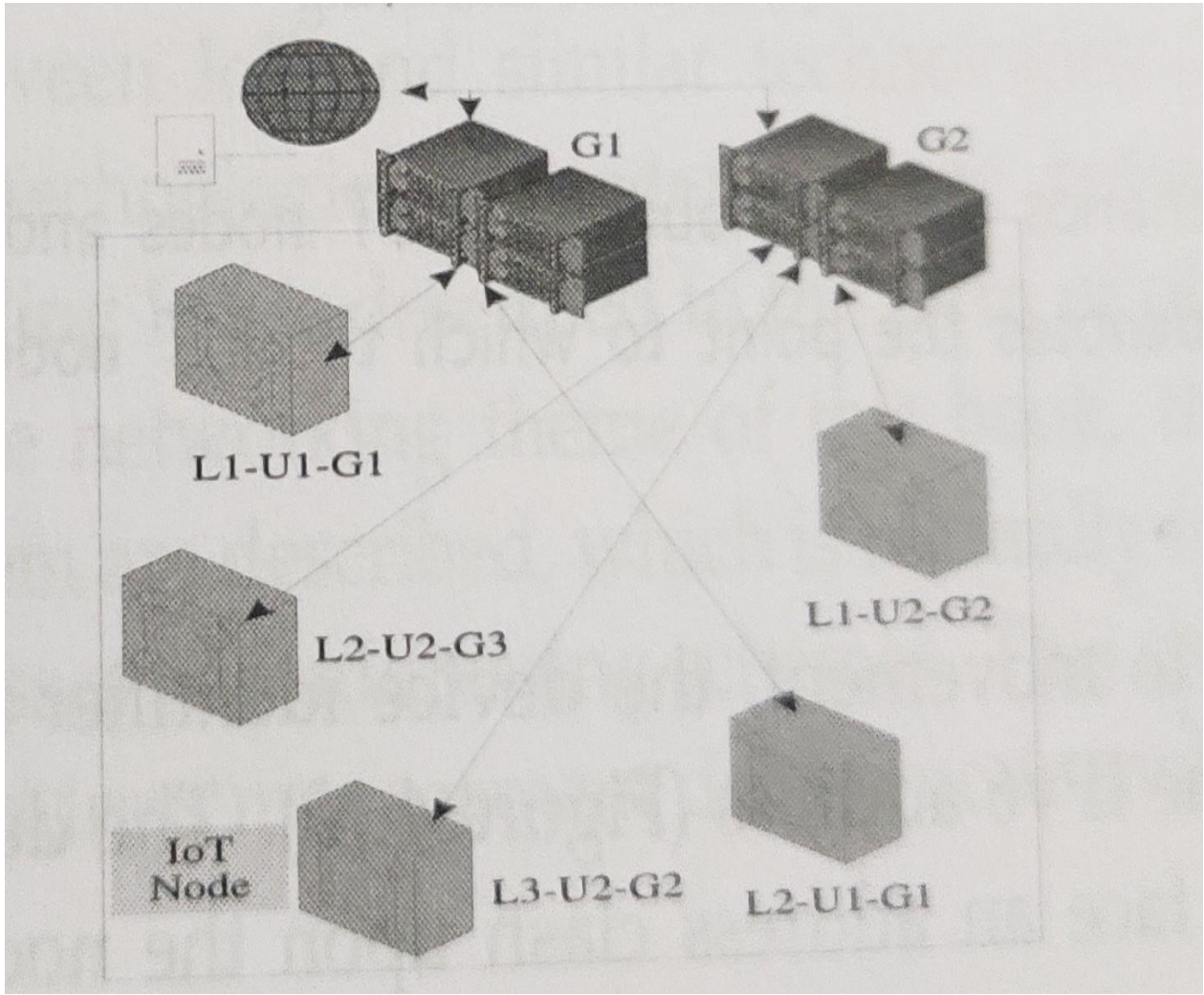
- The configuration is similar to class 5.
- All IoT nodes are assigned unique global address(UGA).
- All IoT nodes enables point-to-point communication network with the Internet gateway.
- It is selectively used for some special purposes.



Address management Class

Class 7:

- Multiple gateways may be present.
- IoT node should be reachable through any gateways.
- Organizational IoT deployment may follow this class of configuration.
- It uses multihoming concepts.



Multihoming in IoT networks

- It is a network configuration in which a node/network connects to multiple networks simultaneously for improved reliability.
- In cases of small IoT LANs, where allotment of address prefixes is not feasible and possible, a proxy based approach is used to manage multiple IP addresses and map them to link local addresses.
- In another, gateway-based approach is used for assigning link local addresses to the nodes under it.
- Providing source addresses, destination addresses and routing information to the multi-homed nodes is the real challenge in multi-homing networks.

Multihoming in IoT networks

- In case the destination and source addresses originate from the same prefix, routing between gateways can be employed for IoT gateway selection.
- Presently, IEFT is still trying to standardize this issue.
- Network proxies are used to manage multiple IP addresses and map them to LL addresses of IoT nodes in small deployments.
- The allotment of addresses of prefixes is not possible.
- Gateways are responsible for allotment of LL addresses to IoT nodes under the gateway’s operational purview.

Tunneling

- It is a network protocol.
- It transfers data from a private network to a public network in the form of encapsulated packets.
- It is used for ensuring connectivity and security of data generated from various technologies and protocols that may not be supported over the public communication channel.
- Example: VPNs(Virtual private networks), Secure shell(SSH)

Addressing during node mobility

Addressing of mobile nodes are done in three ways.

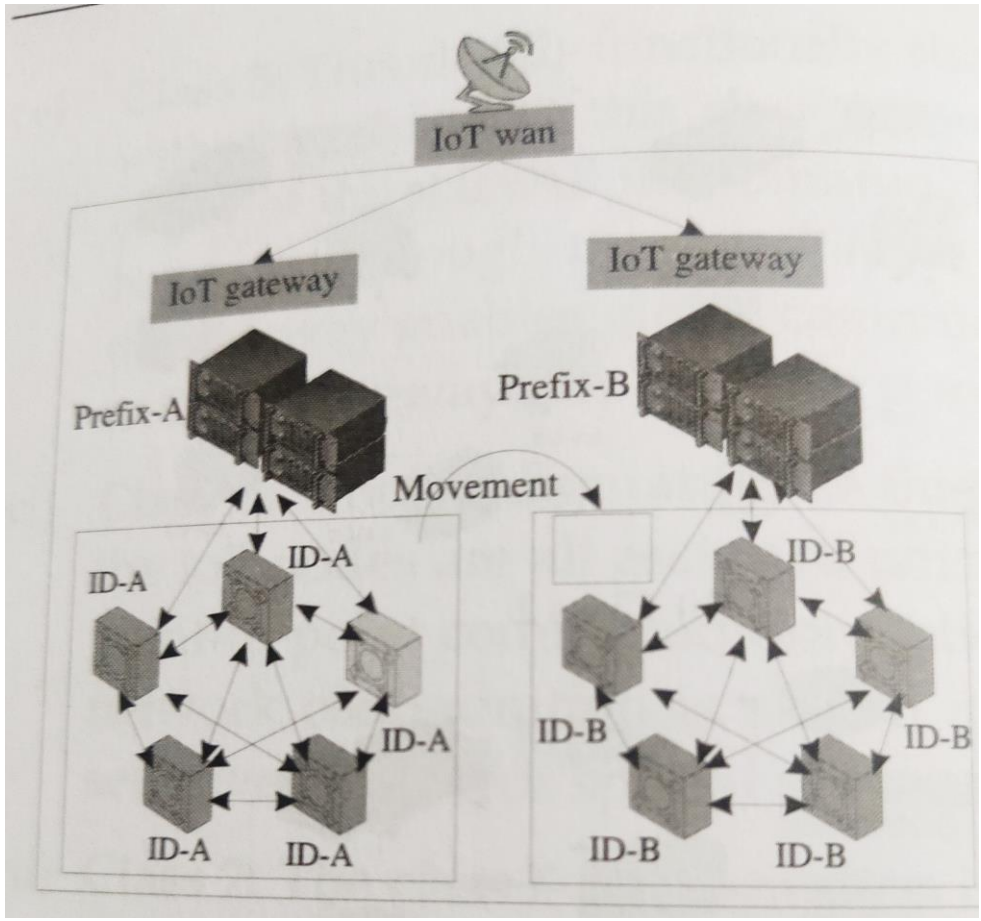
They are

1. *Global prefix changes*
2. *Prefix changes within WANs*
3. *Remote anchoring*

Addressing during node mobility

Global Prefix exchanges

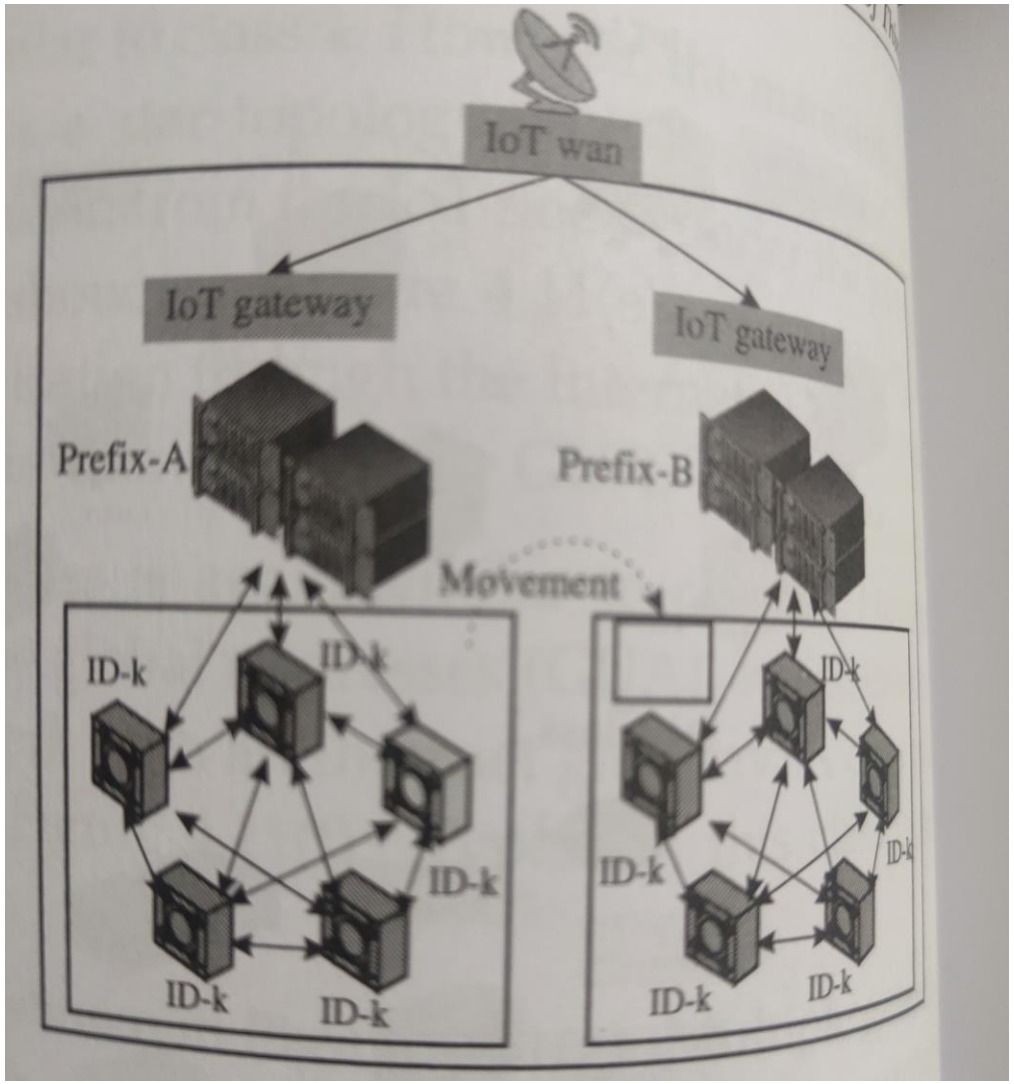
- A node from left LAN is moved to right LAN.
- A IoT node in left LAN have id **A** which changes to id **B**.
- Here addresses are assigned by DHCPv6/SLAAC.



Addressing during node mobility

Prefix exchanges within WANs

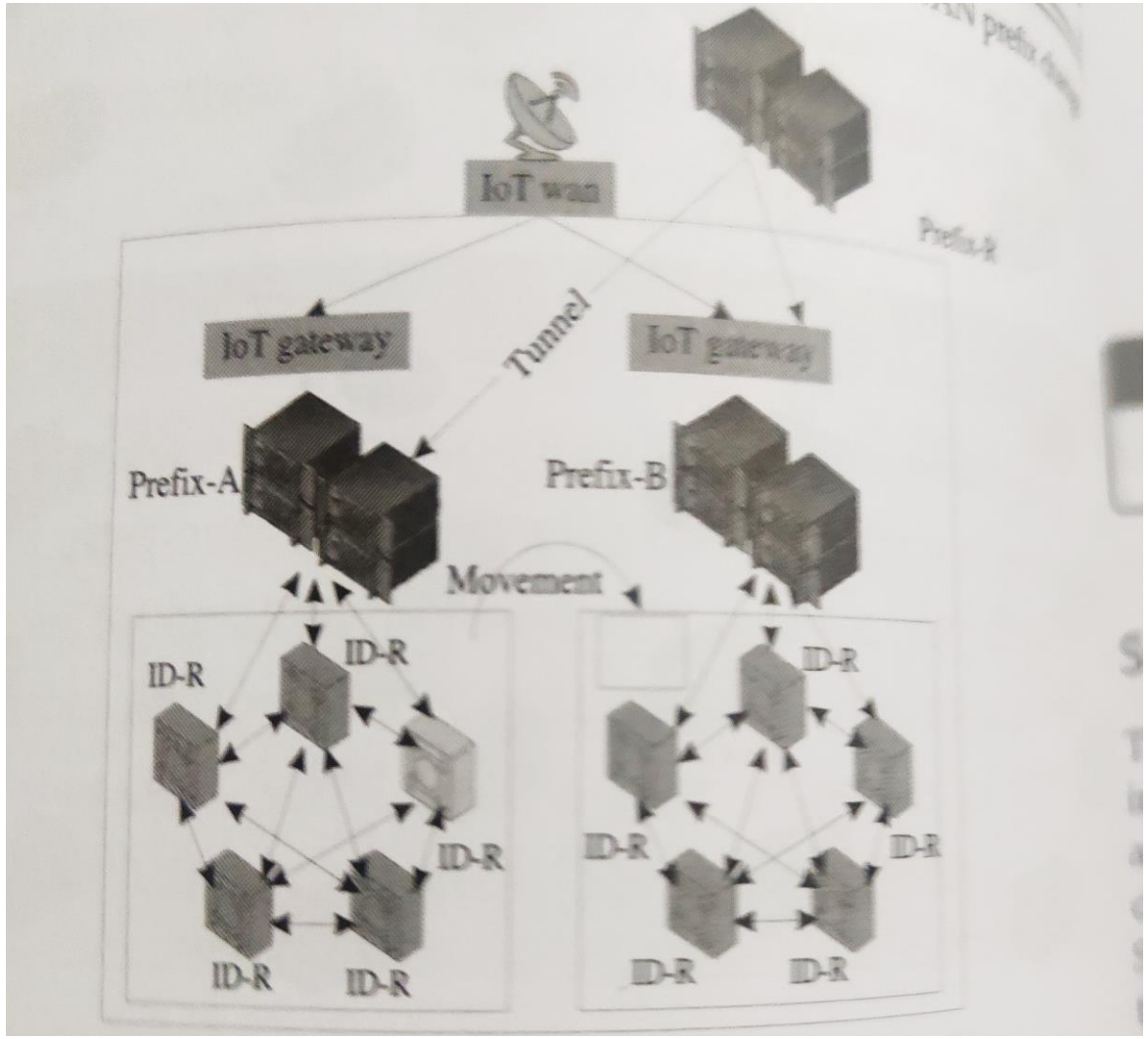
- The WAN changes its global prefix, the network entities underneath it must be resilient to change and function normally.
- The address allocation is delegated to entities such as gateways and proxies which makes use of ULAs to manage the networks within the WAN.



Addressing during node mobility

Remote Anchoring

- The IOT nodes global addresses are maintained by using remote anchoring.
- In this method, global addresses are not affected by its mobility or the change in network prefixies.
- Expensive methodology to implement.
- Here LAN addresses are changed from **A** to **B**, nodes global addresses remain unchanged.



Thank You

IoT Sensing and Actuation

- ✓ List of salient features of transducers
- ✓ Differentiate between sensors and actuators
- ✓ Characterize sensors and distinguish between types of sensors
- ✓ List the multi-faceted considerations associated with sensing
- ✓ Characterize actuators and distinguish between types of actuators
- ✓ List the multi-faceted considerations associated with actuation

Definition

- A sensor detects (senses) changes in the ambient conditions or in the state of another device or a system, and forwards or processes this information in a certain manner.

- *"A device which detects or measures a physical property and records, indicates, or otherwise responds to it".*

  - Oxford Dictionary

Sensors

- They perform some input functions by sensing or feeling the physical changes in characteristics of a system in response to a stimuli.

- For example heat is converted to electrical signals in a temperature sensor, or atmospheric pressure is converted to electrical signals in a barometer.

Transducers

- Transducers convert or transduce energy of one kind into another.

- For example, in a sound system, a microphone (input device) converts sound waves into electrical signals for an amplifier to amplify (a process), and a loudspeaker (output device) converts these electrical signals back into sound waves.

Actuators

- An actuator is a component of a machine or system that moves or controls the mechanism or the system.
- An actuator is the mechanism by which a control system acts upon an environment.
- An actuator requires a control signal and a source of energy.

Difference between transducers, sensors, Actuators

Parameters	Transducers	Sensors	Actuators
Definition	Converts energy from one form to another	Converts various forms of energy into electrical signals	Converts electrical signals into various forms of energy
Domain	Can be used to represent a sensor as well as a transducer	It is an input transducer	It is an output transducer
Function	Can work as a sensor or an actuator but not simultaneously	Used for quantifying environmental stimuli into signals	Used for converting signals into proportional mechanical or electrical outputs
Example	Any sensor or actuator	Humidity sensors, Temperature sensors, Gas sensors	Motors, Force heads

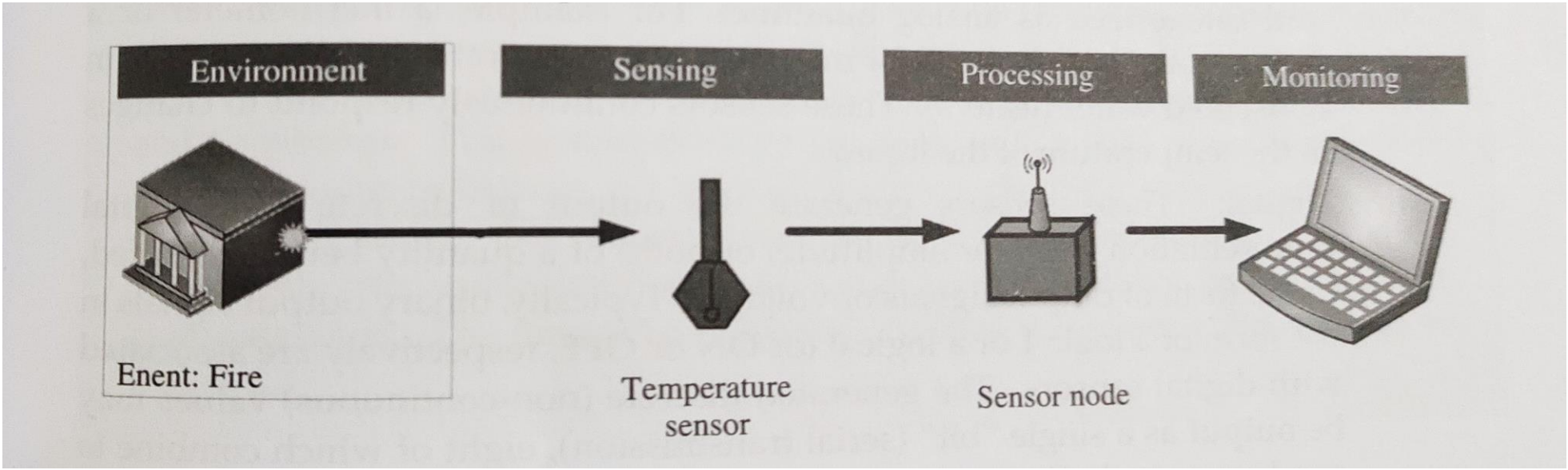
Sensor Features

- It is only sensitive to the measured property (e.g., A temperature sensor senses the ambient temperature of a room.)

- It is insensitive to any other property likely to be encountered in its application (e.g., A temperature sensor does not bother about light or pressure while sensing the temperature.)

- It does not influence the measured property (e.g., measuring the temperature does not reduce or increase the temperature).

Outline of Sensing Process



- An example showing function of a temperature sensor.
- Senses the room continuously.
- Detects fire
- Communicate the information to a remote monitor via processor

Sensor Classes

- Based on Power Requirement
  - Active
  - Passive
- Based on Output
  - Analog
  - Digital
- Based on Data type
  - Scalar
  - Vector/Multimedia

Active Sensor

- It does not require an external circuitry to provide power.
- It directly responds to the external stimuli from its ambient environments and convert it into an output signal.
- Example : Photo diode (Light into electrical signal)

Passive Sensor

- It requires an external circuitry to provide power.
- The sensed properties are modulated with the sensors inherent characteristics to generate patterns in the output of the sensor.
- Example: Thermistor's resistance

Analog Sensors

- **Analog Sensors** produce a continuous output signal or voltage which is generally proportional to the quantity being measured.

- Physical quantities such as Temperature, Speed, Pressure, Displacement, Strain etc. are all analog quantities as they tend to be continuous in nature.

- For example, the temperature of a liquid can be measured using a thermometer or thermocouple (e.g. in geysers) which continuously responds to temperature changes as the liquid is heated up or cooled down.

Digital Sensors

- **Digital Sensors** produce discrete digital output signals or voltages that are a digital representation of the quantity being measured.

- Digital sensors produce a binary output signal in the form of a logic “1” or a logic “0”, (“ON” or “OFF”).

- Digital signal only produces discrete (non-continuous) values, which may be output as a single “bit” (serial transmission), or by combining the bits to produce a single “byte” output (parallel transmission).

Scalar Sensors

- **Scalar Sensors** produce output signal or voltage which is generally proportional to the magnitude of the quantity being measured.

- Physical quantities such as temperature, color, pressure, strain, etc. are all scalar quantities as only their magnitude is sufficient to convey an information.

- For example, the temperature of a room can be measured using a thermometer or thermocouple, which responds to temperature changes irrespective of the orientation of the sensor or its direction.

Vector Sensors

- **Vector Sensors** produce output signal or voltage which is generally proportional to the magnitude, direction, as well as the orientation of the quantity being measured.

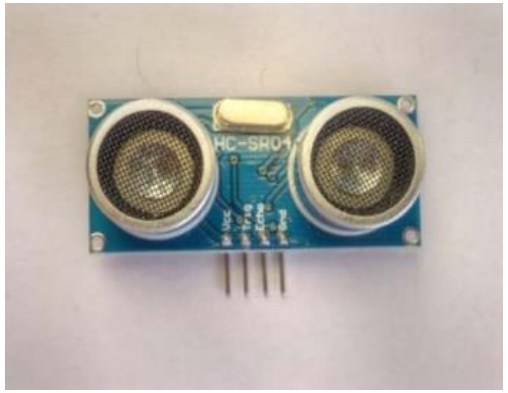
- Physical quantities such as sound, image, velocity, acceleration, orientation, etc. are all vector quantities, as only their magnitude is not sufficient to convey the complete information.

- For example, the acceleration of a body can be measured using an accelerometer, which gives the components of acceleration of the body with respect to the x,y,z coordinate axes.

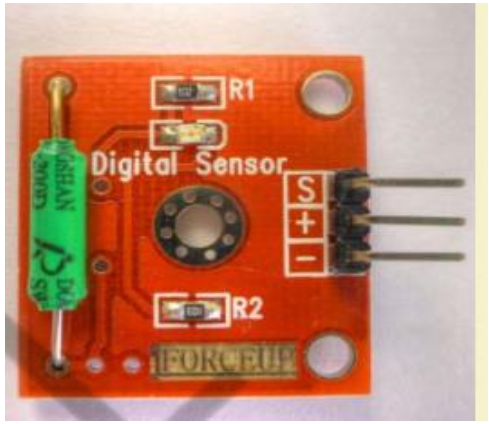
Sensor Types

Light	• **Photo-diode** • **Light Dependent resistor**
Temperature	• **Thermocouple** • **Thermistor**
Force	• **Strain gauge** • **Pressure switch**
Position	• **Potentiometer, Encoders** • **Opto-coupler**
Speed	• **Reflective/ Opto-coupler** • **Doppler effect sensor**
Sound	• **Carbon Microphone** • **Piezoelectric Crystal**
Chemical	• **Liquid Chemical sensor** • **Gaseous chemical sensor**

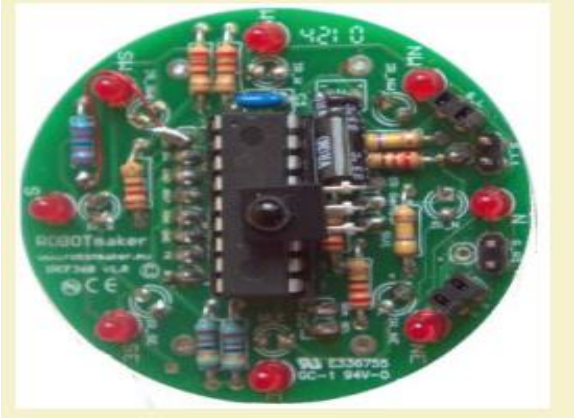
Pressure Sensor



Ultra sonic distance sensor

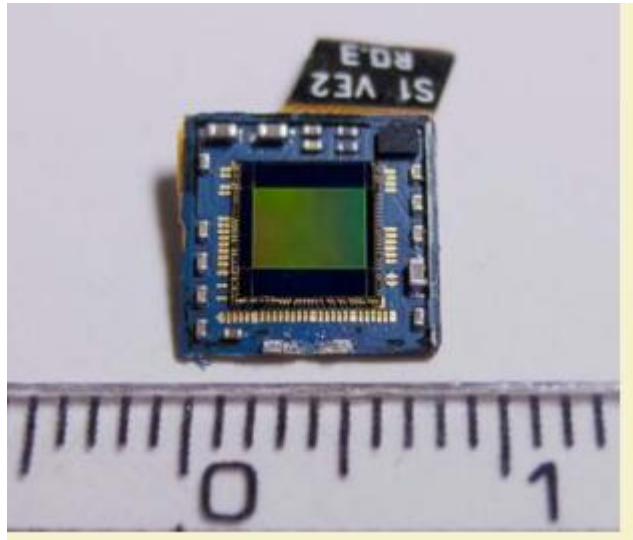


Tilt Sensor



Infrared Motion Sensor

Analog Temperature Sensor

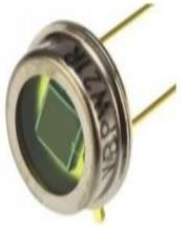


Camera Sensor

Temperature Sensor

Humidity Sensor

Proximity Sensor

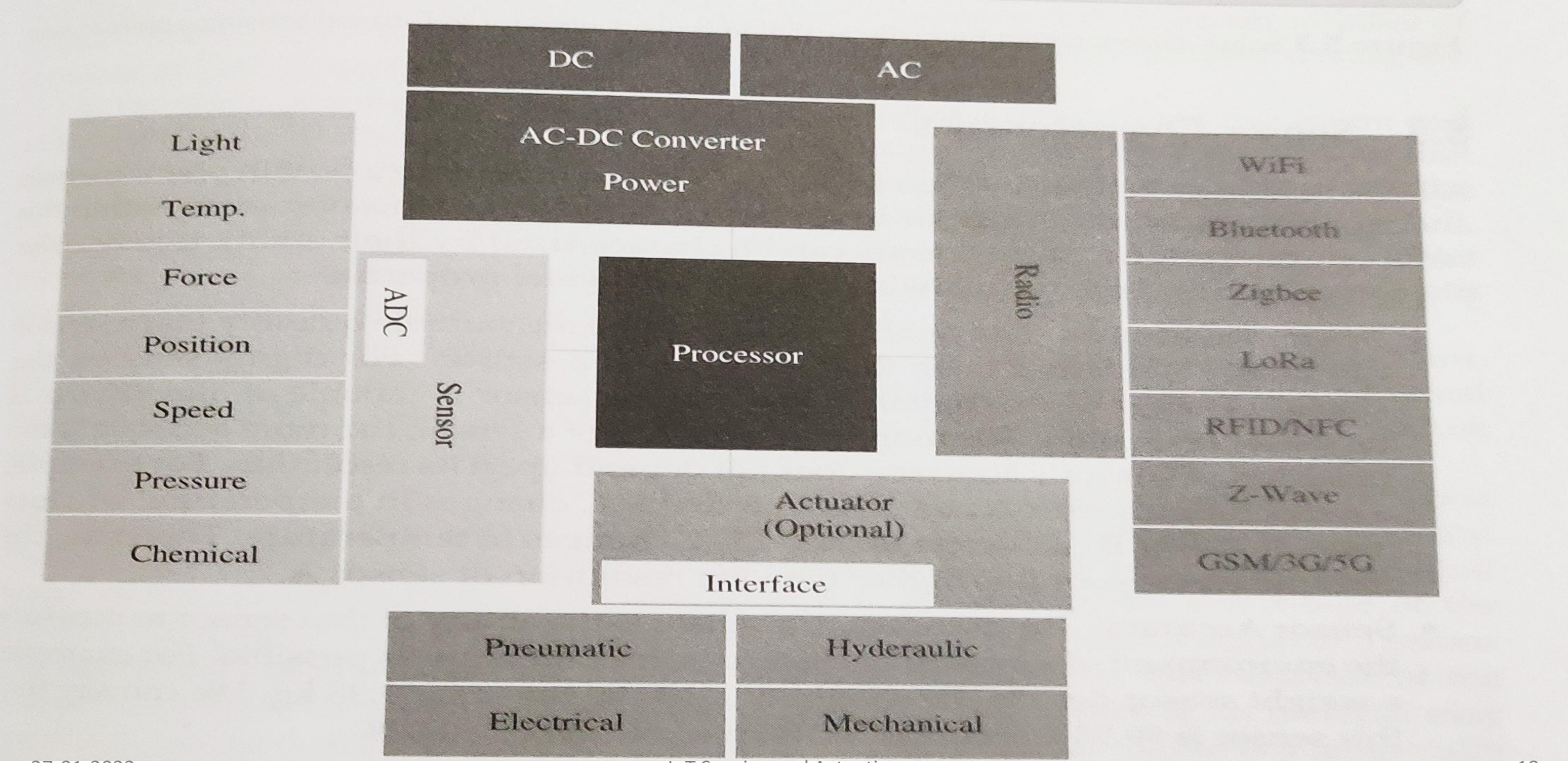


Light Sensor

Metal Sensor

Color Sensor

Functional Blocks of a sensor node in IoT



Sensor Characteristics

- **Sensor resolution**
- **Sensor Accuracy**
- **Sensor Precision**

Sensor Resolution

- The resolution of a sensor is the smallest change it can detect in the quantity that it is measuring.

- The resolution of a sensor with a digital output is usually the smallest resolution the digital output it is capable of processing.

- The more is the resolution of a sensor, the more accurate is its precision.

- A sensor's accuracy does not depend upon its resolution.

- Example:-A temperature sensor **A** detect up to 0.5^{o}C changes in temperature.

Another temperature sensor **B** detect up to 0.25^{o}C changes in temperature.

Resolution of sensor **B** is higher than the resolution of sensor **A**.

Sensor Accuracy

- The ability of a sensor to measure the environment of a system as close to its true measure as possible.
- Example: A weight sensor detects the weight of 100kg mass as 99.98kg.
- Then the sensor is 99.98% accurate with an error rate of +0.02%.

Sensor Precision

- The principle of repeatability is known as precision of a sensor node.
- Multiple repetitions on a sensor's data, the sensor node is found to have the same error rate and can be deemed as high precise.
- Example: A weight sensor detects a weight as 98.28kg, 100.34kg, 101.11kg of actual weight 100kg.
- Here sensor precision is not high because of significant variations in the temporal measurements for the same object under the same condition.

Sensorial Deviations

- Since the range of the output signal is always limited, the output signal will eventually reach a minimum or maximum, when the measured property exceeds the limits. The full scale range of a sensor defines the maximum and minimum values of the measured property.

- The sensitivity of a sensor under real conditions may differ from the value specified. This is called a **sensitivity error**.

- If the output signal differs from the correct value by a constant, the sensor has an **offset error** or **bias**.

Non-linearity

- Nonlinearity is deviation of a sensor's transfer function (TF) from a straight line transfer function.
- This is defined by the amount the output differs from ideal TF behavior over the full range of the sensor, which is denoted as the percentage of the full range.
- Most sensors have linear behavior.
- If the output signal slowly changes independent of the measured property, this is defined as drift. Long term drift over months or years is caused by physical changes in the sensor.
- Noise is a random deviation of the signal that varies in time.

Hysteresis Error

- A hysteresis error causes the sensor output value to vary depending on the sensor’s previous input values.
- If a sensor's output is different depending on whether a specific input value was reached by increasing or decreasing the input, then the sensor has a hysteresis error.
- The present reading depends on the past input values.
- Typically in analog sensors, magnetic sensors, heating of metal strips.

Other Errors

- If the sensor has a digital output, the output is essentially an approximation of the measured property. This error is also called **quantization error**.

- If the signal is monitored digitally, the sampling frequency can cause a dynamic error, or if the input variable or added noise changes periodically at a frequency proportional to the multiple of the sampling rate, **aliasing errors** may occur.

- The sensor may to some extent be sensitive to properties other than the property being measured. For example, most sensors are influenced by the temperature of their environment.

Sensing Types

- Based on nature of environment being sensed and physical sensor being used, the sensing is broadly categorized into four types.
- They are

✓**Scalar sensing**

✓**Multimedia sensing**

✓**Hybrid sensing**

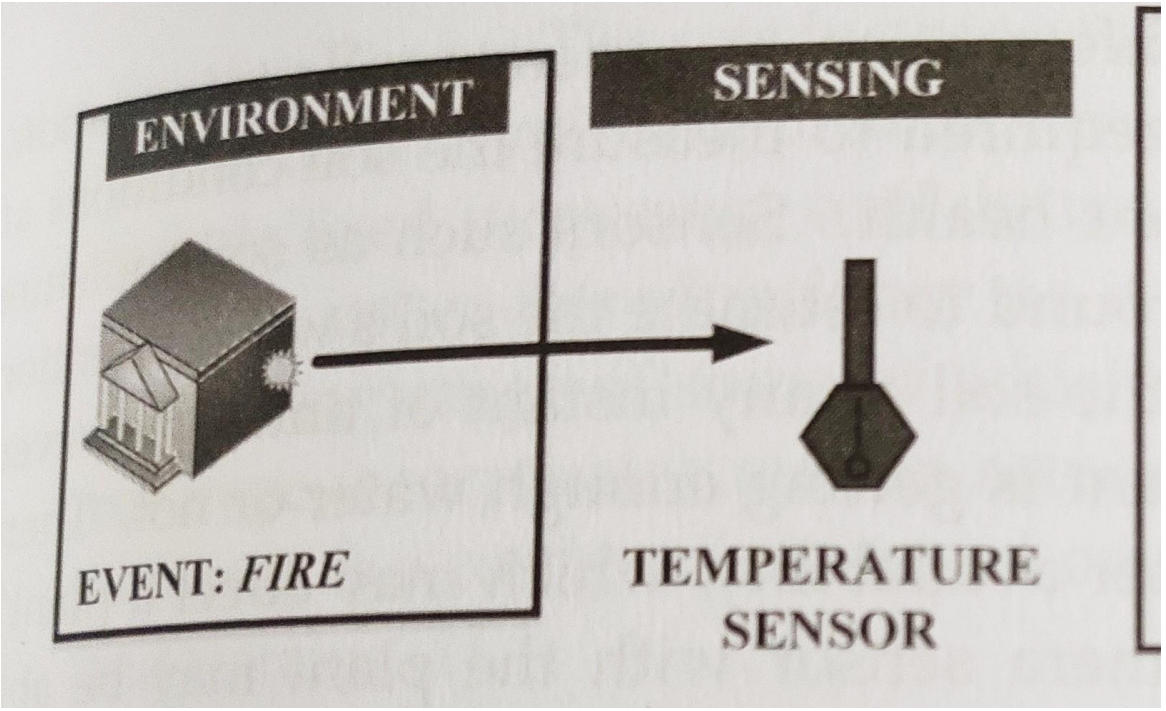
✓**Virtual sensing**

Scalar Sensing

- Measuring changes in the amplitude of the measured values with respect to time.

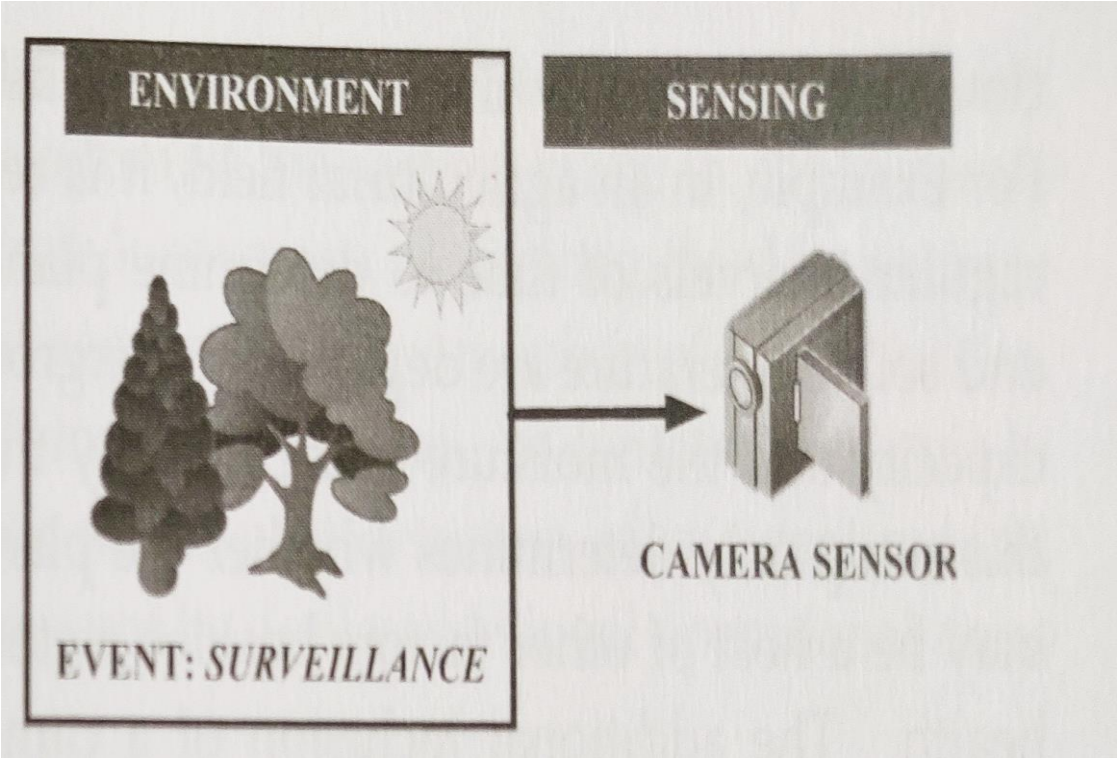
- Example:- Ambient temperature, current, atmospheric pressure, rainfall, light, humidity, flux.

- The sensors used for measuring scalar quantities are called scalar sensors and the act is known as scalar sensing.



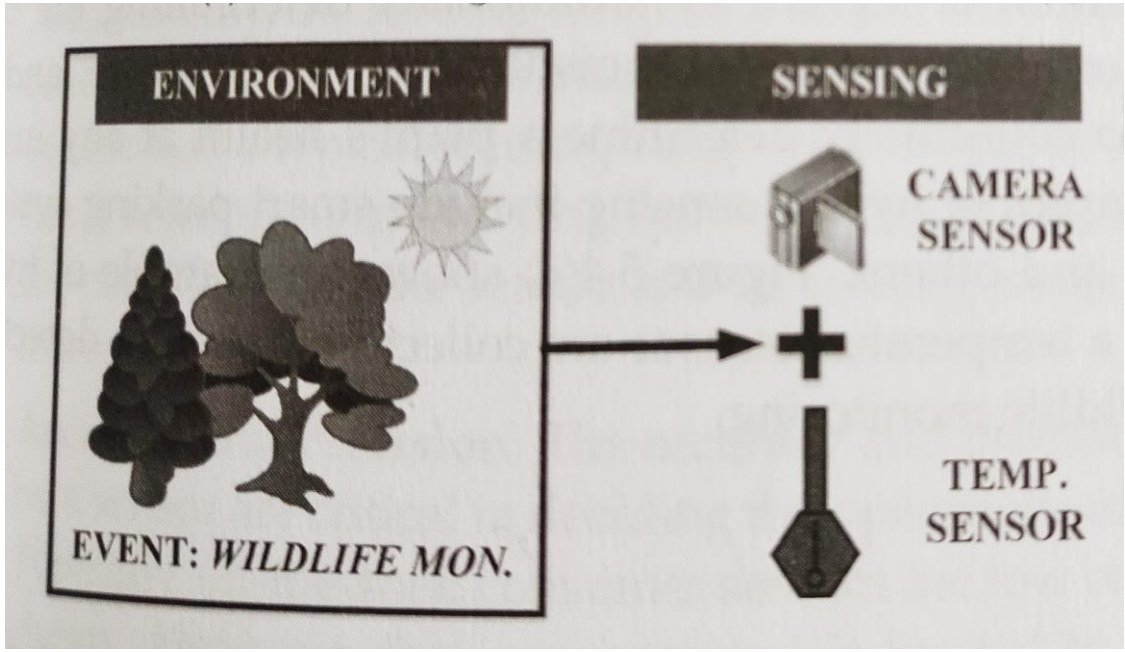
Multimedia sensing

- Multimedia sensing encompasses the sensing of features that have a spatial variance property associated with the property of temporal variance.
- Example:-Image, direction, flow, speed, acceleration, sound, force, mass, energy, momentum.
- These sensors are used to capture the changes in amplitude of a quantifiable property concerning space and time.
- These sensors are called vector sensors as its sensed quantities follow the vector law of addition.



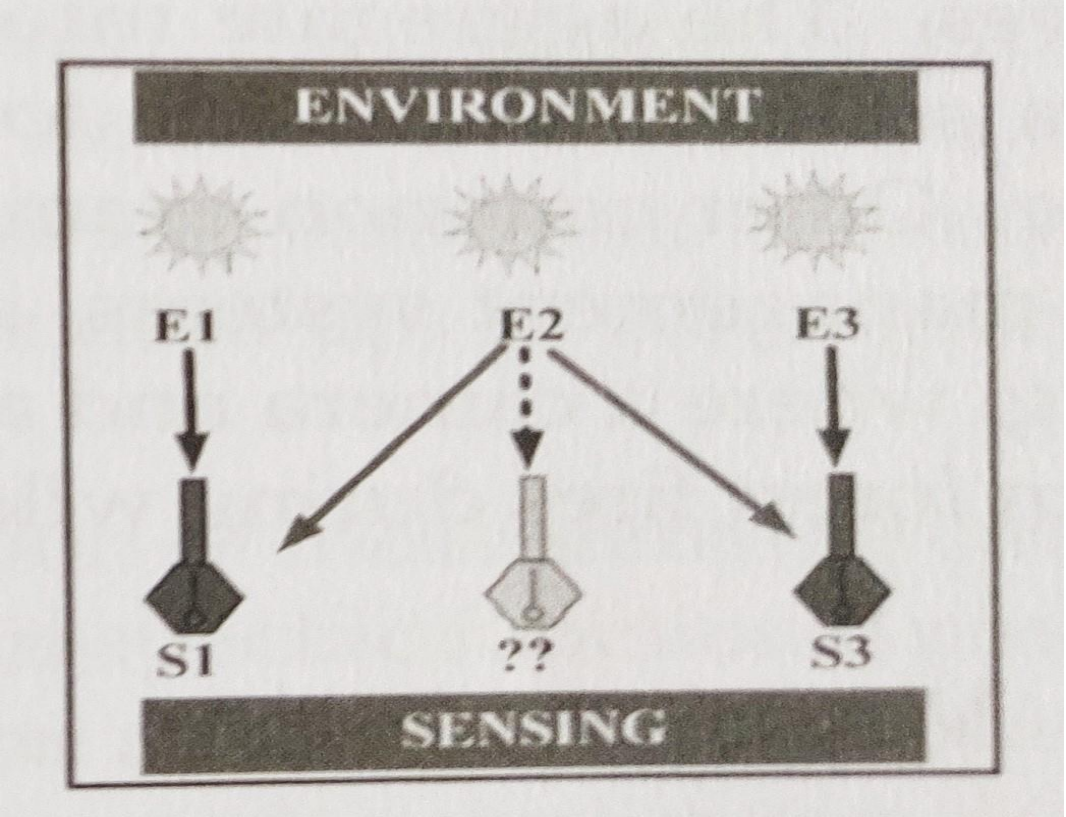
Hybrid Sensing

- The act of using scalar as well as multimedia sensing at the same time is known as hybrid sensing.
- Scalar and vector property of environments at the same time.
- Example: In agriculture field, measure the soil condition (Soil moisture, soil temperature), plant health (camera sensor) at regular time interval.
- Smart parking system and traffic management system
- Camera and temperature sensor to collectively determine the forest fires during wildlife monitoring.



Virtual sensing

Specific area (A say) have physical sensors.
Some area (B say)have no physical sensors.
B areas data are derived from A's data.
That whole phenomena is called virtual sensing.



Sensing Consideration

- The choice of sensors in IoT based sensing solutions are
  - ✓Sensing range
  - ✓Accuracy and precision
  - ✓Energy
  - ✓Device size

Sensing Consideration

Sensing range

- The detection fidelity of a sensor node is known as sensing range.

- It is two types
  - ✓Fixed k-coverage
  - ✓Dynamic k-coverage (Mobile sensor node, costly solution)

Sensing Consideration

Accuracy and precision

- It decides the operations of specific functional processes.
- Example: Temperature sensors are easily used in day to day applications but not suitable for industrial applications.

Sensing Consideration

Energy

- It determines the life time of a sensor and estimated cost of its deployment.
- If a sensor node is energy inefficient, then we need to replace that sensor frequently. By this maintenance cost increases and deployment feasibility goes down.

Sensing Consideration

Device size

- Larger the device size , larger the obstruction caused by it, higher the cost and energy requirement and lesser is its demand for the bulk of IoT applications

- Example: Wearable sensors

Actuator

- An actuator is a component of a machine or system that moves or controls the mechanism or the system.
- An actuator is the mechanism by which a control system acts upon an environment.
- An actuator requires a control signal and a source of energy.
- Upon receiving a control signal is received, the actuator responds by converting the energy into mechanical motion.
- The control system can be simple (a fixed mechanical or electronic system), software-based (e.g. a printer driver, robot control system), a human, or any other input.

Actuation Mechanisms

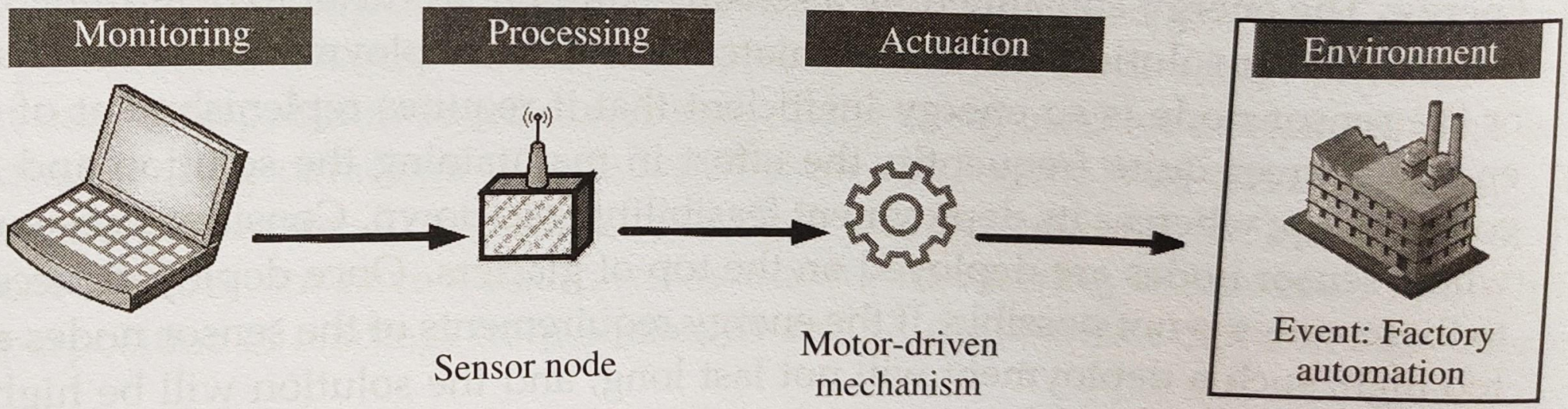
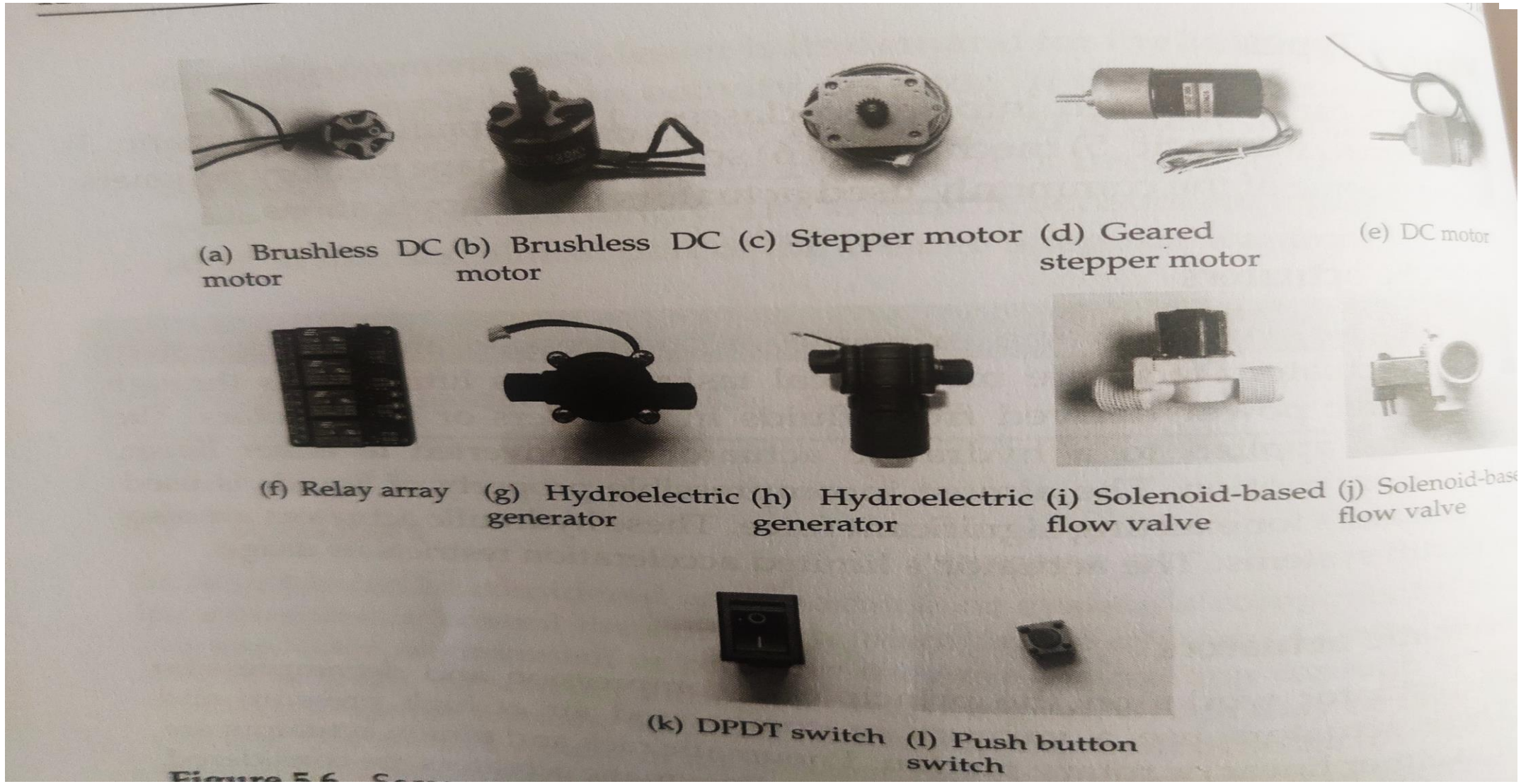


Figure 5.5 The outline of a simple actuation mechanism

Commonly used actuators in IoT Applications



Actuator Types

Hydraulic

Pneumatic

Electrical

Thermal/ Magnetic

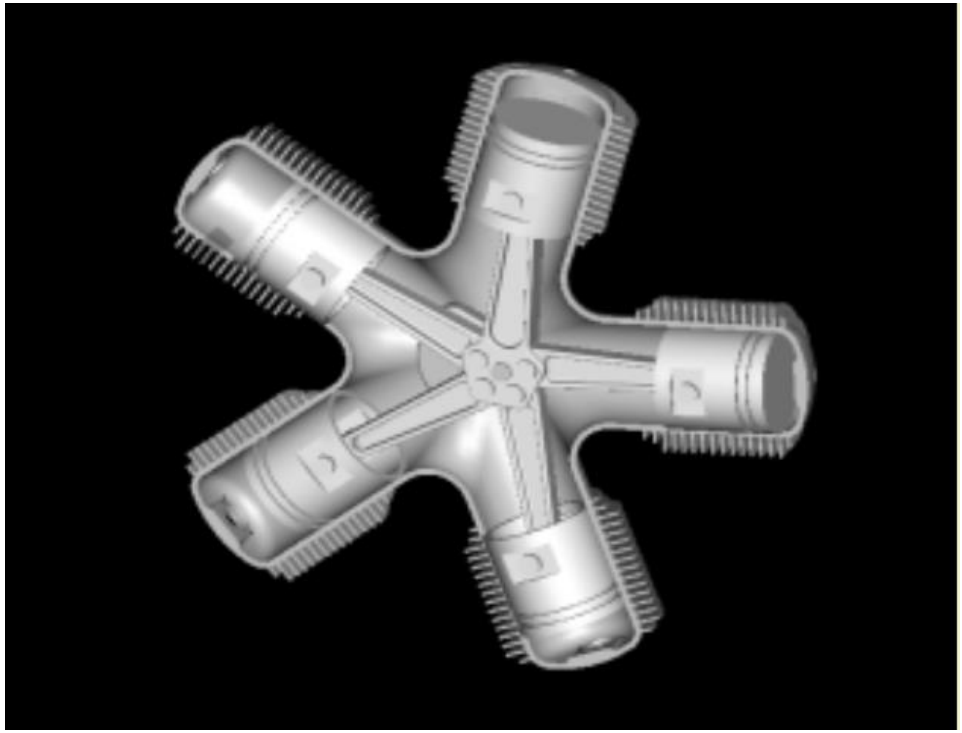
Mechanical

Hydraulic Actuators

- A hydraulic actuator consists of a cylinder or fluid motor that uses hydraulic power to facilitate mechanical operation.
- The mechanical motion is converted to linear, rotary or oscillatory motion.
- Since liquids are nearly impossible to compress, a hydraulic actuator exerts considerable force.
- The actuator's limited acceleration restricts its usage.

Hydraulic Actuators

Hydraulic Actuator



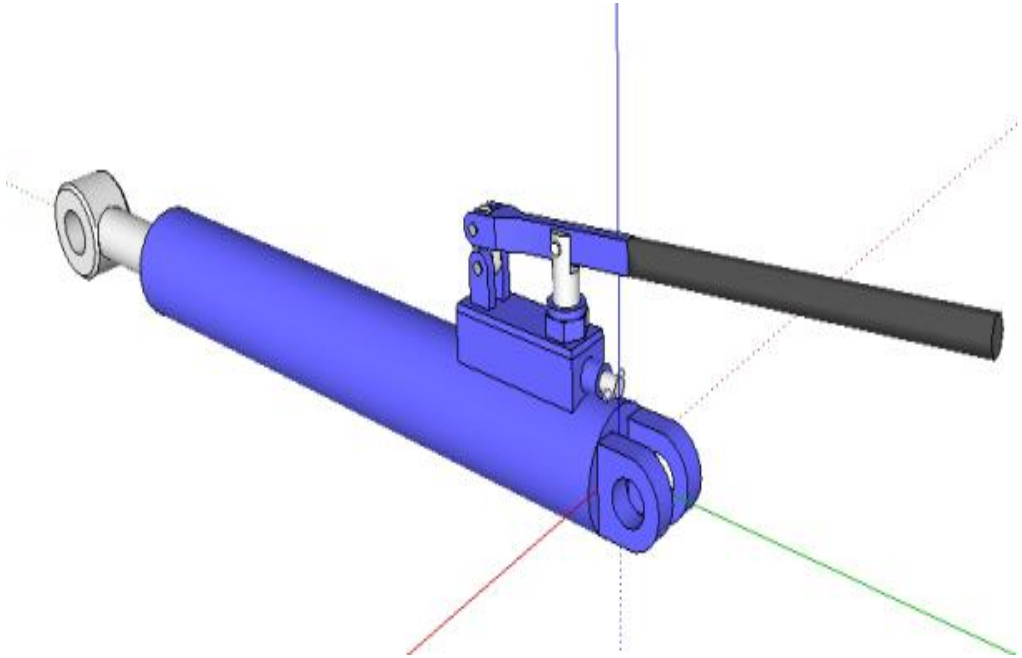
A radial engine acts as a hydraulic actuator

Pneumatic Actuators

- A pneumatic actuator converts energy formed by vacuum or compressed air at high pressure into either linear or rotary motion.
- Pneumatic rack and pinion actuators are used for valve controls of water pipes.
- Pneumatic energy quickly responds to starting and stopping signals.
- The power source does not need to be stored in reserve for operation.
- Pneumatic actuators enable large forces to be produced from relatively small pressure changes (e.g., Pneumatic brakes can are very responsive to small changes in pressure applied by the driver).
- It is responsible for converting pressure into force.

Pneumatic Actuators

An air pump acts as a pneumatic actuator



A manual linear pneumatic actuator

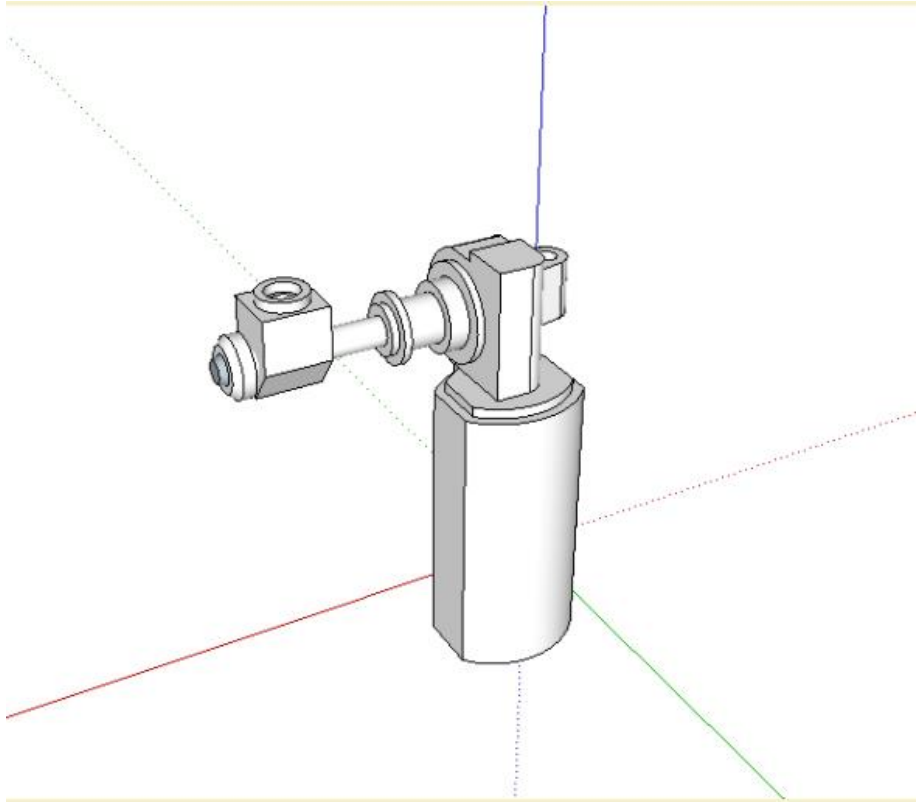
Electric Actuators

- An electric actuator is generally powered by a motor that converts electrical energy into mechanical torque.

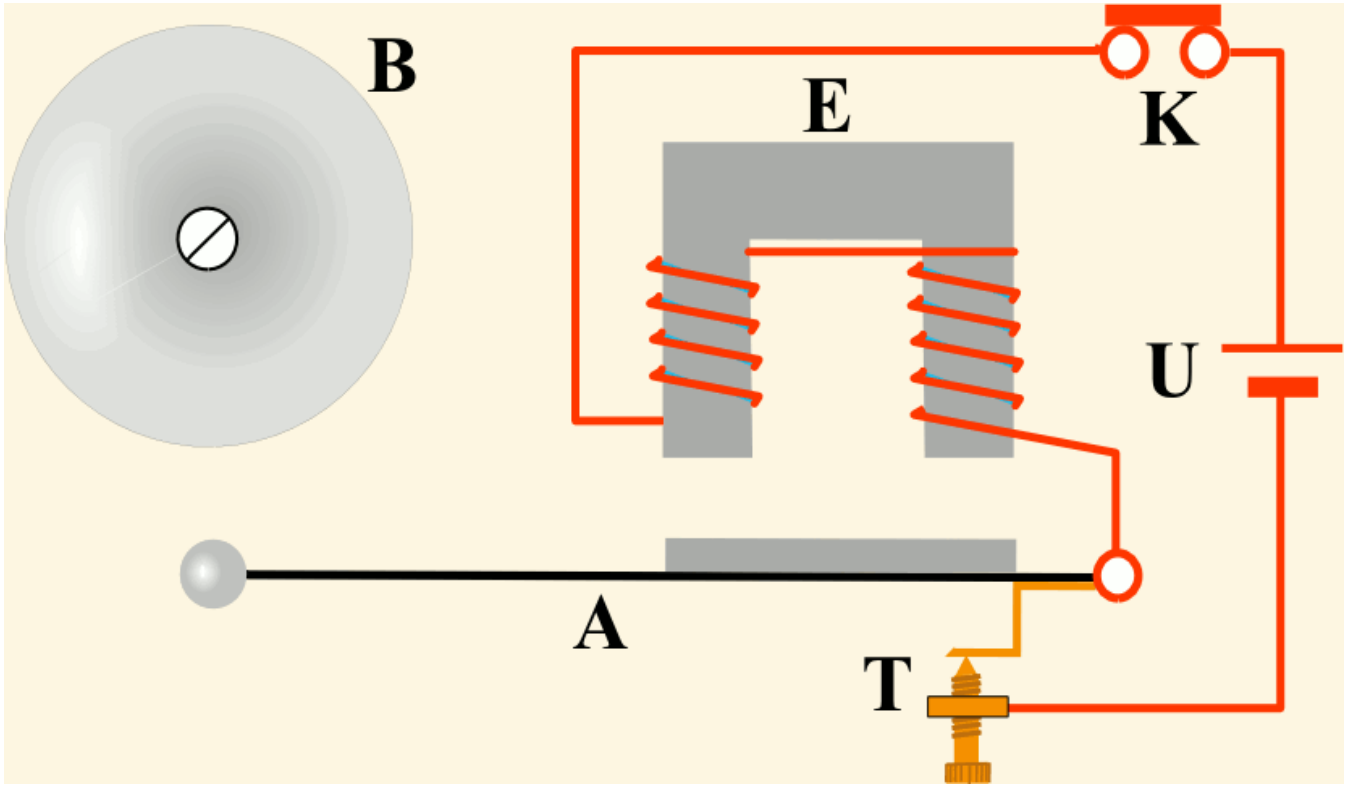
- The electrical energy is used to actuate equipment such as solenoid valves which control the flow of water in pipes in response to electrical signals.

- Considered as one of the cheapest, cleanest and speedy actuator types available.

Electric Actuators



A motor drive-based rotary actuator

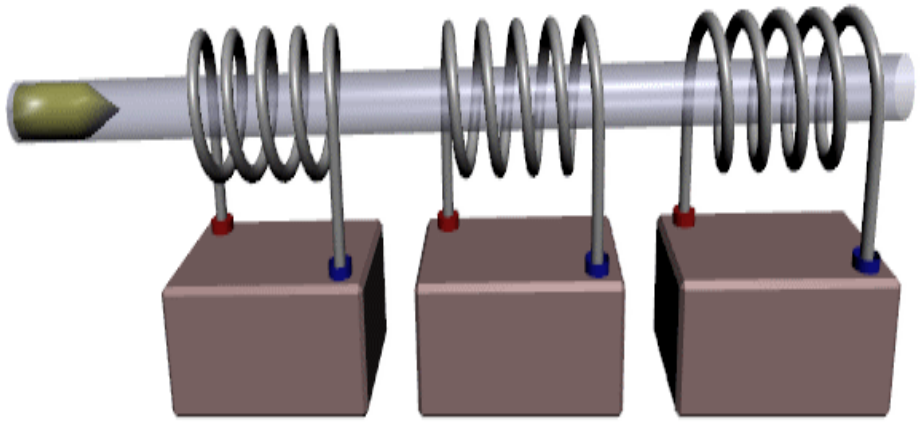


A solenoid based electric bell ringing mechanism

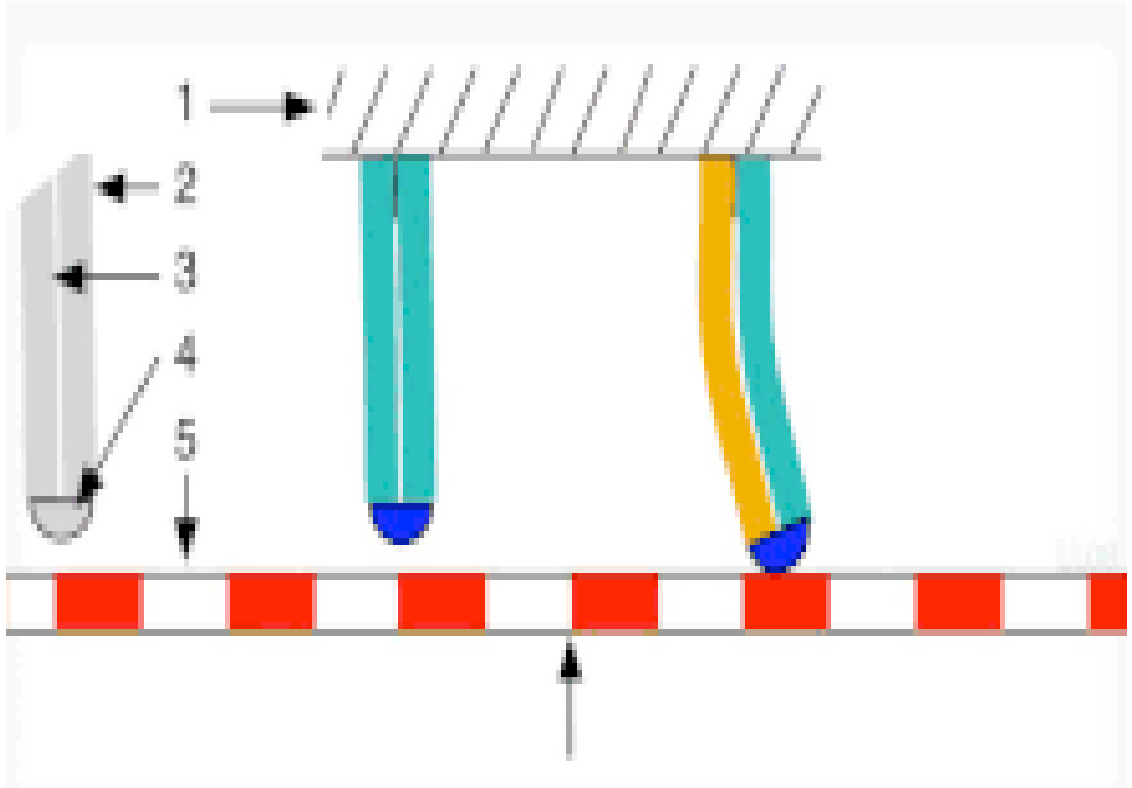
Thermal or Magnetic Actuators

- These can be actuated by applying thermal or magnetic energy.
- They tend to be compact, lightweight, economical and with high power density.
- These actuators use shape memory materials (SMMs), such as shape memory alloys (SMAs) or magnetic shape-memory alloys (MSMAs).
- Some popular manufacturers of these devices are *Finnish Modti Inc*. and *American Dynalloy*.

Thermal or Magnetic Actuators



A coil gun works on the principle of magnetic actuation

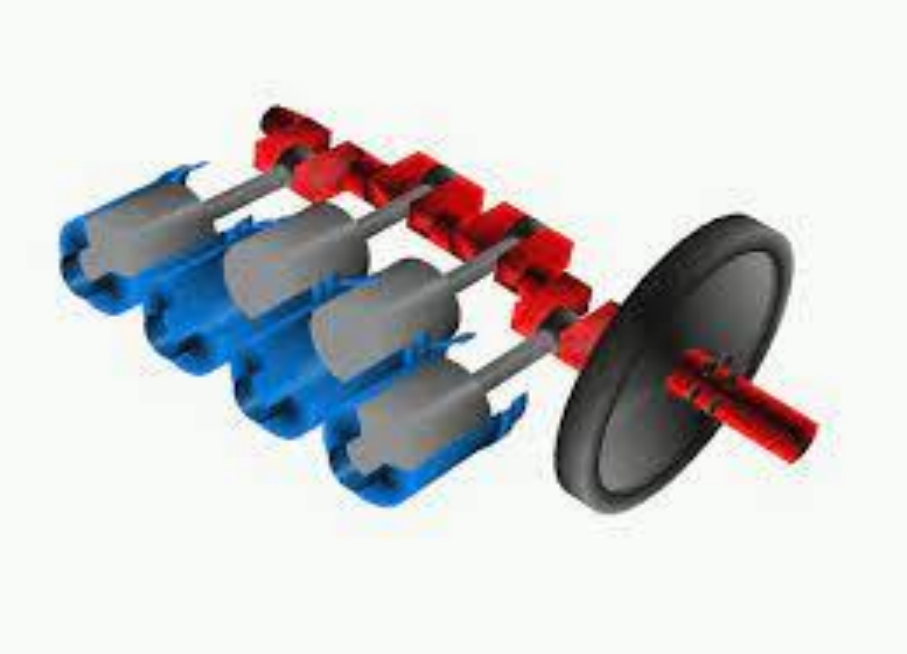


A piezo motor using SMA

Mechanical Actuators

- A mechanical actuator converts rotary motion into linear motion to execute some movement.
- It involves gears, rails, pulleys, chains and other devices to operate.
- Example: rack and pinion

Mechanical Actuators



A crank shaft acting as a mechanical actuator

A rack and pinion mechanism

Soft Actuators

- Soft actuators (e.g. polymer based) are designed to handle fragile objects like fruit harvesting in agriculture or manipulating the internal organs in biomedicine.
- They typically address challenging tasks in robotics.
- Soft actuators produce flexible motion due to the integration f microscopic changes at the molecular level into a macroscopic deformation of the actuator materials.

Light Activated Polymers

- Photopolymer/light activated polymers (LAP) are a special type of SMP that are activated by light stimuli.
- The LAP actuators have instant response.
- They can be controlled remotely without any physical contact, only using the variation of light frequency or intensity.

Shape Memory Polymers

- Shape memory polymer (SMP) actuators function similar to our muscles, even providing a response to a range of stimuli such as light, electrical, magnetic, heat, pH, and moisture changes.

- SMP exhibits surprising features such a low density, high strain recovery, biocompatibility, and biodegradability.

Actuator Characteristics

Choice or selection of actuators in an IoT deployment depends on

- ✓Weight
- ✓Power Rating
- ✓Torque to weight Ratio
- ✓Stiffness and compliance

Actuator Characteristics

Weight

- Heavier weight actuators is preferred for Industrial applications, applications that does not require mobility of the IoT deployments.

- Light weight actuators are found in portable systems, in vehicles, drones, and home IoT applications

Actuator Characteristics

Power Rating

- It decides the nature of the application with which an actuator can be associated.
- It defines the minimum and maximum operating power an actuator can safely withstand without damage to itself.
- It is power to weight ratio for an actuator.
- Example:- servo motors used in hobby projects have maximum rating of 5VCD, 500mA.

Actuator Characteristics

Torque to weight Ratio

- Torque to weight Ratio is defined as the ratio of torque to the weight of the moving part of an instrument/device.
- This indicates the sensitivity of the actuator.
- Higher the weight of the moving part, lower will be the torque to weight ratio for a given power.

Actuator Characteristics

Stiffness and compliance

- The resistance of a material against the deformation is known as stiffness.
- The opposite of the stiffness is known as compliance.
- Stiffness is directly related to modules of elasticity of that material.
- Stiff system is more accurate than compliant system as they have faster response to the change in load applied to it.
- Example: Hydraulic systems are stiff systems and pneumatic systems are compliant systems

THANK YOU

IoT connectivity Technologies

- List of common connectivity protocols in IoT.
- Identify the salient features and application scope of each connectivity protocol.
- Understand the terminologies and technologies associated with IoT connectivity.
- Determine the requirements associated with each of these connectivity protocols in real-world solutions.
- Determine the most appropriate connectivity protocol for each segment of their IoT implementation.

Communication Protocols

The following IoT connectivity enablers have immediate importance to consumer and industrial IoTs:

1. IEEE 802.15.4
2. Zigbee
3. Thread
4. ISA 100.11A
5. Wireless HART
6. RFID
7. NFC
8. DASH7
9. Z-Wave
10. Weightless
11. Sigfox
12. LoRa
13. NB-IoT
14. Wifi
15. Bluetooth

IoT connectivity Technologies

- These connectivity enablers can integrated with existing sensing, actuation and processing solution units.
- These enablers requires minimal form of processing infrastructure (ex: wifi).
- It can work in a standalone mode i.e. without need of external processing and hardware support (ex: Zigbee)

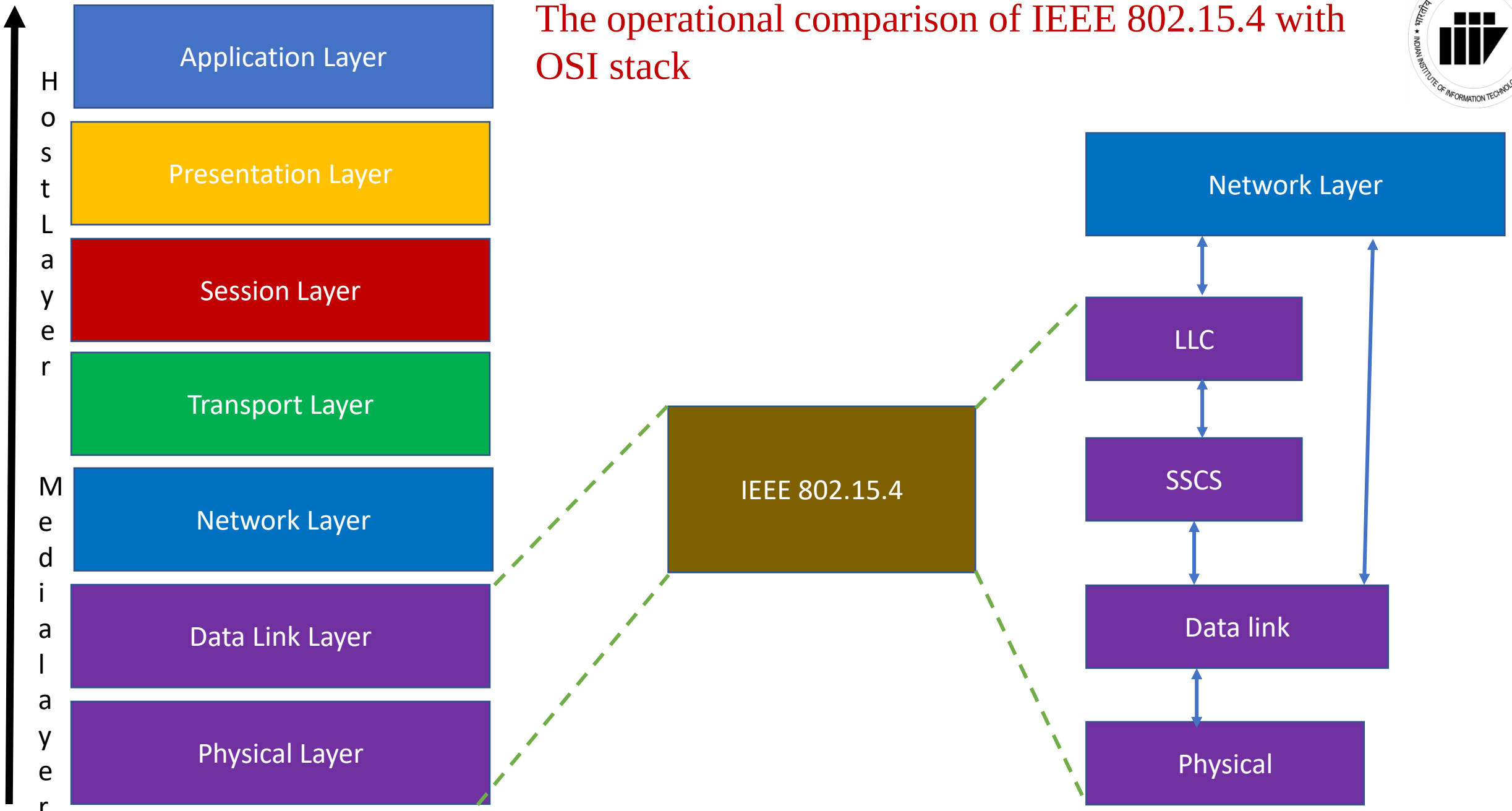
IEEE 802.15.4

IEEE : Institute of Electrical and Electronics Engineers

Features of IEEE 802.15.4

- Well-known standard for low data-rate WPAN.
- Developed for low-data-rate monitoring and control applications and extended-life for uses with low-power-consumption.
- This standard uses only the first two layers (PHY, MAC) plus the Logical Link Control (LLC) and service specific convergence sub-layer (SSCS) additions to communicate with all upper layers
- Operates in the ISM (Industrial, Scientific, and Medical)band.

The operational comparison of IEEE 802.15.4 with OSI stack



IEEE 802.15.4

- Uses direct sequence spread spectrum (DSSS) modulation which enables wider bandwidth and enhance security by modulating pseudo-random noise signal.
- Highly tolerant of noise and interference and offers link reliability improvement mechanisms.
- Low-speed versions use Binary Phase Shift Keying (BPSK).
- High data-rate versions use offset-quadrature phase-shift keying (O-QPSK) for encoding the messages.
- Uses carrier sense multiple access with collision avoidance (CSMA-CA) for channel access which maintains the sequence of transmitted signals and prevents deadlocks due to multiple sources trying to access the same channel.
- Multiplexing allows multiple users or nodes interference-free access to the same channel at different times.

IEEE 802.15.4

- Power consumption is minimized due to infrequently occurring very short packet transmissions with low duty cycle (<1%).
- The minimum power level defined is –3 dBm or 0.5 mW.
- Transmission, for most cases, is Line of Sight (LOS).
- Standard transmission range varies between 10m to 75m.
- Best case transmission range achieved outdoors can be up to 1000m.
- Networking topologies defined are -- Star, and Mesh.

IEEE 802.15.4 Variants

A/B

- Base Version

C

- For China

D

For Japan

E

Industrial applications

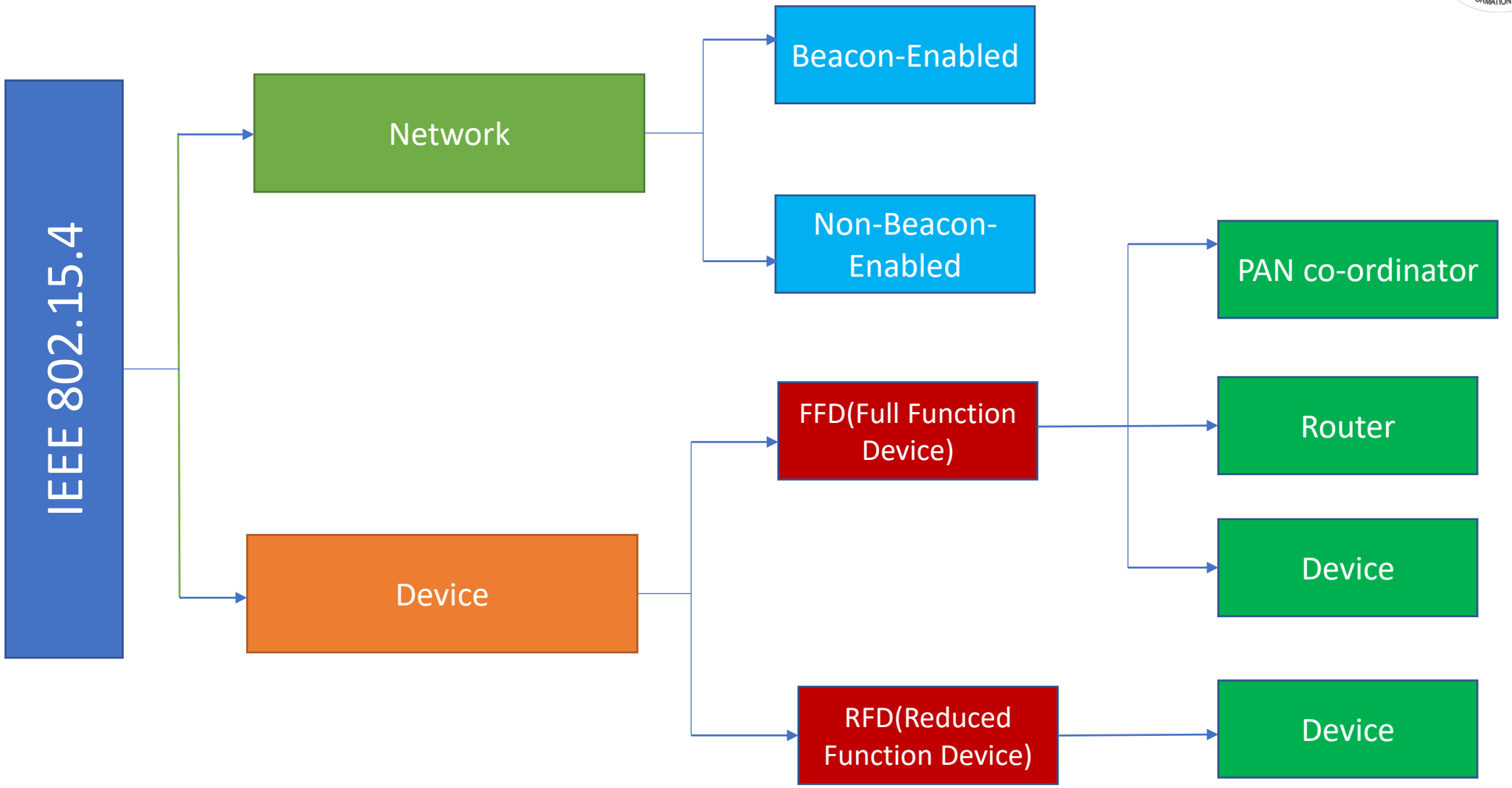
F

Active RFID uses

G

- Smart utility networks (Smart Grids)

Various devices and network types supported in IEEE 802.15.4 standard



IEEE 802.15.4 Device Types

- **Full Function Device (FFD)**

  ✓ Can talk to all types of devices

  ✓ Supports full protocol

  ✓ Costly and energy consuming due to increased requirements for full support stacks.

- **Reduced Function Device (RFD)**

  ✓ Can only talk to an FFD

  ✓ Lower power consumption

  ✓ Minimal CPU/RAM required

IEEE 802.15.4 Network Types

Beacon Enabled Networks

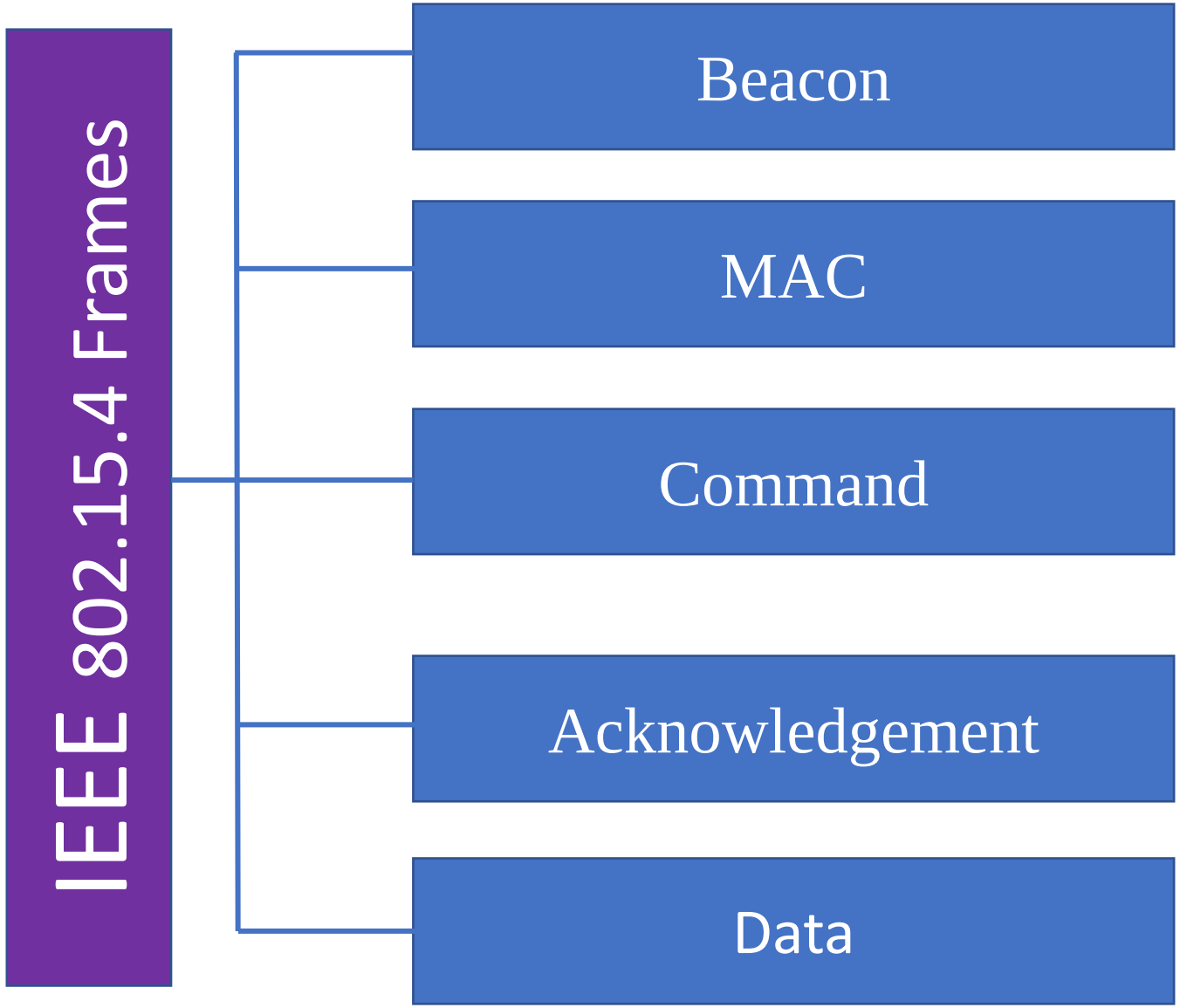
- Periodic transmission of beacon messages.
- Data-frames sent via Slotted CSMA/CA with a super frame structure managed by PAN coordinator.
- Beacons used for synchronization & association of other nodes with the coordinator.
- Scope of operation spans the whole network.

IEEE 802.15.4 Network Types

Non-Beacon Enabled Networks

- Data-frames sent via un-slotted CSMA/CA (Contention Based).
- Beacons used only for link layer discovery.
- Requires both source and destination IDs.
- As 802.15.4 is primarily, a mesh protocol, all protocol addressing must adhere to mesh configurations.
- De-centralized communication amongst nodes

IEEE 802.15.4 Frames



IEEE 802.15.4 Frames

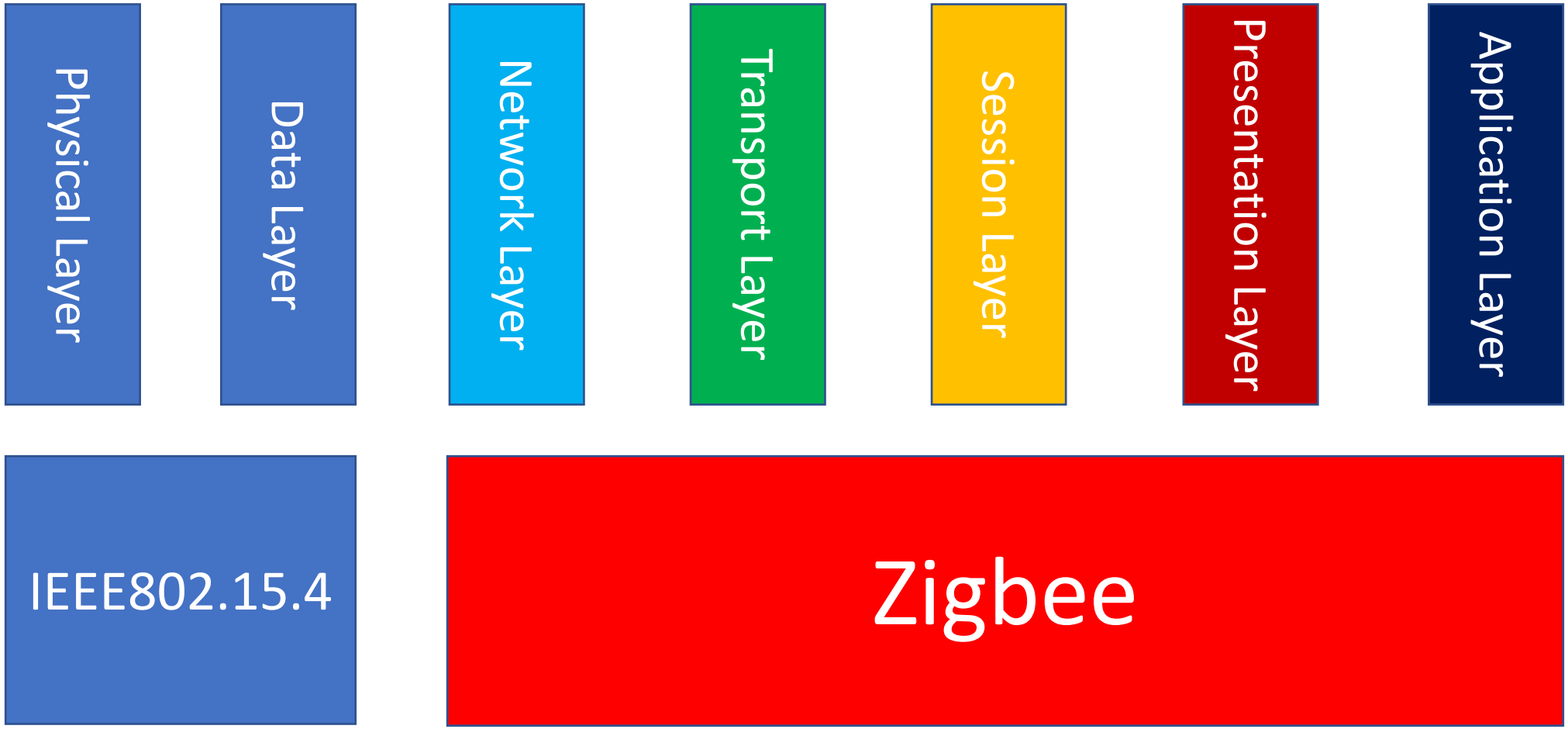
- Beacon frames are used for signaling and synchronization.
- Data frames are used for data transmission.
- Message reception is confirmed using acknowledgement frames.
- MAC and command frames are used for association request/responses, dissociation request, data request, beacon request, co-Ordinator realignment and orphan notifications.

ZigBee

Features of ZigBee

- Designed for WPAN and common usage in sensor and control network.
- Most widely deployed enhancement of IEEE 802.15.4.
- The ZigBee protocol is defined by **layer 3 and above**. It works with the 802.15.4 layers 1 and 2.
- The standard uses layers 3 and 4 to define additional communication enhancements.
- These enhancements include authentication with valid nodes, encryption for security, and a data routing and forwarding capability that enables mesh networking.

ZigBee

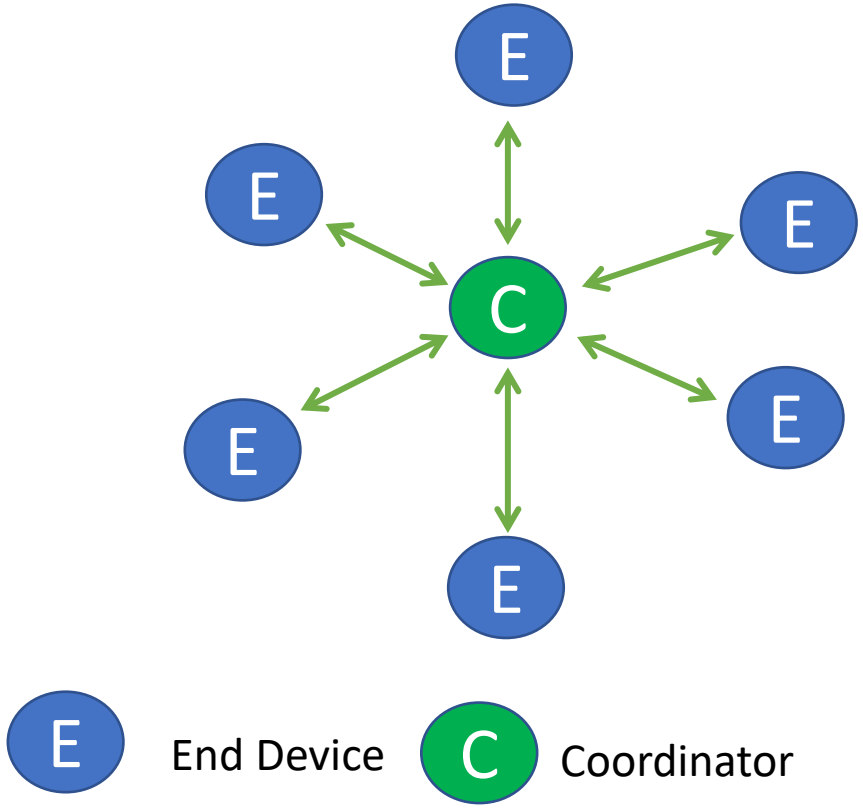

Physical Layer
Data Layer
Network Layer
Transport Layer
Session Layer
Presentation Layer
Application Layer
IEEE802.15.4
Zigbee

Features of ZigBee

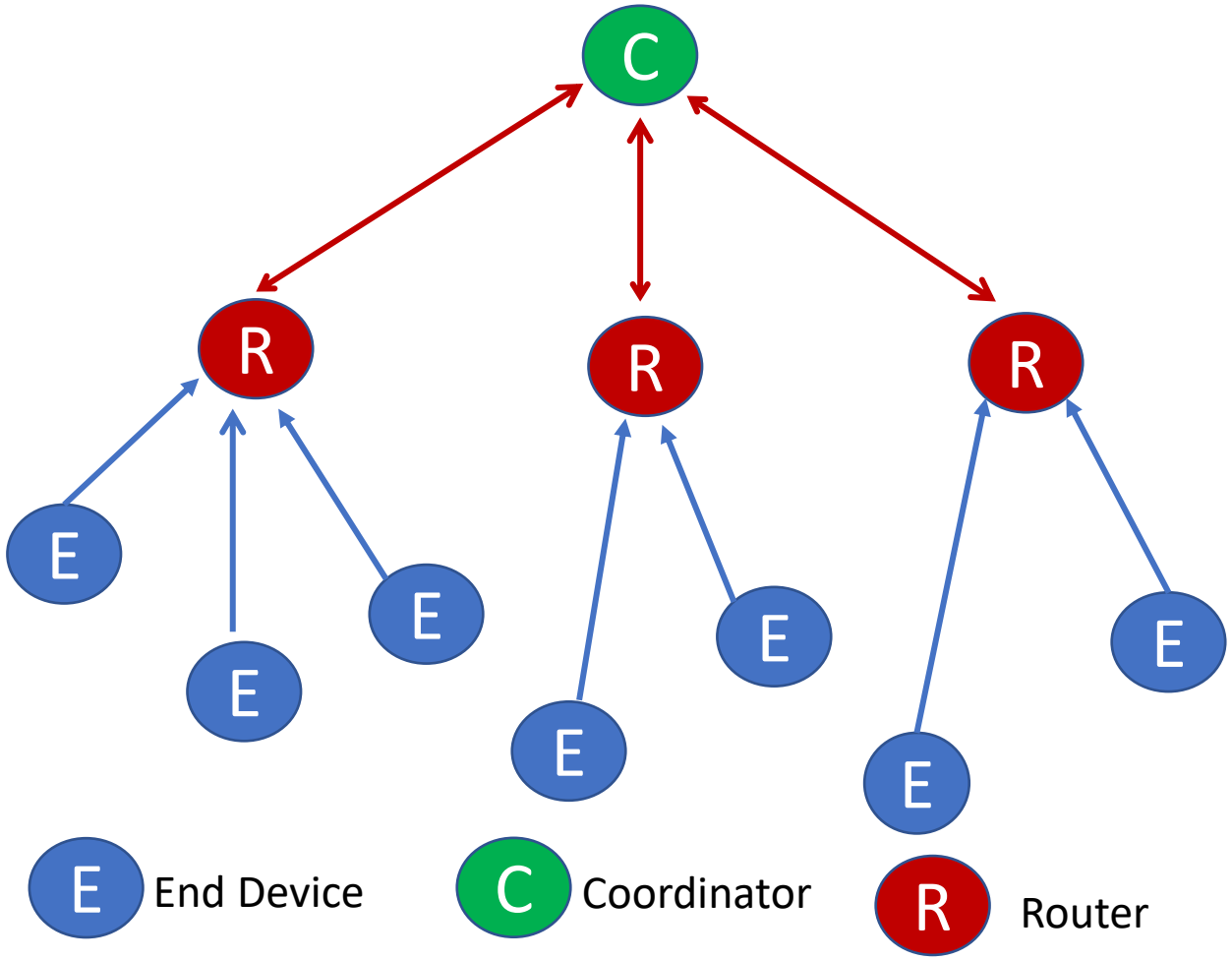
- It can be implemented for controlling and monitoring applications in the range of 10-100 meters.
- The PHY and MAC layers can handle multiple low data rate operating devices.
- The frequency is 2.4GHz, 902-928 MHz, or 868 MHz
- Data rate is 250kbps.
- The most popular use of ZigBee is wireless sensor networks using the mesh, star, and cluster topology.
- It supports master to master communication and master to slave communication.

Various communication topologies in Zigbee

Star Topology



Cluster Tree



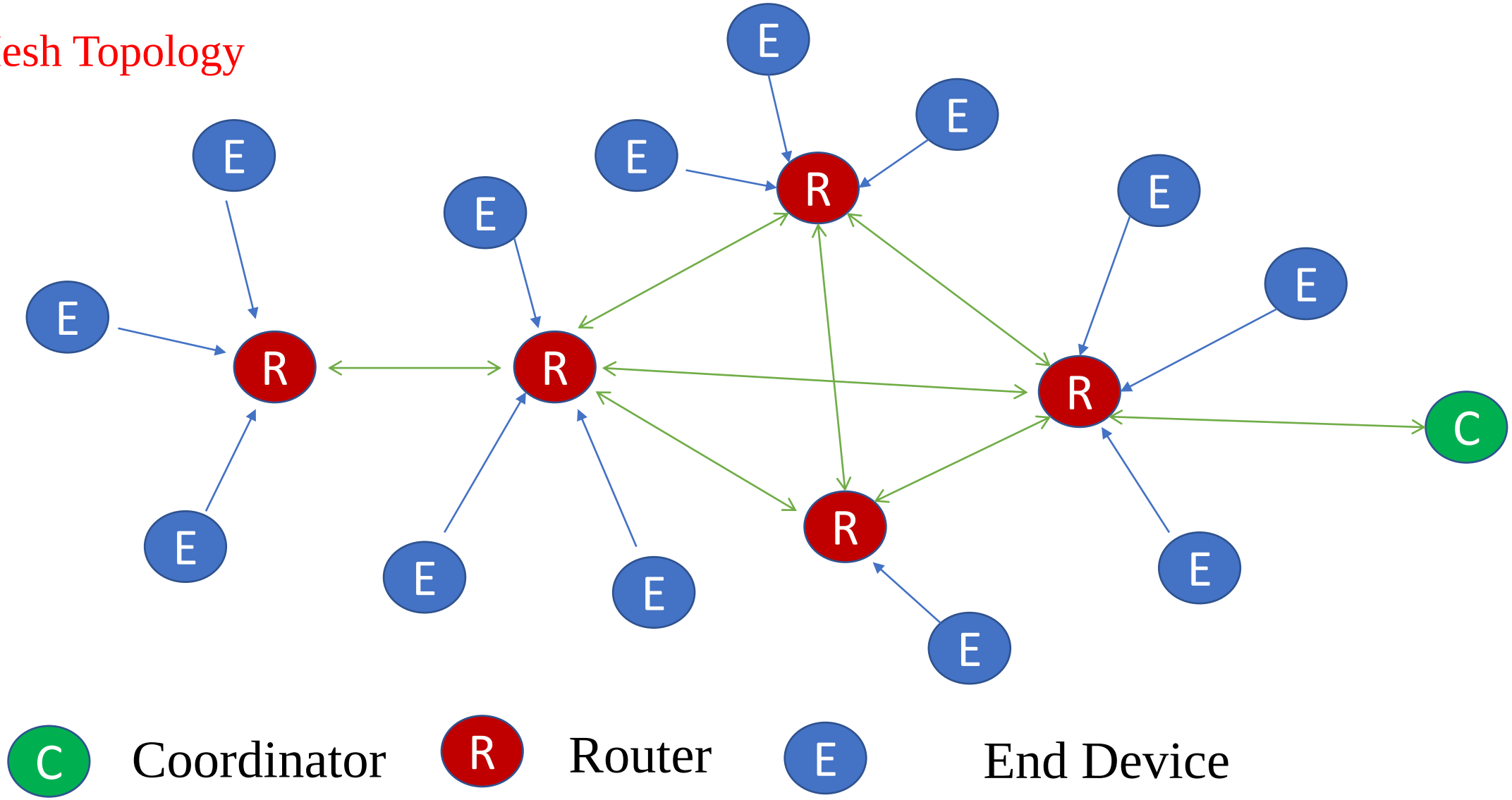
Various communication topologies in Zigbee

1. Star Topology

- The coordinator initiates and manages the other devices in ZigBee network.
- The other devices which communicate with the coordinator are called end devices.
- Easy to maintain and deploy.
- Widely used in IoT application.
- It suffers with single point of failure.

Various communication topologies in Zigbee

Mesh Topology



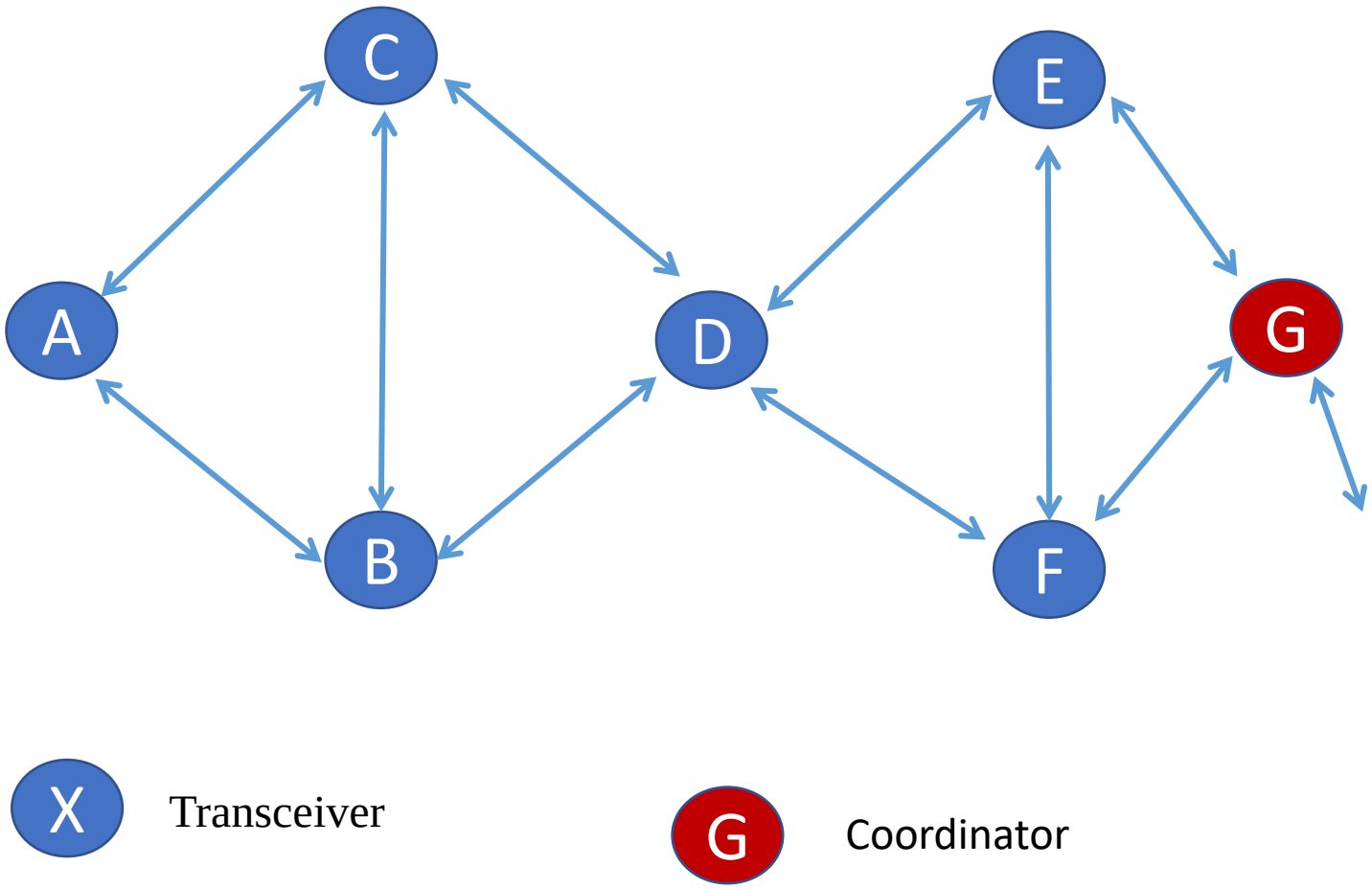
Various communication topologies in Zigbee

2. Cluster and Mesh Topology

- Root of the topology is coordinator.
- It allows any node or device to communicate with any other adjacent node.
- In case of failure of one or more nodes, the information is automatically forwarded to other functional devices.
- In cluster network, co-Ordinator is placed in leaf node position of the cluster.
- Parent co-Ordinator initiates the entire network activities.

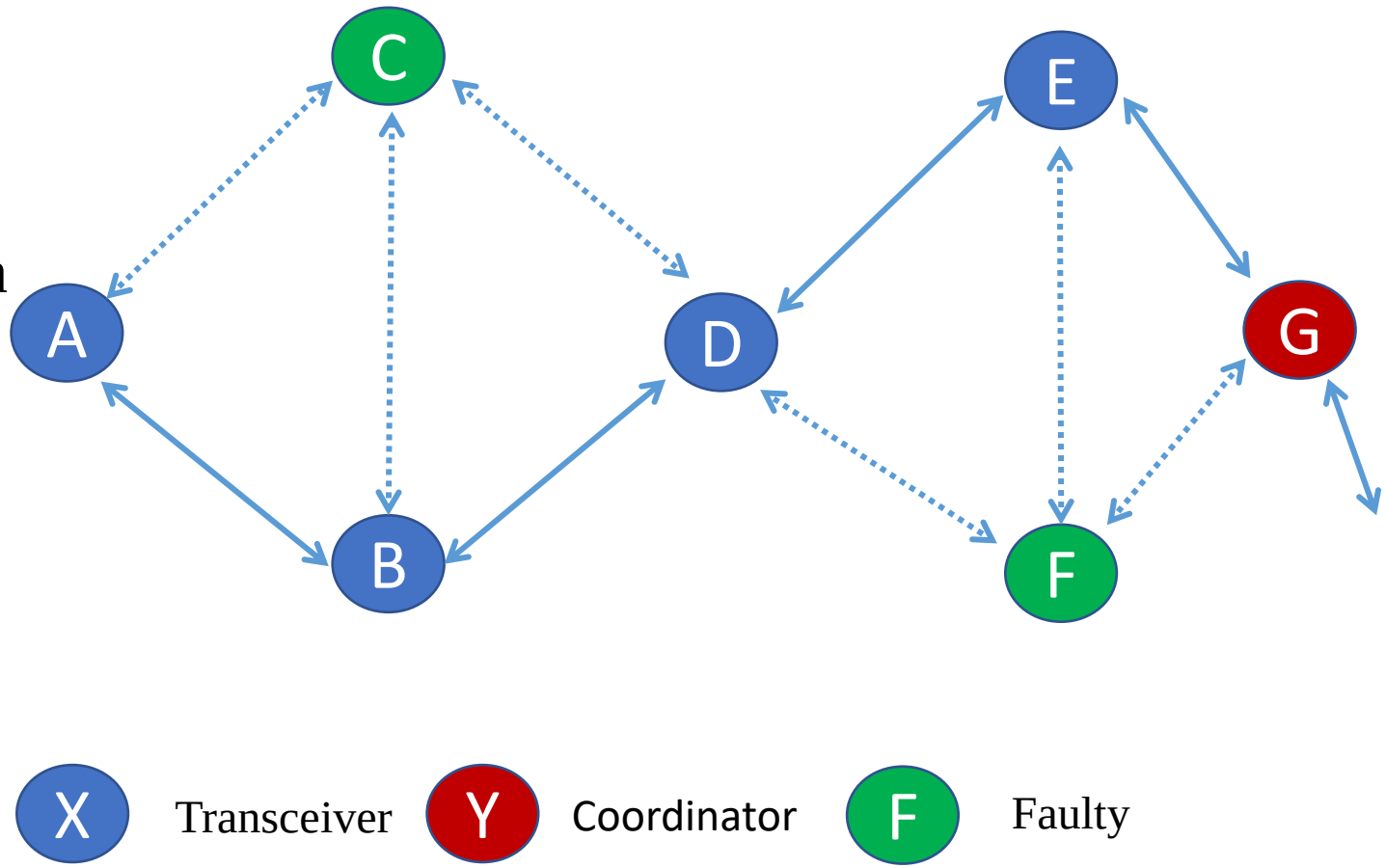
ZigBee Mesh

- In a mesh, any node can communicate with any other node within its range.
- If nodes are not in range, messages are relayed through intermediate nodes.
- This allows the network deployment over large areas.



ZigBee Mesh

- Meshes have increased network reliability.
- For example, if nodes C and F are down, the message packets from A can still be relayed to G via B, D and E.
- ZigBee mesh networks are self-configuring and self-healing.



ZigBee Network Structure

It consist of *three* types of devices.

1. Zigbee coordinator

2. Zigbee Router

3.Zigbee End devices

ZigBee Types

ZigBee Coordinator (ZC):

- The Coordinator forms the root of the ZigBee network tree and might act as a bridge between networks.
- There is a single ZigBee Coordinator in each network, which originally initiates the network.
- It stores information about the network under it and outside it.
- It acts as a Trust Center & repository for security keys.

ZigBee Types

- *ZigBee Router (ZR):*

  ✓ Play the role of intermediate nodes that connects two or more Zigbee devices of same or different types.

  ✓ Capable of running applications, as well as relaying information between nodes connected to it.

- *ZigBee End Device (ZED)*:

  ✓ It contains just enough functionality to talk to the parent node, and it cannot relay data from other devices.

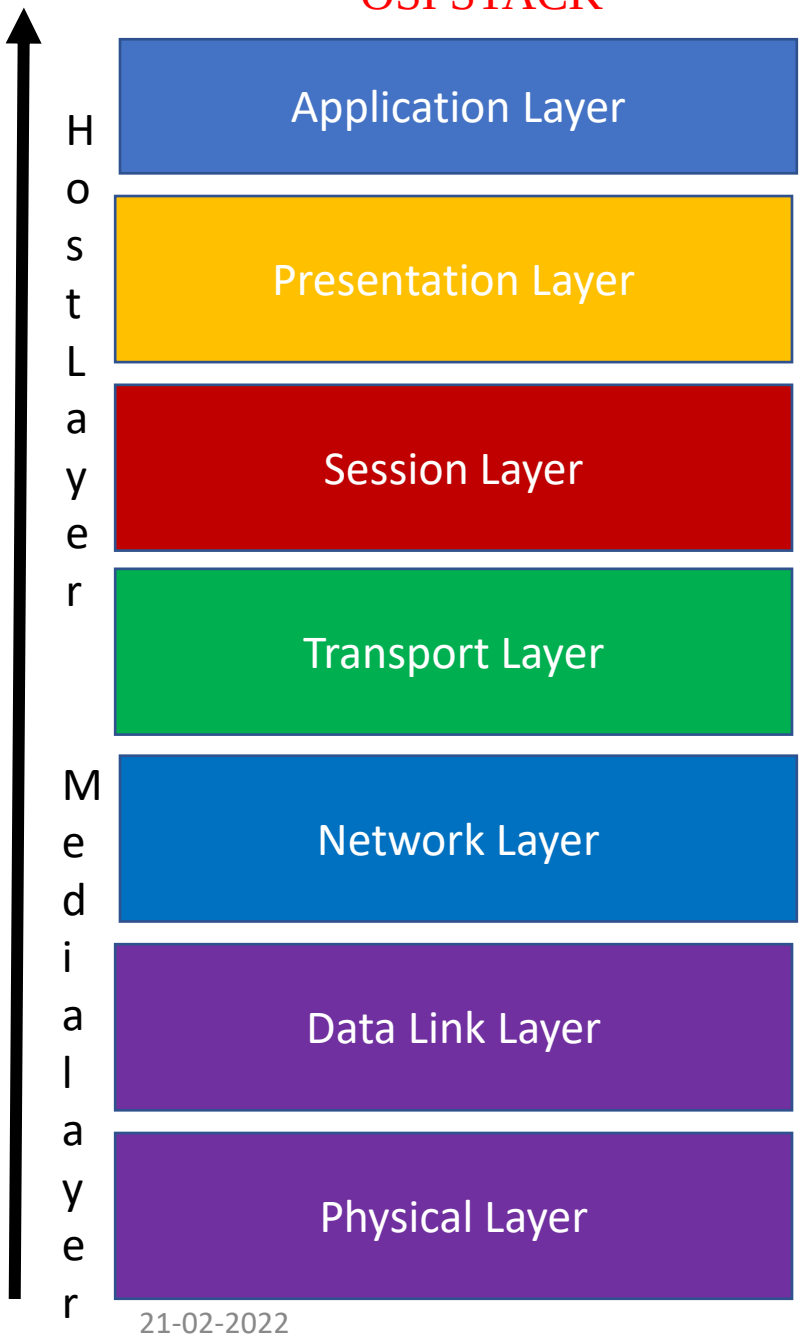
  ✓ This allows the node to be asleep a significant amount of the time thereby enhancing battery life.

  ✓ Memory requirements and cost of ZEDs are quite low, as compared to ZR or ZC

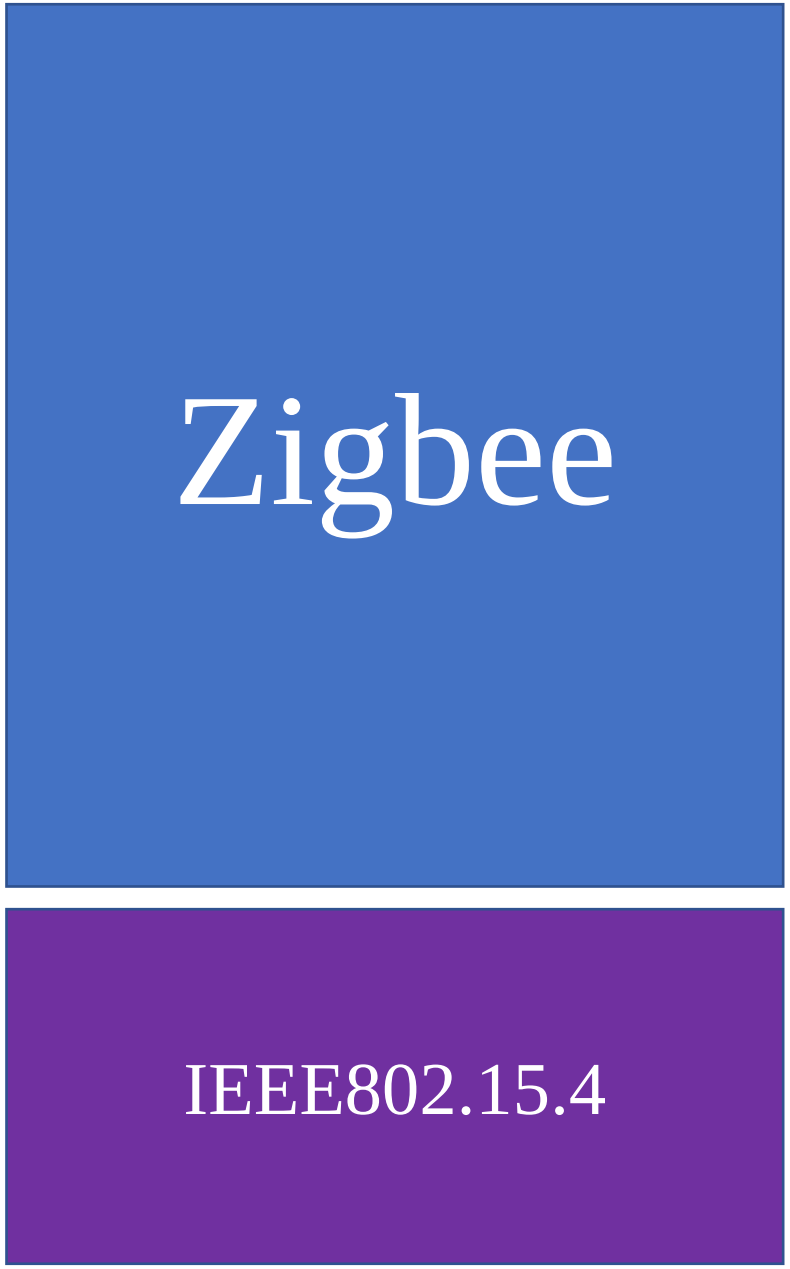
ZigBee Network Layer

- The network layer uses Ad Hoc On-Demand Distance Vector (AODV) routing.
- To find the final destination, the AODV broadcasts a route request to all its immediate neighbors.
- The neighbors relay the same information to their neighbors, eventually spreading the request throughout the network.
- Upon discovery of the destination, a low-cost path is calculated and informed to the requesting device via unicast messaging.

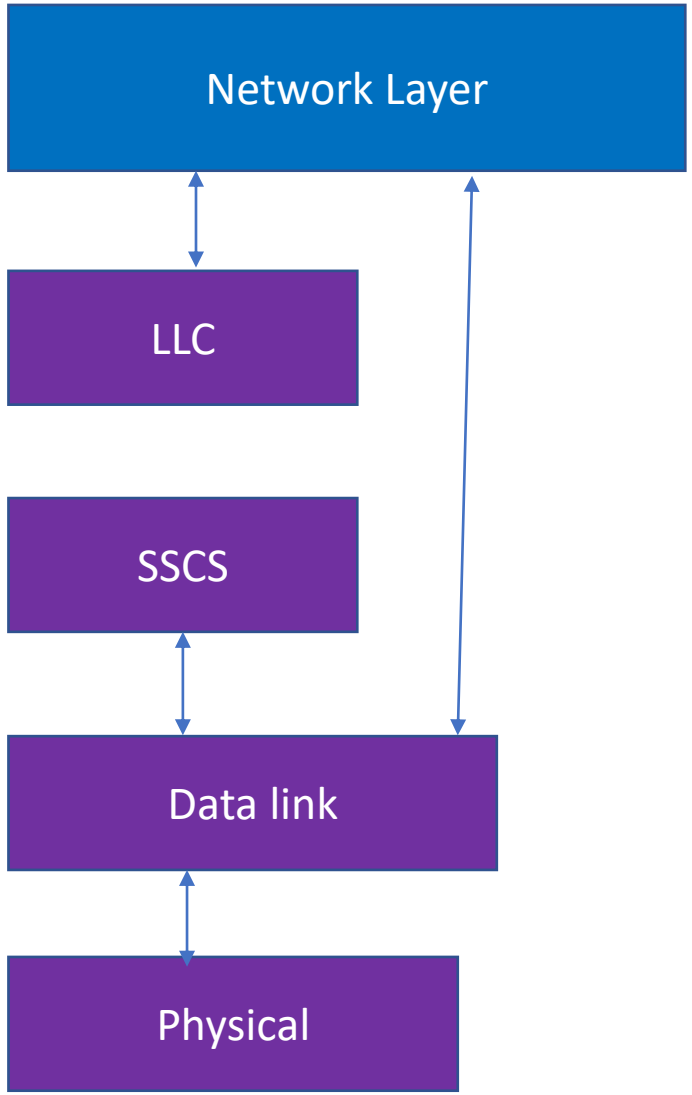
OSI STACK



Zigbee STACK



IEEE 802.15.4 STACK



Zigbee STACK

Physical Layer

- It transmits and receives signals.
- It performs modulation and demodulation operation on the data.
- It consists of 3 bands made up of 27 channels.
  - ✓ 2.4 GHz band has 16 channels at 250kbps.
  - ✓ 868.3 MHz has one channel at 20kbps.
  - ✓ 902-928 MHz has ten channel at 40kbps.

Zigbee STACK

MAC Layer

- It ensures channel access and reliability of data transmission.
- CSMA/CA is used for channel access and intra-channel interference avoidance.
- It handles communication synchronization using beacon frames.

Zigbee STACK

Network Layer

It handles operations such as

- ✓Setting up the network
- ✓Connecting and disconnecting the devices
- ✓Configuring the devices
- ✓Routing

Zigbee STACK

Application support sub-Layer

- It handles the interfacing services, control services, bridge between network and other layers.
- It enables the necessary services to interface with the lower layers for Zigbee device object (ZDO) and Zigbee application objects(ZAO).
- It handles data management services and service based device matching.

Important Components

ZDO

- ZigBee Device Object (ZDO)
  (Device management, Security, Policies)

APS

Application Support Sub-layer
(Interfacing and control services, bridge between network and other layers)

Zigbee STACK

Application Framework

- It provides provision for key-value pair and generation of generic messages.
- A key-value pair is used for getting attributes within the application objects.
- Generic messages are the developer defined structure.

Zigbee Data transfer Mode

It supports two types of data transfer modes.

1. Beacon mode
2. Non-beacon mode

Zigbee Data transfer Mode

Non-beacon mode

- The coordinator and router monitor the active state of the received data continuously.
- It is power intensive method.
- No provision to coordinator and router to sleep.

Zigbee Data transfer Mode

Beacon mode

- It allows co-Ordinator and router to launch into a very low power sleep state in the absence of data communication from end devices.
- The coordinator periodically wake up and transmits beacons to the available routers in the network.
- This method is used when there is no need for low duty cycle and more extended battery power consumption.

Applications

- Building automation
- Remote control (RF4CE or RF for consumer electronics)
- Smart energy for home energy monitoring
- Health care for medical and fitness monitoring
- Home automation for control of smart homes
- Light Link for control of LED lighting
- Telecom services

Thread

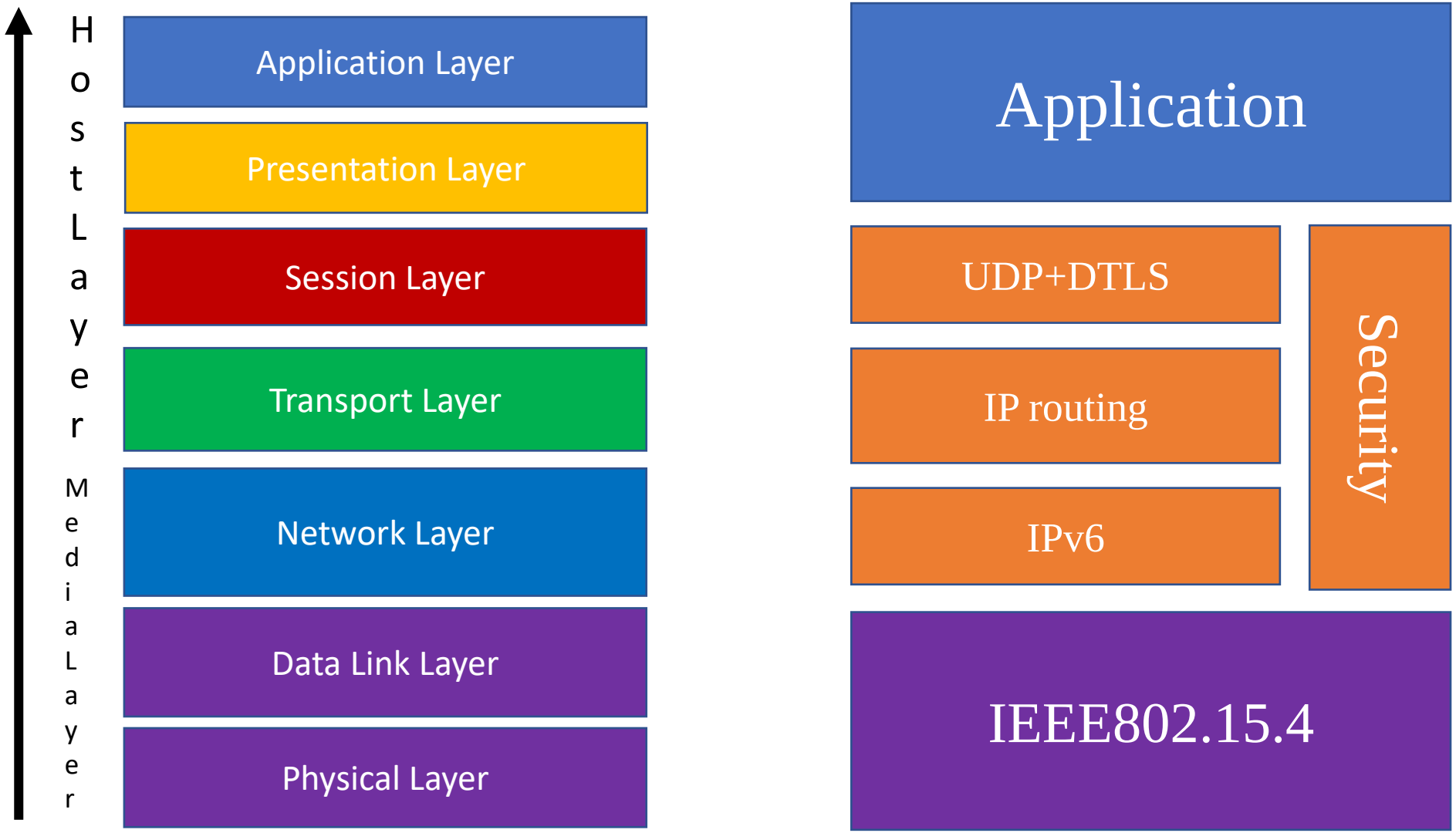
Thread

Introduction

- It is built upon IEEE 802.15.4 radio standard.
- Easy to set up and simple to build up.
- Used for low power consumption and low latency deployment applications.
- It can extend direct Internet connectivity to the connected devices.
- It supports interoperability, security, power, and architecture addressed in a single radio platform.
- It does not require any mobile phone or proprietary gateway to be in the range of devices for accessing the Internet.

Thread

The functional protocol stack of Thread in comparison to the OSI stack

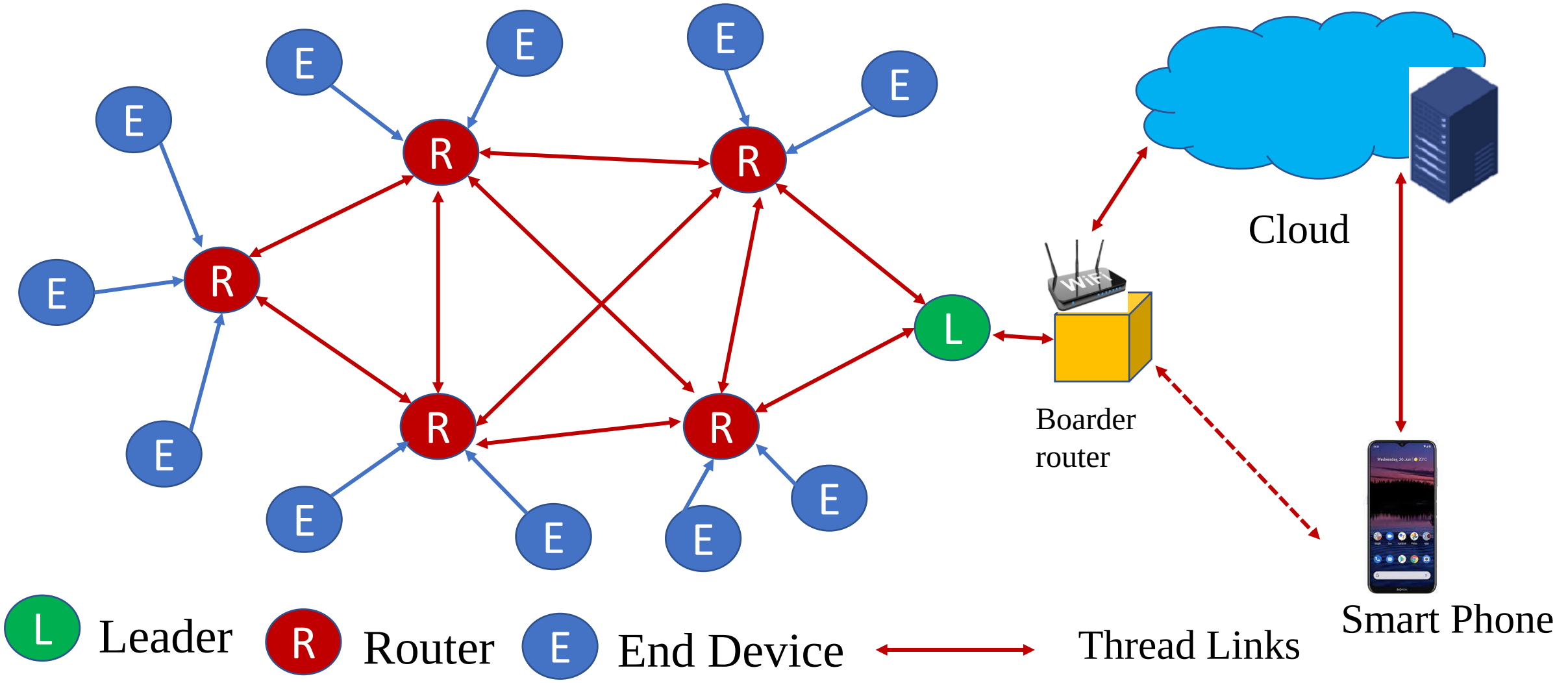


Thread

- It supports low power wireless mesh networking protocol with universal Internet protocol(IP) support.
- It can reliably connect thousand of devices to the Internet or cloud without single point of failure.
- It has self healing and reconfiguration feature with respect to the addition or removal of devices.
- It supports IoT interoperability by utilizing a certification application that validates a device's conformance to the specification and interoperability against multiple certified stacks.

Thread

Outline of the Thread network architecture (from end device to the cloud



Thread

Thread Devices

- Thread end devices are low power wireless devices with IP connectivity enablers.
- It can use common infrastructure similar to Wi-Fi network.
- It can directly connected to the smartphones or computers if they are in the same IP network without requiring any additional setup for thread.

Thread

Feature

- Thread devices removes the need for Internet enabled proprietary gateways and cross-stack translators for connection between other technologies.
- It supports larger IP-based networks.
- Better resilience to single point of failure.
- Highly economical deployments.
- Less complex infrastructure.
- Enhanced IoT end-to-end device security on Internet.

Thread

Applications

- Smart homes/ Buildings
- Connected vehicles

ISA 100.11A

ISA 100.11A

Introduction

- It is a low power communication standard.
- Developed and maintained by International Society of Automation.
- It uses IEEE 802.15.4 standard as a base for developing this protocol.
- Designed mainly for large scale industrial plant automation systems.
- More than 1 billion devices use ISA 100.11A.

ISA 100.11A

- For communication purpose, it uses 2.4 GHz frequency band.
- IoT compliant protocol stack can be integrated with wired network using ethernet, support for open access protocols and device-level interoperability.
- To avoid interference over wireless channels in the same band, it uses FHSS(frequency hopping spread spectrum) over the 16 channels.
- To achieve immunity over interference, it uses channel black listing concept (Black list the channel already used by the protocol).

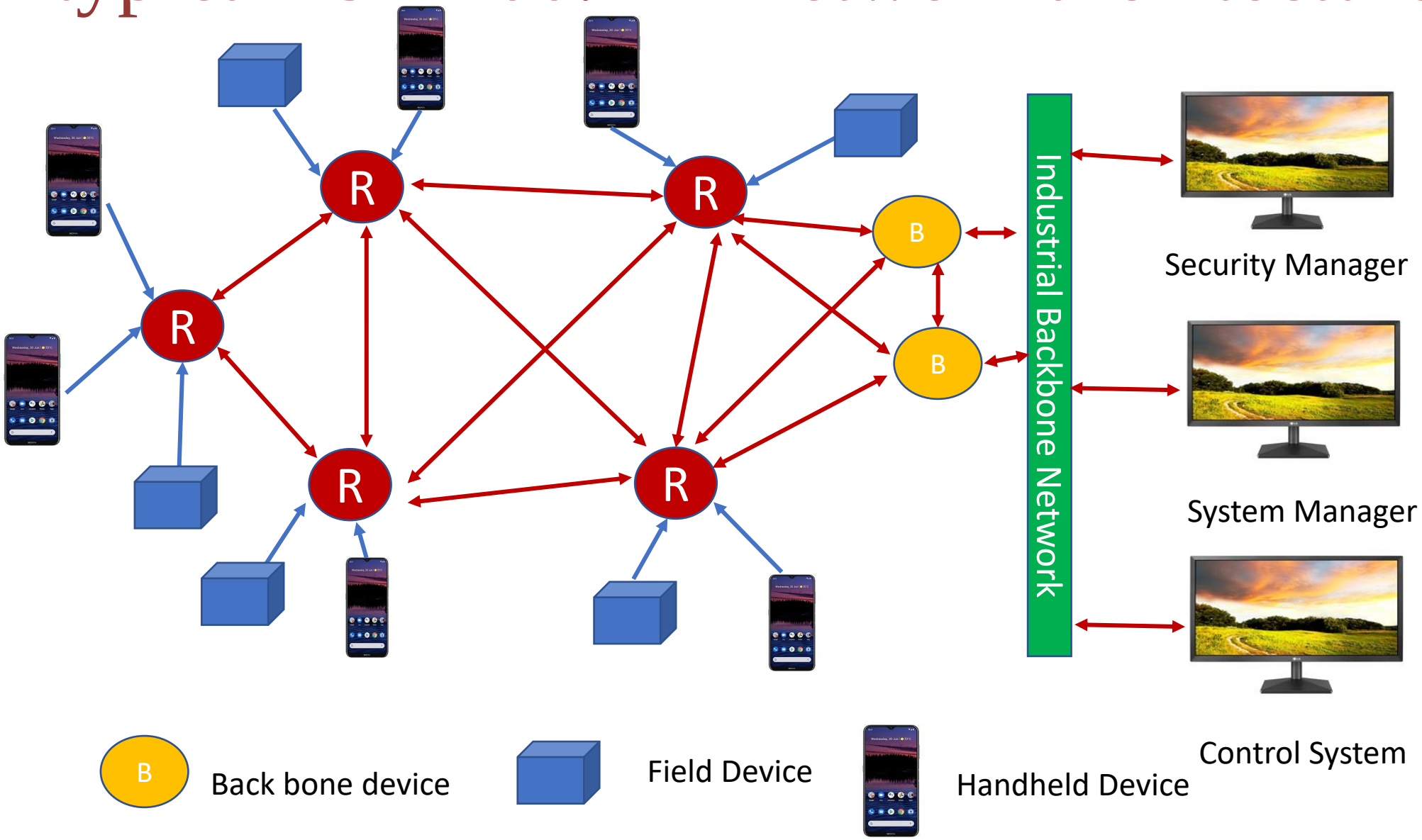
ISA 100.11A

- The use of IPv6 provides certain benefits and they are
  - ✓Enhances the address size
  - ✓Enhances IPSec-based security measures
  - ✓Saving network bandwidth by virtue of multicasting
  - ✓Auto address configuration

- 128-bit AES(Advanced Encryption Standard) encryption technique is used for communication of data.

- It uses TDMA (time division multiple access) based resource sharing with CSMA/CA.

A typical ISA 100.11A network architecture



ISA 100.11A network architecture

ISA 100.11A Devices:

It consist of two devices

- Field devices
- Backbone devices

ISA 100.11A network architecture

Field Devices

- Field devices are non routing I/O devices, handheld devices, routing devices.
- They are either fixed or mobile devices.
- For industrial usage, portable and mobile devices are highly desirable as it allows floor supervisors and workers to keep checking various parts of the plant without the need for dedicated devices for each part.

ISA 100.11A network architecture

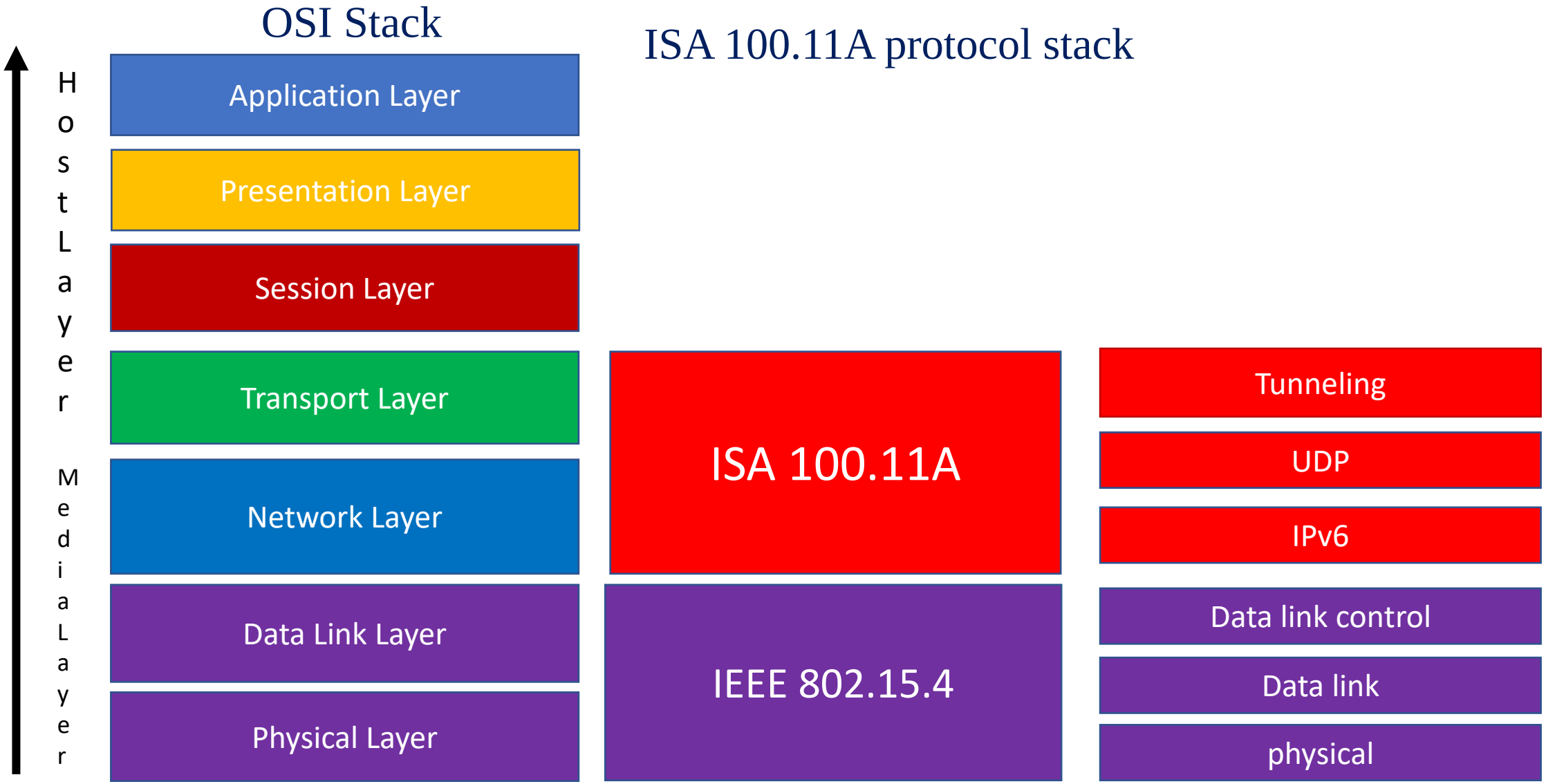
Backbone Devices

- It includes backbone routers, gateways, the system managers and security managers.
- These devices are fixed and not portable.

ISA 100.11A network architecture

- It supports for mesh, star and star-mesh topology.
- The connected devices are collectively referred to as Down link subnet.
- A wireless industrial sensor network (WISN) gateway connects the ISA 100.11A network to the plant network.
- A central system manager handles network routing by scheduling communication.

The ISA 100.11A protocol stack in comparison to the OSI Stack



ISA 100.11A

Physical Layer

- Physical layer is based on IEEE 802.15.4-2006 standard.
- It communicates on the 2.4 GHz frequency band using DSSS modulation.

ISA 100.11A

Data link layer

- It handles the creation, maintenance, forwarding packet functionalities, and MAC functionalities (operations dealing with the structure of the data packets, formation of frames, detecting errors, bus arbitration).

- DLC layer uses a graph based routing protocol (adaptive channel hopping, detection and recovery of message loss and clock synchronization).

ISA 100.11A

Network Layer

- This layer is 6LowPAN-compliant.
- It uses IPv6 addressing for an end to end routing.
- Protocol conversion from IPv6 to 6LowPAN and 6LowPAN to IPv6 is executed by router.

ISA 100.11A

Transport Layer

- It uses UDP based connectionless services.

Application Layer

- It supports system management applications.

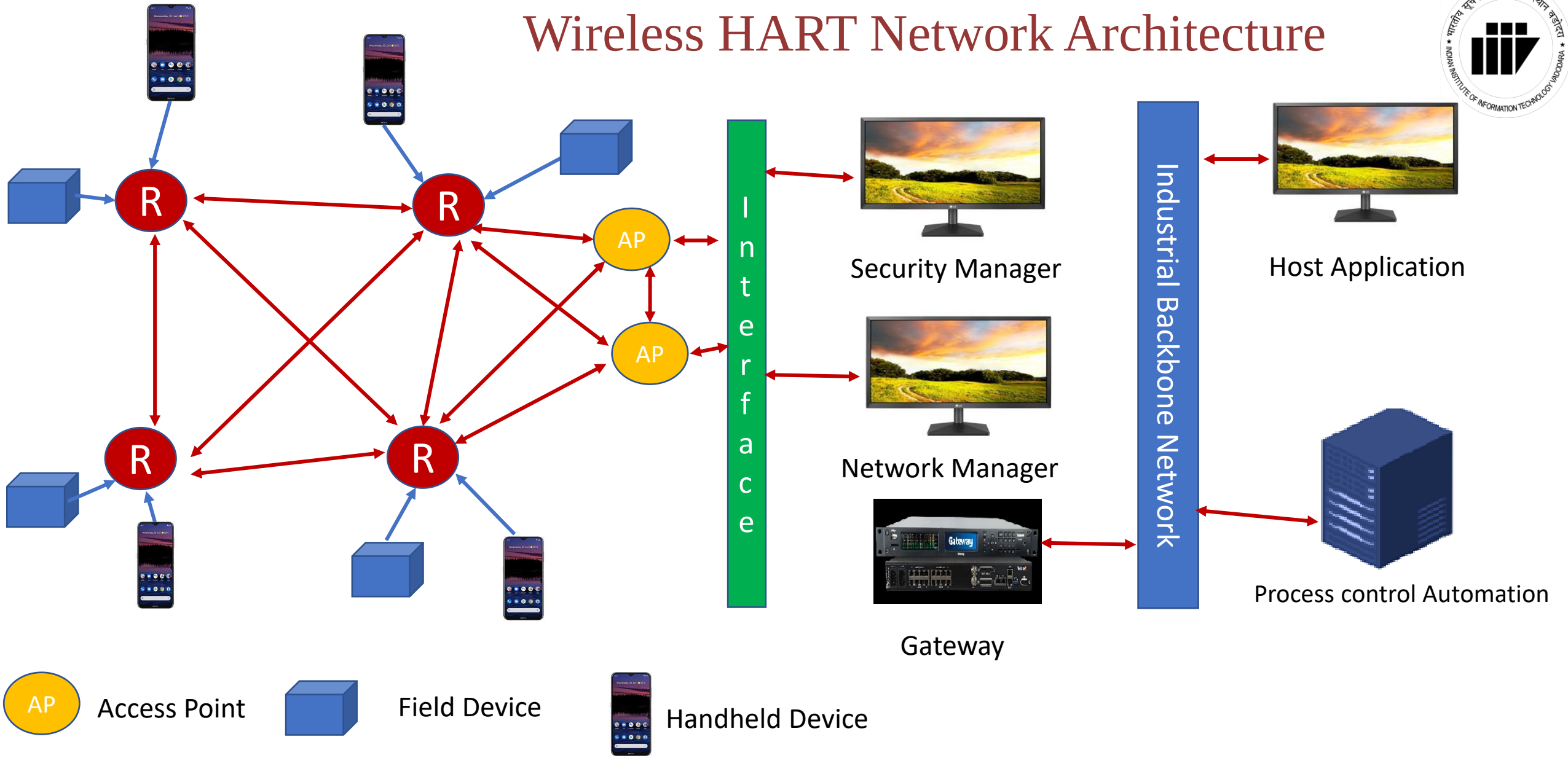
WirelessHART

WirelessHART

Introduction

- WirelessHART is the latest release of **Highway Addressable Remote Transducer** (HART) Protocol.
- It is license-free protocol.
- HART standard was developed for **networked smart field devices** in industrial environments.
- The wireless protocol makes the implementation of HART **cheaper and easier**.
- HART encompasses the most number of field devices incorporated in any field network.
- It uses IEEE 802.15.4 standard for its protocol designing.
- It supports highly encrypted communication

Wireless HART Network Architecture



Wireless HART Network Architecture

- It can communicate with a central control system in direct or indirect communication method.
- Direct communication is achieved when a device transmits data directly to the gateway in a clear LOS(max distance is 250m).
- Indirect communication is achieved between devices in a mesh and a gateway when messages jump from device to device until it reaches gateway.
- Communication between devices are 99.99% reliable due to the maintenance of a tight schedule between message transmission.

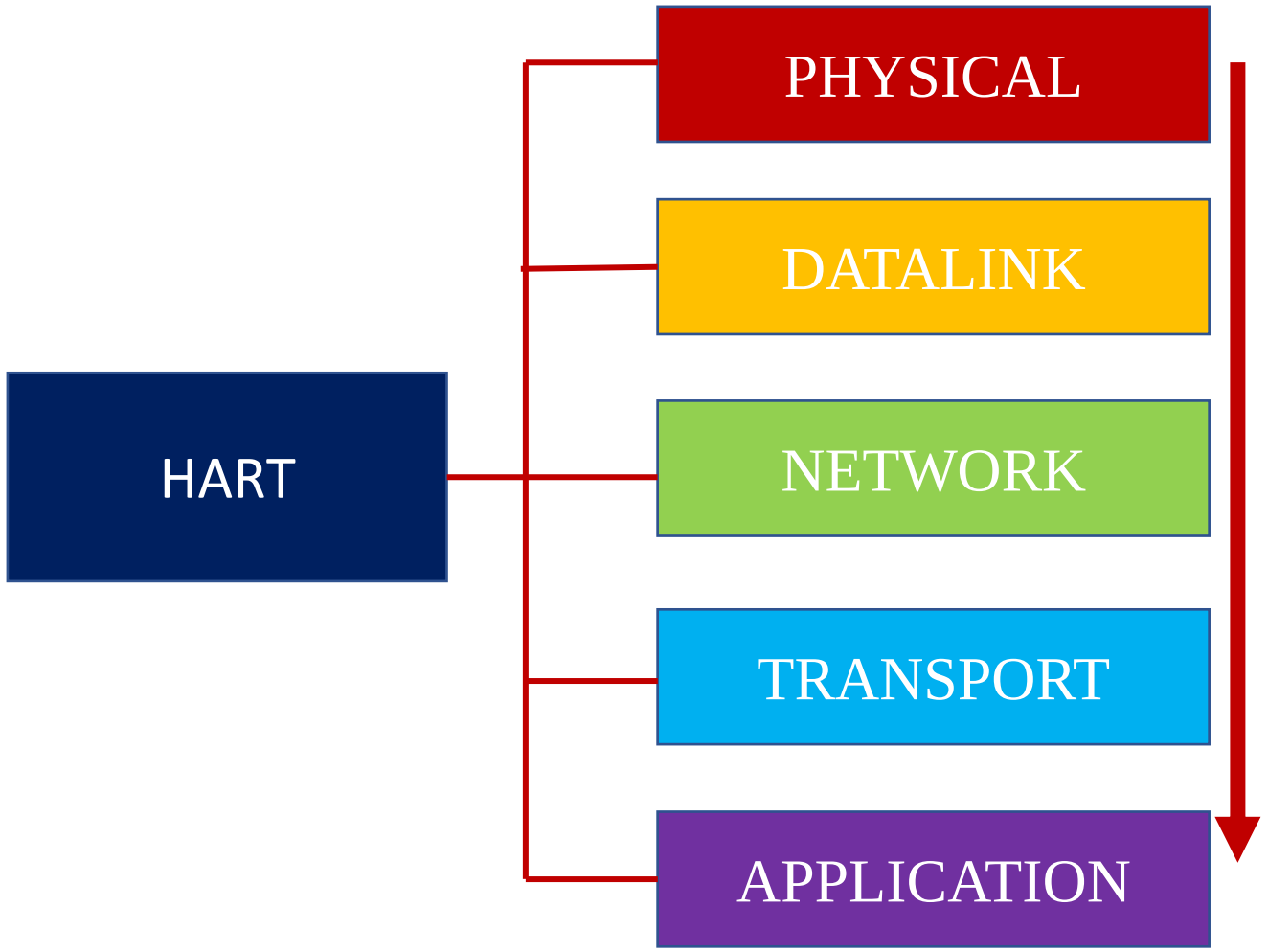
Wireless HART Network Architecture

Various components of wireless Hart network is

- Field device
- Handheld device
- Router
- Access Point
- Gateway
- Security Manager
- Network Manager

WirelessHART

- Wireless HART enables device placements more accessible and cheaper– such as the top of a reaction tank, inside a pipe, or at widely separated warehouses.
- Main difference between wired and unwired versions is in the physical, data link and network layers.
- Wired HART lacks a network layer



WirelessHART

HART Congestion Control

- Restricted to 2.4Ghz ISM band with channel 26 removed, due to its restricted usage in certain areas.
- Interference-prone channels avoided by using channel switching post every transmission.
- Transmissions synchronized using 10ms slots.
- During each slot, all available channels can be utilized by the various nodes in the network allowing for the propagation of 15 packets through the network at a time, which also minimizes the risk of collisions.

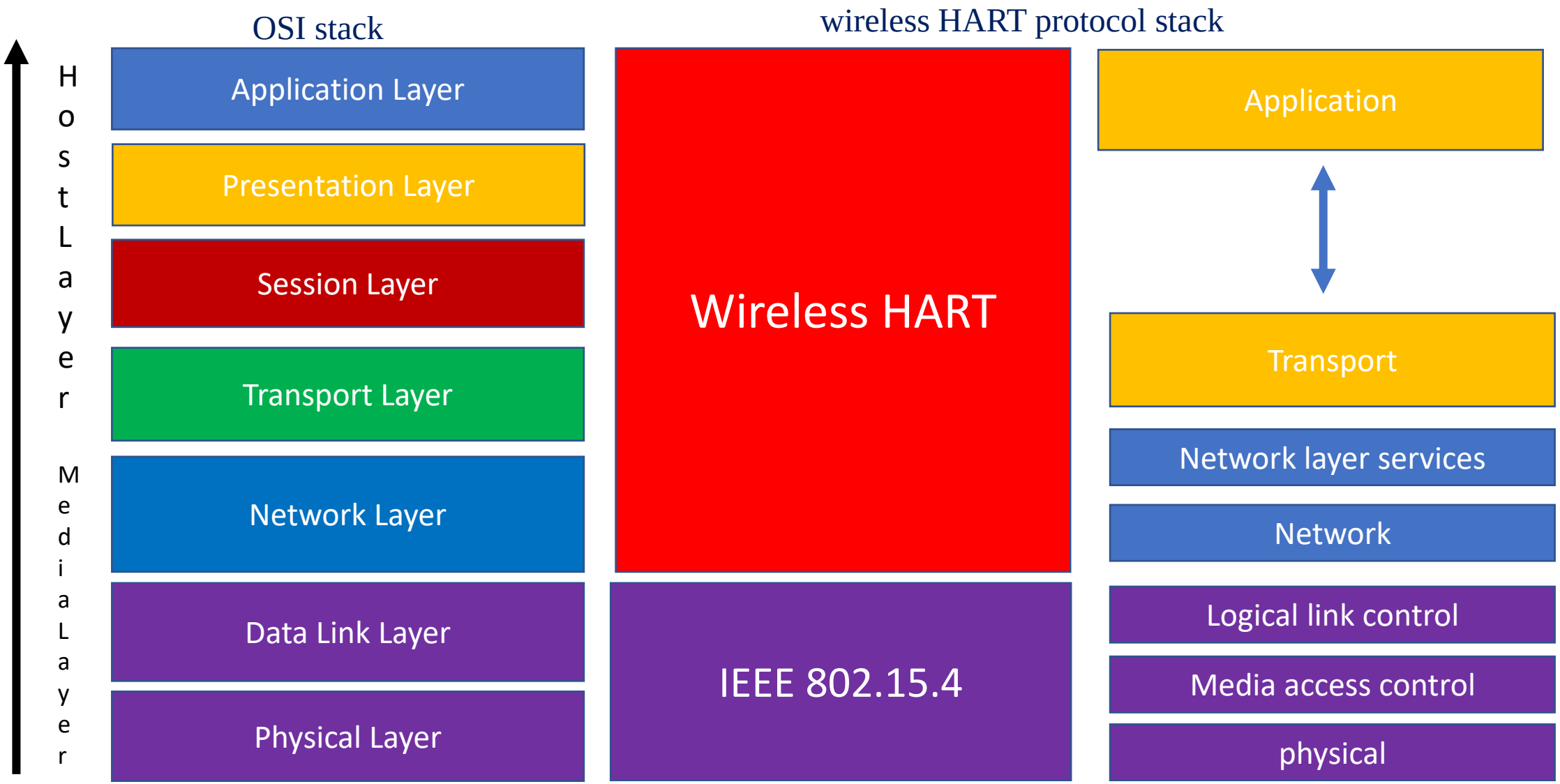
WirelessHART

WirelessHART Network Manager

- The network manager **supervises each node** in the network and guides them on **when and where** to send packets.
- Allows **for collision-free** and **timely delivery** of packets between a source and destination.
- The network manager **updates** information about neighbors, **signal strength**, and information needing delivery or **receipt**.
- Decides who will send, who will listen, and at what frequency is each time-slot.
- Handles **code-based network security** and prevents unauthorized nodes from joining the network.

WirelessHART

The wireless HART protocol stack in comparison to the OSI stack



WirelessHART

HART Physical Layer

- Derived from IEEE 802.15.4 protocol.
- It operates only in the 2.4 GHz ISM band.
- Employs and exploits 15 channels of the band to increase reliability.

WirelessHART

HART Data Link Layer

- Collision free communication is achieved by use of TDMA.
- Deterministic communication is made by the use of super-frames.
- Super-frames consist of grouped 10ms wide timeslots.
- Super-frames control the timing of transmission to ensure collision free and reliable communication.
- This layer incorporates channel hopping and channel blacklisting to increase reliability and security.
- Channel blacklisting identifies channels consistently affected by interference and removes them from use.

WirelessHART

HART Network & Transport Layers

- Cooperatively handle various types of network traffic, routing, session initiation/termination, and security.
- WirelessHART relies on **Mesh networking** for its communication, and each device is primed to forward packets from every other devices.
- Each device is armed with an updated network graph (i.e., updated topology) to handle routing.
- **Network layer (HART)=Network + Transport + Session layers (OSI)**

WirelessHART

HART Application Layer

- Handles communication between gateways and devices via a series of **command and response messages**.
- Responsible for **extracting** commands from a message, **executing** it and generating responses.
- This layer is seamless and does not differentiate between wireless and wired versions of HART.

WirelessHART

WirelessHART vs. ZigBee

- A WirelessHART node **hops after every message**, changing channels every time it sends a packet. ZigBee does not feature hopping at all, and only **hops when the entire network hops**.

- At the MAC layer, WirelessHART utilizes time division multiple access (**TDMA**), allotting individual time slots for each transmission. ZigBee applies carrier sense multiple access with collision avoidance (**CSMA/CA**).

WirelessHART

- WirelessHART represents a true mesh network, where each node is capable of serving as a router so that, if one node goes down, another can replace it, ensuring packet delivery. ZigBee utilizes a tree topology, which makes nodes along the trunk critical.

- WirelessHART devices are all back compatible, allowing for the integration of legacy devices as well as new ones. ZigBee devices share the same basis for their physical layers, but ZigBee, ZigBee Pro, ZigBee RF4CE, and ZigBee IP are otherwise incompatible with each other

RFID

RFID

Introduction

- RFID is an acronym for “radio-frequency identification”.
- This technology uses tags and readers for communication.
- Data digitally encoded in RFID tags, which can be read by a reader.
- Somewhat similar to barcodes.
- Data read from tags are stored in a database by the reader.
- As compared to traditional barcodes and QR codes, RFID tag data can be read outside the line-of-sight.

RFID

RFID Features

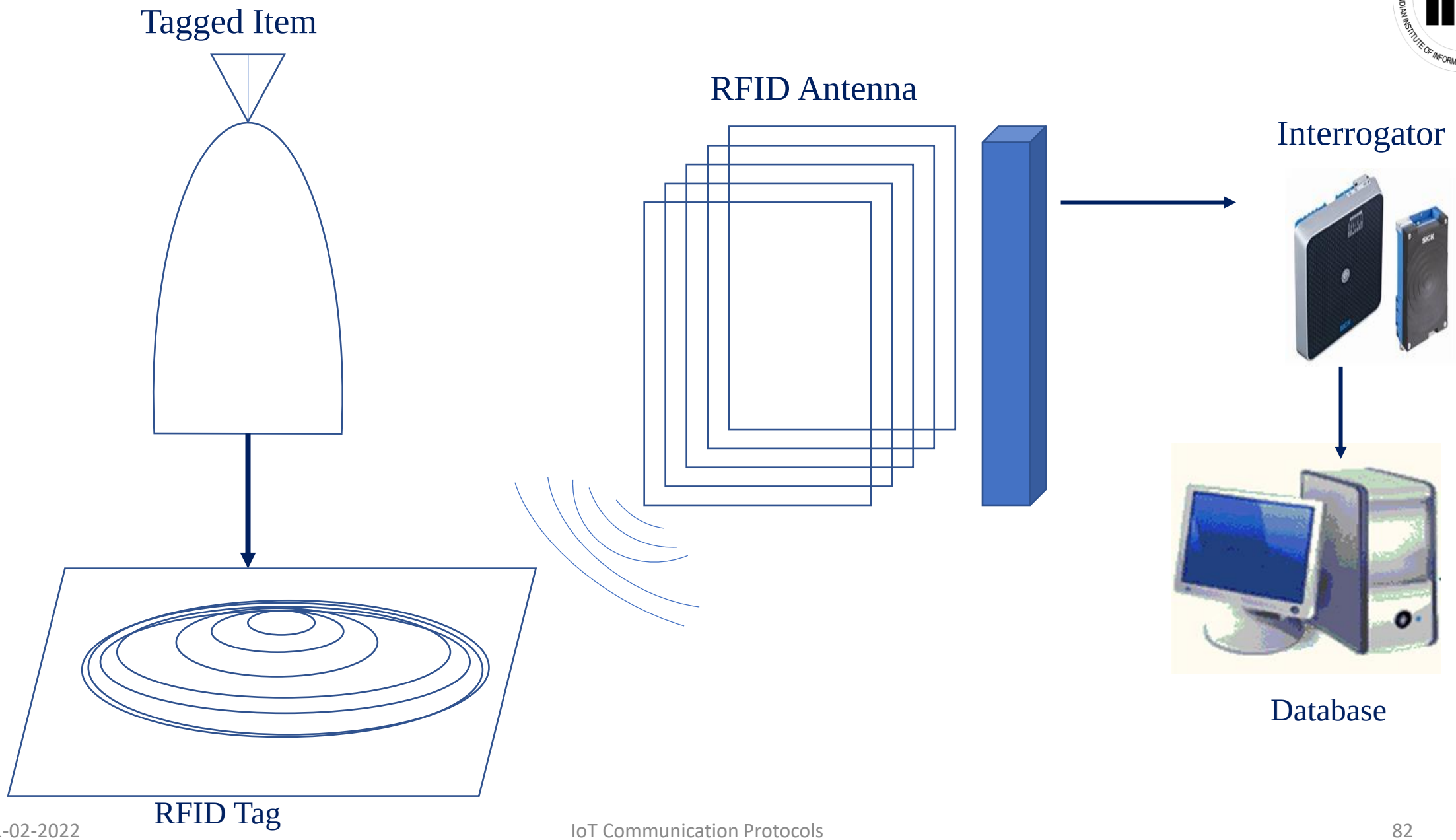
- RFID tag consists of an integrated circuit and an antenna.
- The tag is covered by a protective material which also acts as a shield against various environmental effects.
- Tags may be passive or active.
- Passive RFID tags are the most widely used.
- Passive tags have to be powered by a reader inductively before they can transmit information, whereas active tags have their own power supply.

RFID

Working Principle

- Derived from Automatic Identification and Data Capture (AIDC) technology.
- AIDC performs object identification, object data collection and mapping of the collected data to computer systems with little or no human intervention.
- AIDC uses wired communication.
- RFID uses radio waves to perform AIDC functions.
- The main components of an RFID system include an RFID tag or smart label, an RFID reader, and an antenna.

An outline of the RFID operation and communication



RFID

- RFID tag is consist of an integrated circuit and an antenna, enclosed in a protective casing to protect from wear and tear and environmental effects.

- RFID tag is of two types.
  - ✓ Active tag
  - ✓ Passive tag

- Passive tag is widely used in various applications.
- Low cost tag
- Tag is powered by RFID reader before data transmission.

- Active tag has its own power sources.
- It does not require external activation by readers.
- High cost tag

RFID

- RFID tag are used for transmitting data to an RFID interrogator or an RFID reader.
- Radio waves are converted into a more usable form data by this reader.
- A host computer system accesses collected data on the reader by a communication technology such as wifi or ethernet.
- Data on the host system is finally updated in the database.

RFID

Applications

- ✓ Inventory management
- ✓ Asset tracking
- ✓ Personnel tracking
- ✓ Controlling access to restricted areas
- ✓ Supply chain management
- ✓ Counterfeit prevention (e.g. in the pharmaceutical industry)

THANK YOU

IoT Processing Topologies and Types

- List common data types in IoT applications
- Understand the importance of processing
- Explain the various processing topologies in IoT
- Understand the importance of processing offloading toward achieving scalability and cost effectiveness of IoT solutions
- Determine the importance of choosing the right processing topologies and associated considerations while designing IoT application.
- Determine the requirements that are associated with IoT based processing of sensed and communicated data.

Data Format

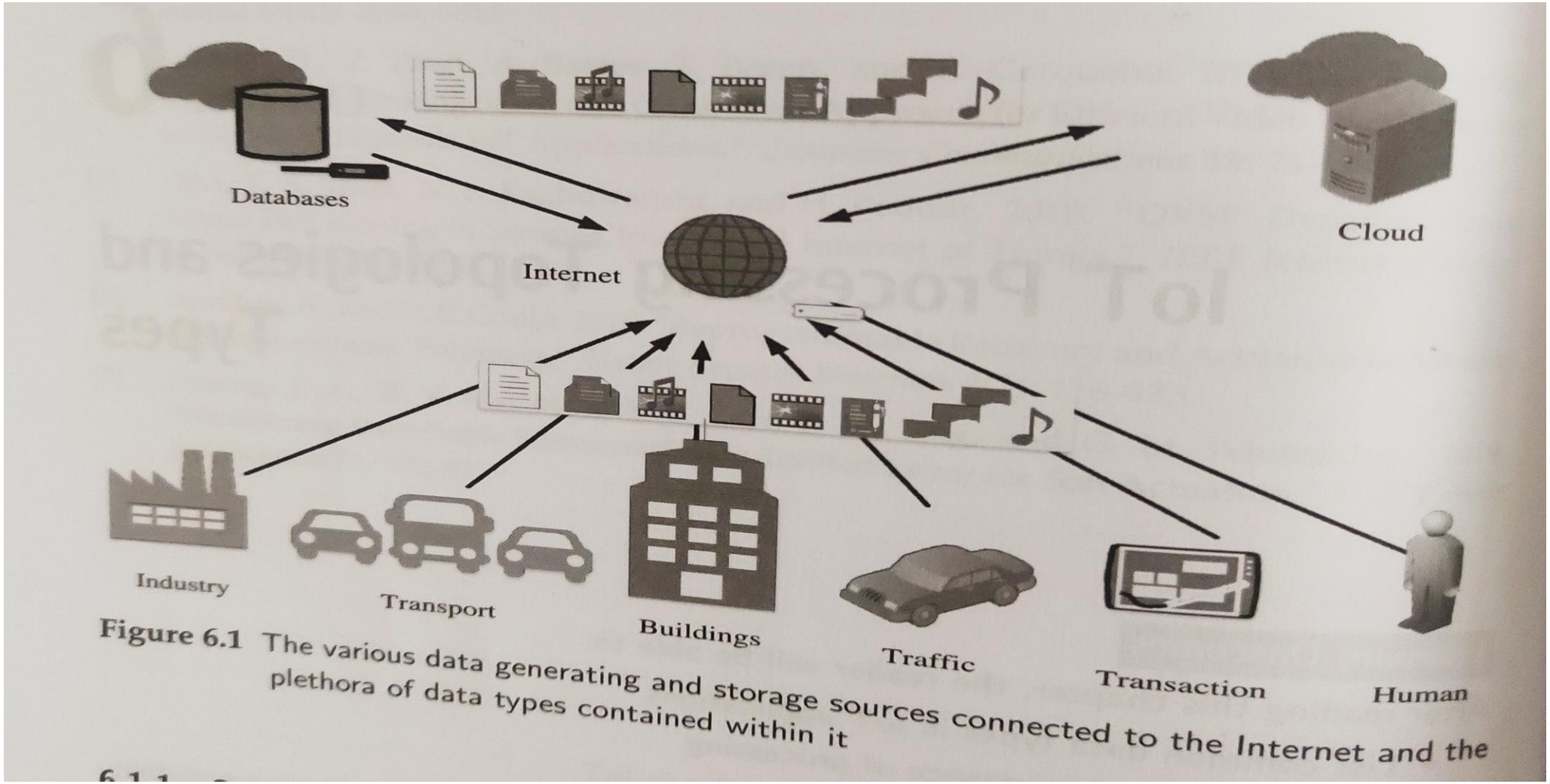


Figure 6.1 The various data generating and storage sources connected to the Internet and the plethora of data types contained within it

Data Format

- Huge quantities and varieties of data are generated regularly by users in Internet.

- Data generating sources include human (e-mails, text documents, social media posts, videos, audios, images etc.)and non human data generating sources(sensor nodes, automated monitoring systems etc.).

- These data are broadly grouped into two types and they are
  - ✓Structured data
  - ✓Unstructured data

Data Format

Structured data

- It has predefined structure.
- It is associated with RDBMS.
- It is created by length limited data fields.
- These data are either human or machine generated.
- It is searchable by querying algorithms.
- Example: Flight or train reservation system, banking system, Inventory control, etc.
- Accessing data is done by SQL.
- In IoT, it holds minor share of total generated data over Internet.

Data Format

Unstructured data

- It has no predefined structure and can vary according to application and data generating sources.
- These data are either human or machine generated.
- It is very difficult to search by querying algorithms.
- Example of human generated data: text, e-mails, videos, images, phone recording, chats etc.
- Example of machine generated data: sensor data from traffic, buildings, industries, etc.
- Accessing data is done by NoSQL.
- In IoT, it holds major share of total generated data over Internet.

Importance of processing in IoT

- It needs intelligent and resourceful processing techniques.
- When to process and what to process???
- The data to be processed is divided into three types.

  ✓Very time critical data

  ✓ Time critical data

  ✓Normal data

Importance of processing in IoT

Very time critical data

- The data which needs immediate decision support are called as very critical data.
- Example: healthcare, flight control system, etc.
- These data have very low threshold of processing latency.
- Its processing latency varies in the range of few milliseconds.
- Requirements of data processing is critically high.
- The need for data processing in place or almost nearer to the source is crucial in achieving the deployment success.

Importance of processing in IoT

Time critical data

- Data from sources can tolerate normal processing latency.
- Example: vehicles, traffic, machine systems, smart home systems, surveillance systems etc.
- It can tolerate a processing latency of few seconds.
- The processing requirements allow for transmission of data to be processed to remote locations/processors such as clouds or through collaborative processing.

Importance of processing in IoT

Normal data

- Data from less sensitive domains and can tolerate normal processing latency.
- Example: Agriculture, environmental monitoring etc.
- It can tolerate a processing latency of few minutes to hours.
- It has no time requirements for processing urgently and pursued leisurely as such.

Processing Topologies

- Processing solutions are broadly categorized into two types.

  ✓On-site processing topologies

  ✓Offsite processing topologies.

    - Remote Processing
    - Collaborative processing

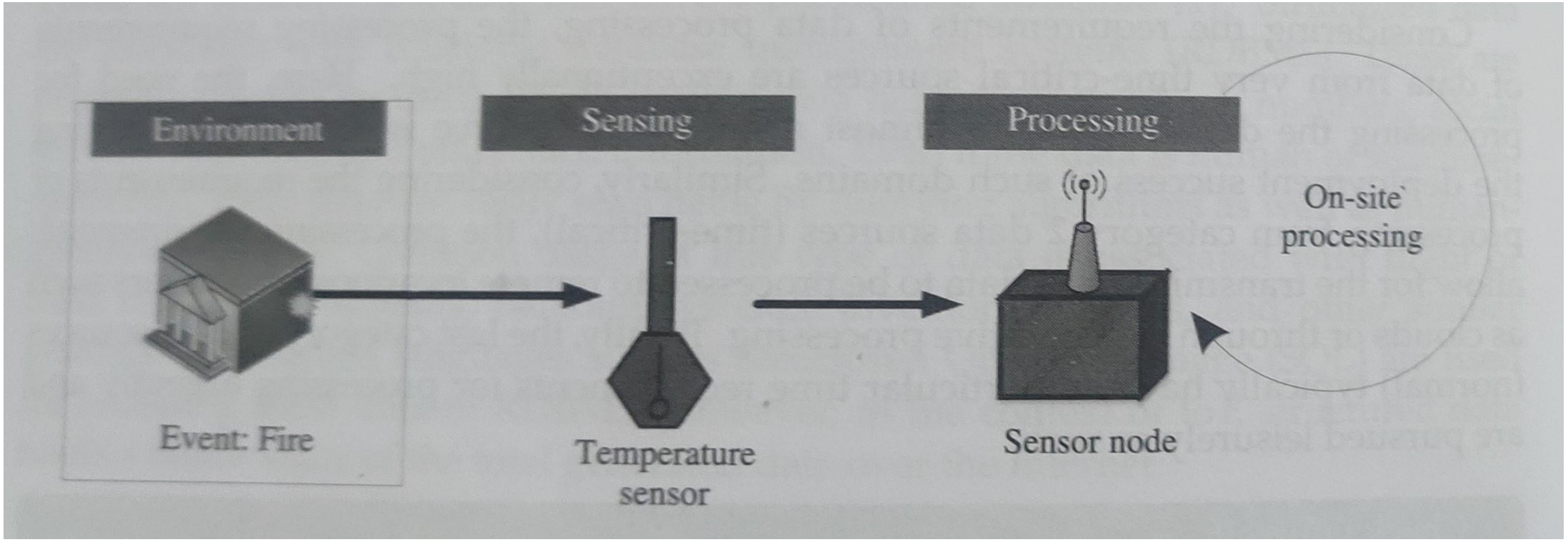
Processing Topologies

On-site processing topologies

- The data is processed at the source itself.
- It is used for IoT applications having a very low tolerance of latencies.
- Example: Healthcare, flight control systems.
- These show rapid temporal changes that can be missed unless the processing infrastructure is fast and robust enough to handle such data.

Processing Topologies

Event detection using an on-site processing topologies



Processing Topologies

Off-site processing

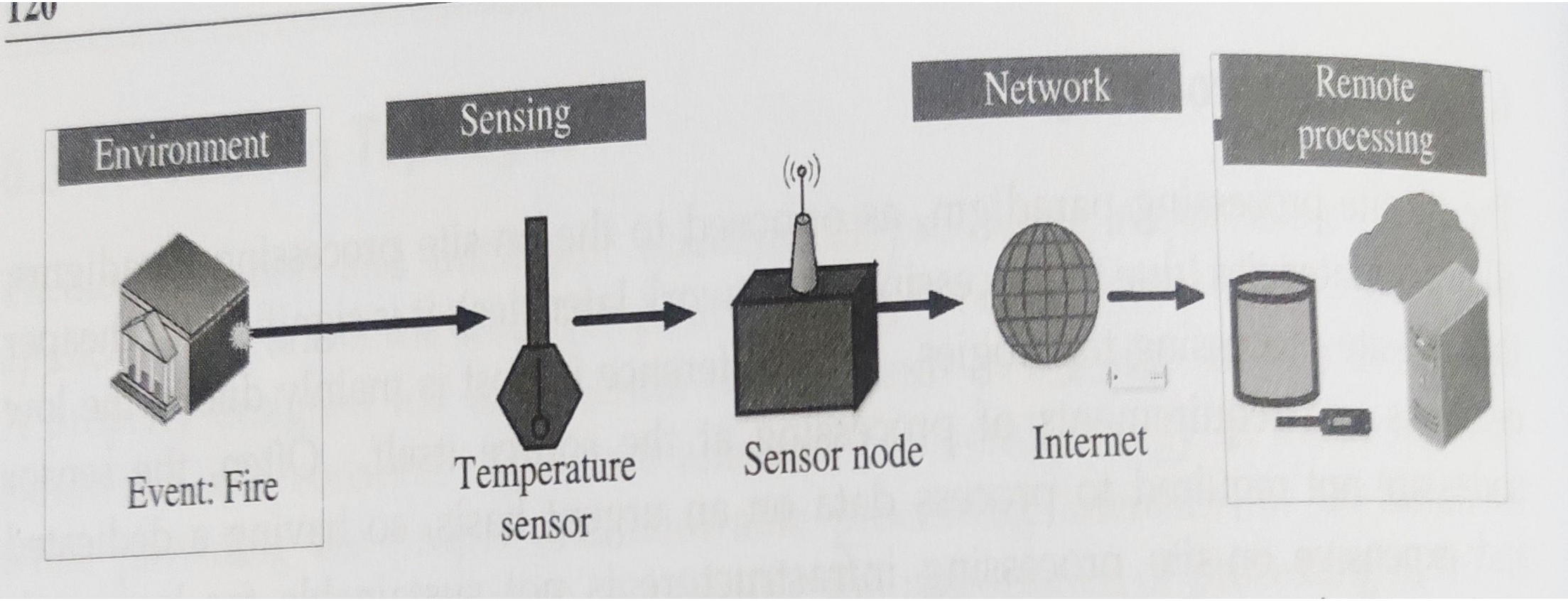
- It allows processing and network latencies.
- It is cheaper than onsite processing topologies.
- It is suitable for low demands and requirements of processing at source itself.
- As it does not require a dedicated and expensive onsite processing infrastructure, it is suitable for large scale IoT deployment applications.
- Sensor node is responsible for collection and framing of data that was eventually transmitted to another location for processing.
- It has few dedicated high processing enabled devices.
- The data generated from sources are transmitted to a remote location which can be a server or cloud or multiple processing nodes.

Processing Topologies

Remote Processing

- It is more popular processing topologies.
- It encompasses sensing of data by various sensor nodes, the data is then forwarded to a remote sensor or a cloud based infrastructure for further processing and analytics.
- It is cost effective and energy efficient processing topologies.
- Reuse and reallocation of same processing resources.
- Deployment of smaller and simpler processing nodes at the site of deployment.
- It ensures massive scalability of solutions without affecting the cost of deployments.
- It uses a lot of network bandwidth and relies heavily on presence of network connectivity between the sensor nodes and remote processing infrastructure.

Event detection using an off-site remote processing topologies

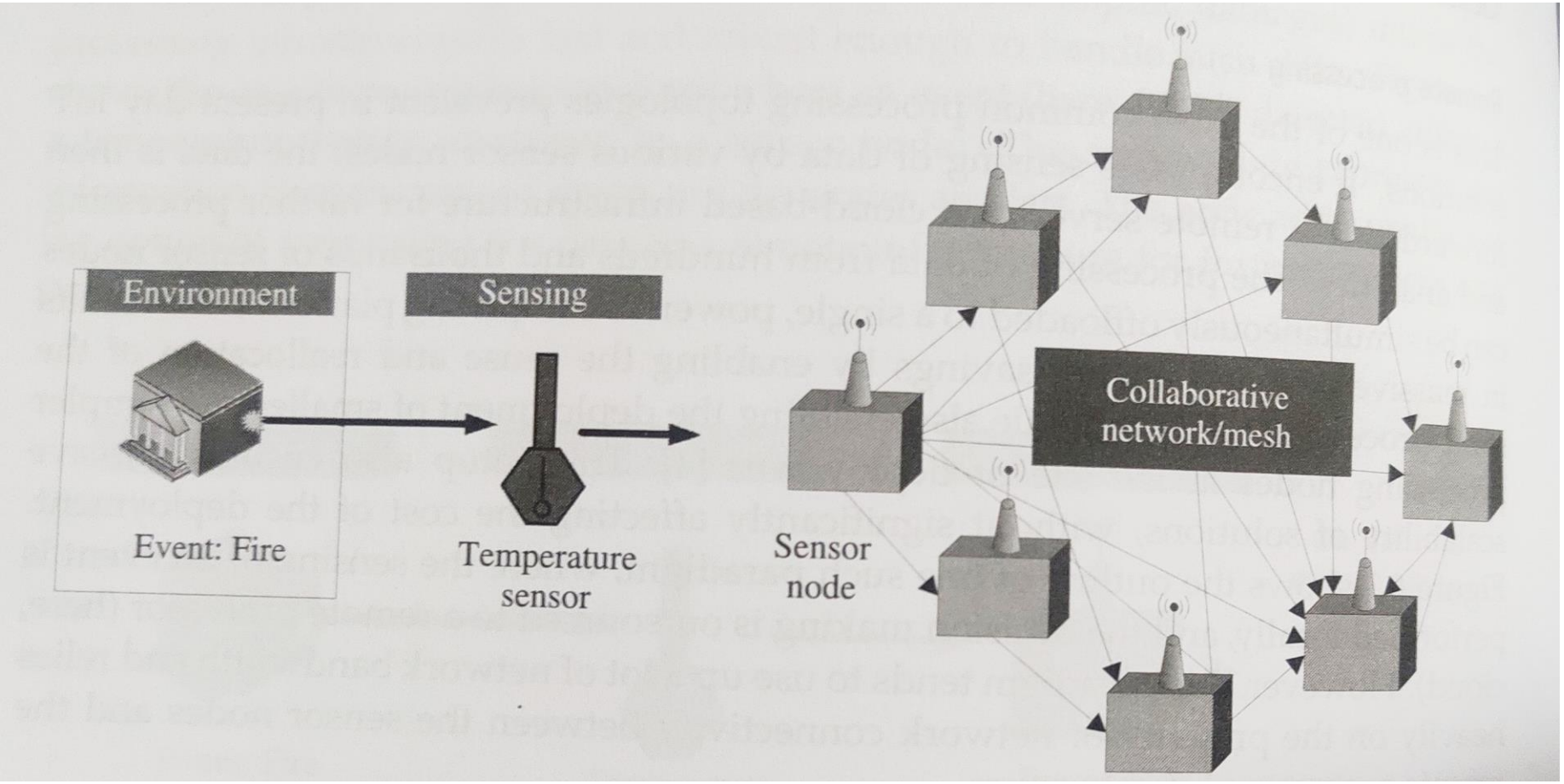


Processing Topologies

Collaborative processing

- It is suitable for systems lacking of a backbone network.
- Economical for large scale deployments spread over a vast areas.
- Providing network access to a remote infrastructure is not viable.
- Club together the processing power of nearby processing nodes and collaboratively process the data in the vicinity of the data source itself.
- It reduces the processing and network latencies.
- It conserves bandwidth of the network.
- It is suitable for agriculture applications.
- It uses mesh network for easy implementation of topology.

Event detection using collaborative processing topologies



IoT Device Design and Selection Considerations

- The selection of processor for developing the sensing solution is governed by usability, design, and affordability of IoT solution.

- The major factors governing the IoT device design and selection are
  - ✓Size
  - ✓Energy
  - ✓Cost
  - ✓Memory
  - ✓Processing power
  - ✓I/O rating
  - ✓Add-ons

IoT Device Design and Selection Considerations

Size

- This is a crucial factor for deciding the form factor.
- Larger the form factor, larger the energy consumption of the hardware.
- Larger the form factor are not suitable for most of IoT applications (wearable solutions).

IoT Device Design and Selection Considerations

Energy

- Energy requirements of a processor is a important deciding factor in designing a IoT solution.
- Higher the energy requirements, higher the energy source replacement frequency.
- This solution automatically lowers the long term sustainability of sensing hardware.

IoT Device Design and Selection Considerations

Cost

- The cost of a processor is the driving force in deciding the density of the deployment of sensor nodes.
- Cheaper the cost of hardware enables a much higher density of hardware deployments by users.
- Example: cheaper gas and fire detection solutions would enable users to include much more sensing hardware for a lesser cost.

IoT Device Design and Selection Considerations

Memory

- The memory requirements of IoT devices determines the capabilities the device can be armed with.
- Devices with higher memory tend to be more costlier.
- Local data processing, data storage, data filtering, data formatting, etc. requires memory heavily.

IoT Device Design and Selection Considerations

Processing power

- Processing power is vital in deciding what type of sensors can be accommodated with the IoT devices and what processing feature can integrated on-site with the IoT device.
- It decides the type of application the device can be associated with.
- Applications that handles video and image data require IoT devices with higher processing power compared to applications requiring simple sensing of the environments.

IoT Device Design and Selection Considerations

I/O Rating

- The input and output rating of IoT device depends on circuit complexity, energy usage, and sensor types.
- New processor have a meager I/O voltage rating of 3.3V as compared to 5V in old processor.
- This translates to requiring additional voltage and logic conversion circuitry to interface legacy technology and sensor with new processor.
- Low power consumption due to reduced I/O voltage levels can affect the complexity of the circuit and also reduces the cost.

IoT Device Design and Selection Considerations

Add-ons

- IoT devices provides add-ons as analog to digital conversion units, in-built clock circuits, connection to the USB and ethernet, inbuilt wireless access capabilities.
- The provision of this add-ons decides how fast a solution can be developed i.e hardware part of the whole application.
- An integration and interfacing of systems at the circuit level can be daunting to the uninitiated, prior presence of these options with the processor make the processor or device highly lucrative to the users/developers.

Processing Offloading

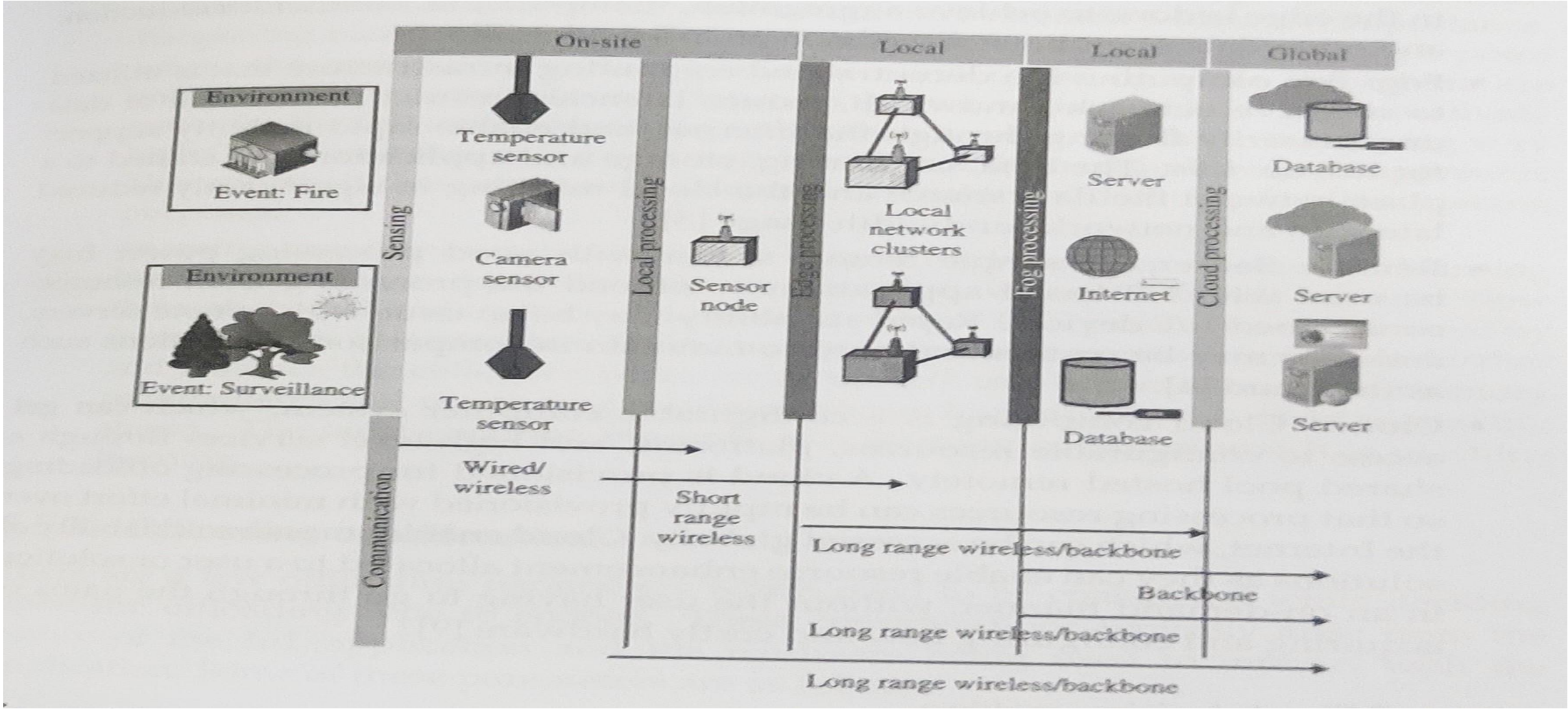
Why process offloading?

- It is important for developing a densely deployable, energy conserving, miniaturized and cheap IoT based solution.

Processing layers include

- ✓ local processing
- ✓ Edge processing
- ✓ Fog processing
- ✓ Cloud processing.

The various data generating and storage sources connected to the Internet and the plethora of data types contained within it



Processing Offloading

- First layer is sensing layer, in which multiple sensing types task (fire, surveillance) are includ
- Sensors integrated with a processor and wireless and wired connections.
- Decide On-site or off-site processing topology is followed based on criticality of application.
- In off-site processing data is forwarded to fog or remote server or cloud or edge.
- The edge layer makes use of local devices to process data using short range communication protocol.
- Fog based processing is limited within a geographical location, uses short range communications.
- Cloud based processing uses long range communication.

Processing Offloading

- Data offloading

Data is processed in a allocation other than the source of data.

- It is divided into three parts.

1. Offload location
2. Offload decision making
3. Offload considerations

Processing Offloading

Offload location

- It outlines where all processing can be offloaded in the IoT architecture.
- It decides the applicability, cost, and sustainability of the IoT application.
- Various offload location includes
  - ✓Edge
  - ✓Fog
  - ✓Remote Server
  - ✓Cloud

Processing Offloading

Edge

- The data processing is facilitated to a location at or near the source of data generation itself.
- Offloading to the edge is done to achieve aggregation, manipulation, bandwidth reduction, and other data operations directly on an IoT device.

Processing Offloading

Fog

- It is a decentralized computing infrastructure that is utilized to conserve network bandwidth, reduce latencies, restrict the amount of data unnecessarily flowing through the Internet, and enable rapid mobility support for IoT devices.

- The data, computing, storage, and application are shifted to a place between the data source and the cloud resulting in significantly reduced latencies and network bandwidth usage.

Processing Offloading

Remote server

- A simple server having good processing power.
- It is used with IoT based applications to offload the processing from resource constrained IoT devices.
- Rapid scalability may not handled by it.
- It is costlier and hard to maintain in comparison to cloud.

Processing Offloading

Cloud

- It is a configurable computer system which can get access to configurable resources, platforms, and high level services through a shared pool hosted remotely.
- A cloud is provisioned for processing offloading so that processing resources can be rapidly provisioned with minimal effort over the Internet, which can be accessed globally.
- It enables massive scalability of solutions as they can enable resource enhancement allocated to a user or solution in an on-demand manner
- No need to the user to go through the pains of acquiring and configuring new and costly hardware.

Processing Offloading

Offload decision making

- The choice of where to offload the processing, to and by how much to offload.
- It is addressed by considering data generation rate, network bandwidth, criticality of the application, processing resources available at the offload site.
- The approaches are
  - ✓Naive Approach
  - ✓Bargaining based approach
  - ✓Learning based approach

Processing Offloading

Naive Approach

- It is a hard approach.
- It is a rule based approach in which data from IoT devices are offloaded to the nearest location based on certain offload criteria.
- Easy to implement.
- It is not recommended approach for densely deployed network, deployment where data generation rate is high, or multimedia and hybrid data generating applications.
- Statistical measures are used for generating rules of offload decision making.

Processing Offloading

Bargaining based approach

- It is processing intensive approach during decision making stage.
- It enables alleviation of network traffic congestion, enhances QoS parameters such as bandwidth, latencies.
- It tries to maximize the QoS.
- Example: Game theory
- It does not depends on historical data for decision making purposes.

Processing Offloading

Learning based Approach

- It relies on past behavior and trends of data flow through the IoT architecture.
- Learning from historical trends and trying to optimize previous solution and enhance the collective behavior of IoT implementation.
- Memory and processing requirement is high during decision making stages.
- Example: Machine learning

Processing Offloading

Offloading Consideration

- Deciding when to offload.
- Parameters required to choose a offloading type depends on nature of IoT application and hardware being used to interact with the application.
- Various parameters include
  - ✓ Bandwidth
  - ✓ Latency
  - ✓ Criticality
  - ✓ Resources
  - ✓ Data volume

Processing Offloading

Bandwidth

- The maximum amount of data that can be simultaneously transmitted over the network between two points.
- Data carrying capacity of a wired or wireless network.
- It is used to describe the data rate of a network.

Processing Offloading

Latency

- Time delay incurred between the start and completion of an operation.
- It occurs due to network or processor.
- It occurs due to physical limitations of infrastructure which is associated with operation.
- The operation can be data transfer over a network or processing of data at a processor.

Processing Offloading

Criticality

- It defines importance of task being pursued by an IoT application.
- More critical task requires less latency.
- Example : More critical task : Fire detection (Response time in milliseconds)
  Less critical task : Agriculture field parameter (Response time in hours or days)

Processing Offloading

Resources

- Actual capabilities of an offload location.
- It includes processing power, the suite of analytical algorithms.
- Example: It is futile and wasteful to allocate processing resources reserved for real-time multimedia processing (which are highly energy intensive and can process and analyze huge volumes of data in a short duration) to scalar data(which can be addressed using nominal resources without wasting much energy)

Processing Offloading

Data volume

- The amount of data generated by a source or sources that can be simultaneously handled by the offload location.

- For large and dense IoT deployments, the offload location should be robust enough to address the processing issues related to massive data volumes.

THANK YOU

IoT connectivity Technologies Part-2

NFC

NFC

Introduction

- Abbreviation of NFC is Near field communication.
- It was developed jointly by Philips and Sony.
- It was a short range wireless connectivity standard.
- It enables peer-to-peer (P2P) data exchange over the network.
- Communication between NFC devices are achieved by the principle of magnetic induction, whenever the devices are brought close to one another.

NFC

Introduction

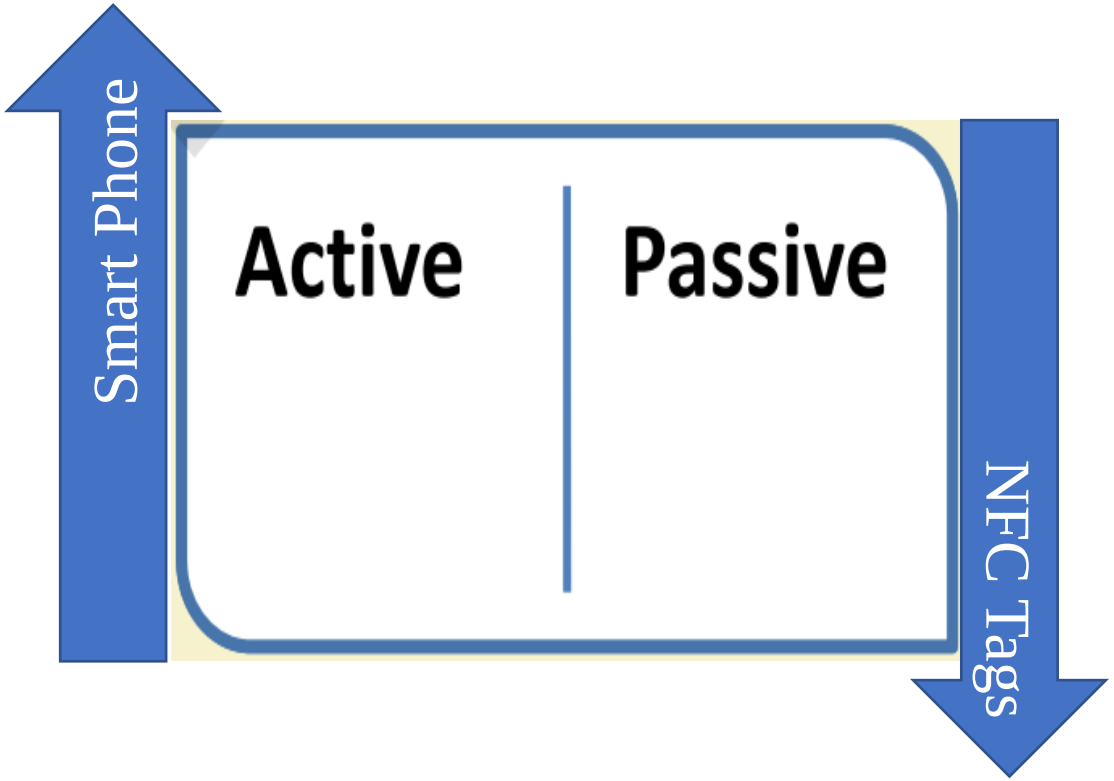
- It can also be used with other wireless technologies such as Wi-Fi after establishing and configuring the P2P network.
- The communication between compatible devices requires a pair of transmitting and receiving devices.
- The operating frequency for data is 13.56MHz.
- Data rate is 106, 212, or 424 kbps.

NFC

NFC devices are categorized into two types.

- Active NFC (Need Power Source)
- Passive NFC

(Do not require any power source)



NFC

NFC Device Types

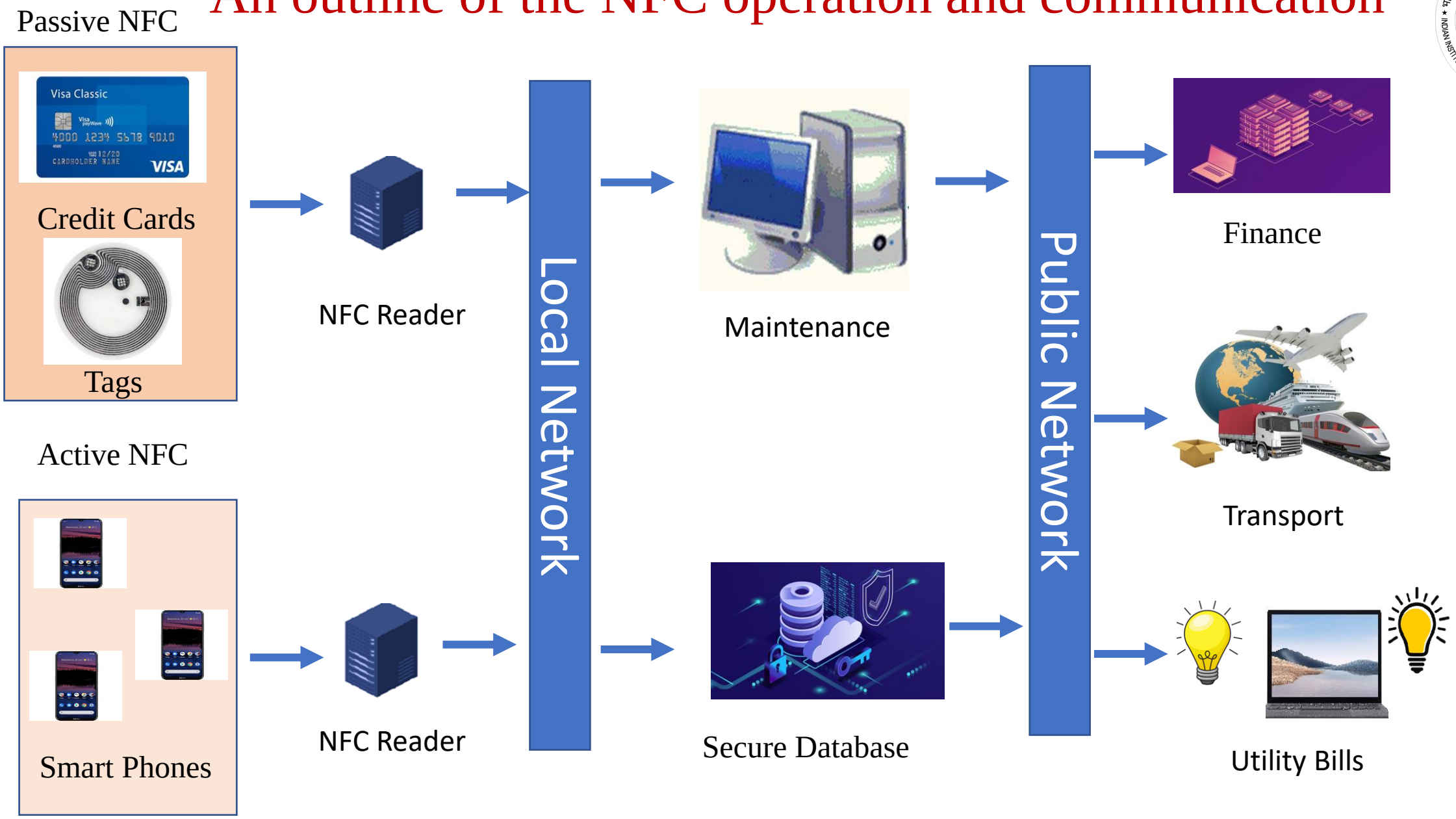
- **Passive devices** contain information which is readable by other devices, however it cannot read information itself.
- It does not need power source for communicating with the NFC reader.
- NFC tags found in supermarket products are examples of passive NFC.
- Passive devices cannot process information.
- They store information which is read by NFC reader

NFC

NFC Device Types

- **Active devices** are able to collect as well as transmit information.
- It can communicate with active as well as passive NFC devices.
- This devices are capable of reading as well as writing data to other NFC terminals.
- Smartphones are a good example of active devices.
- Other examples are public transport card reader, commercial touch payment terminals.

An outline of the NFC operation and communication

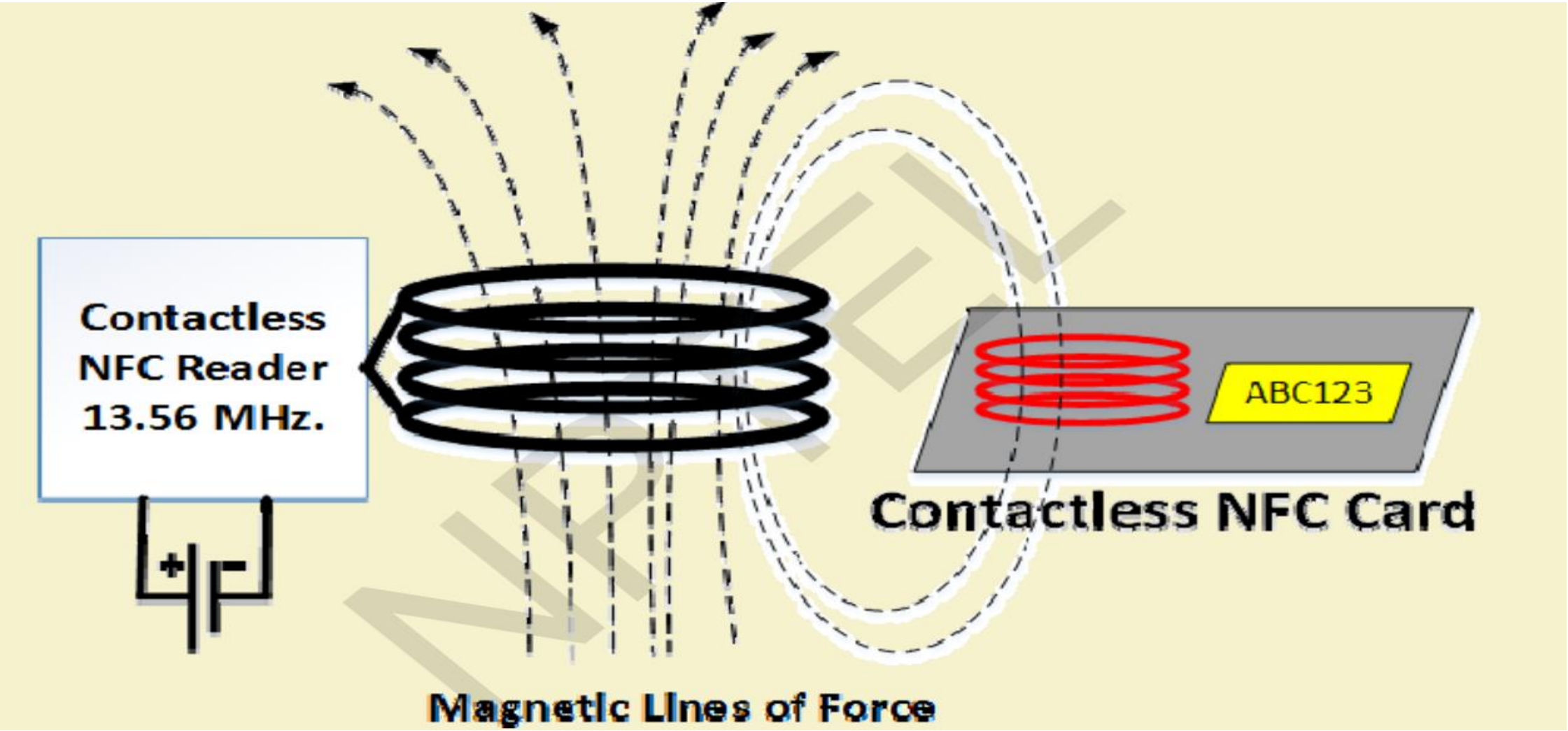


NFC

Working Principle

- Works on the principle of **magnetic induction**.
- A NFC reader emits a small electric current which creates a magnetic field that in turn acts as a bridge in the physical space between two NFC devices.
- The generated EM(electro magnetic) field is received by a similar coil in the client device where it is turned back into electrical impulses to communicate data such as identification number, status information, messages, currency or any other information.
- NFC communication and pairing are speedy due to the use of inductive coupling and the absence of manual pairing.
- ‘Passive’ NFC tags use the energy from the reader to encode their response while ‘active’ or ‘peer-to-peer’ tags have their own power.

NFC


Contactless
NFC Reader
13.56 MHz.
ABC123
Contactless NFC Card
Magnetic Lines of Force

NFC

NFC Specifications

- NFC's data-transmission frequency is 13.56MHz.
- NFC can transmit data at a rate of either 106, 212 or 424 Kbps (kilobits per second).
- Tags typically store between 96 and 512 bytes of data.
- Communication range is less than 20cms.

NFC

Modes of Operation

Peer-to-peer → Lets two smartphones swap data

Read/Write → One active device picks up info from a passive one

Card emulation → NFC device can be used like a contactless credit card

NFC

Peer-to-Peer

- It is used in NFC modes.
- It enables two NFC devices to exchange information.
- Transmitting device goes active while the receiving device becomes passive.
- During reverse transmission, both devices changes their roles.

NFC

Read/Write Mode

- Information exchange allows only one-way data transmission.
- An active NFC device connects to a passive device to read information from it.

Card Emulation mode

- It enables an NFC device to act as a contactless credit card and make payments using just a simple tap on an NFC reader.

NFC

NFC Applications

- Smartphone based payments.
- Parcel tracking.
- Information tags in posters and advertisements.
- Computer game synchronized toys.
- Low-power home automation systems.

DASH7

DASH7

Introduction

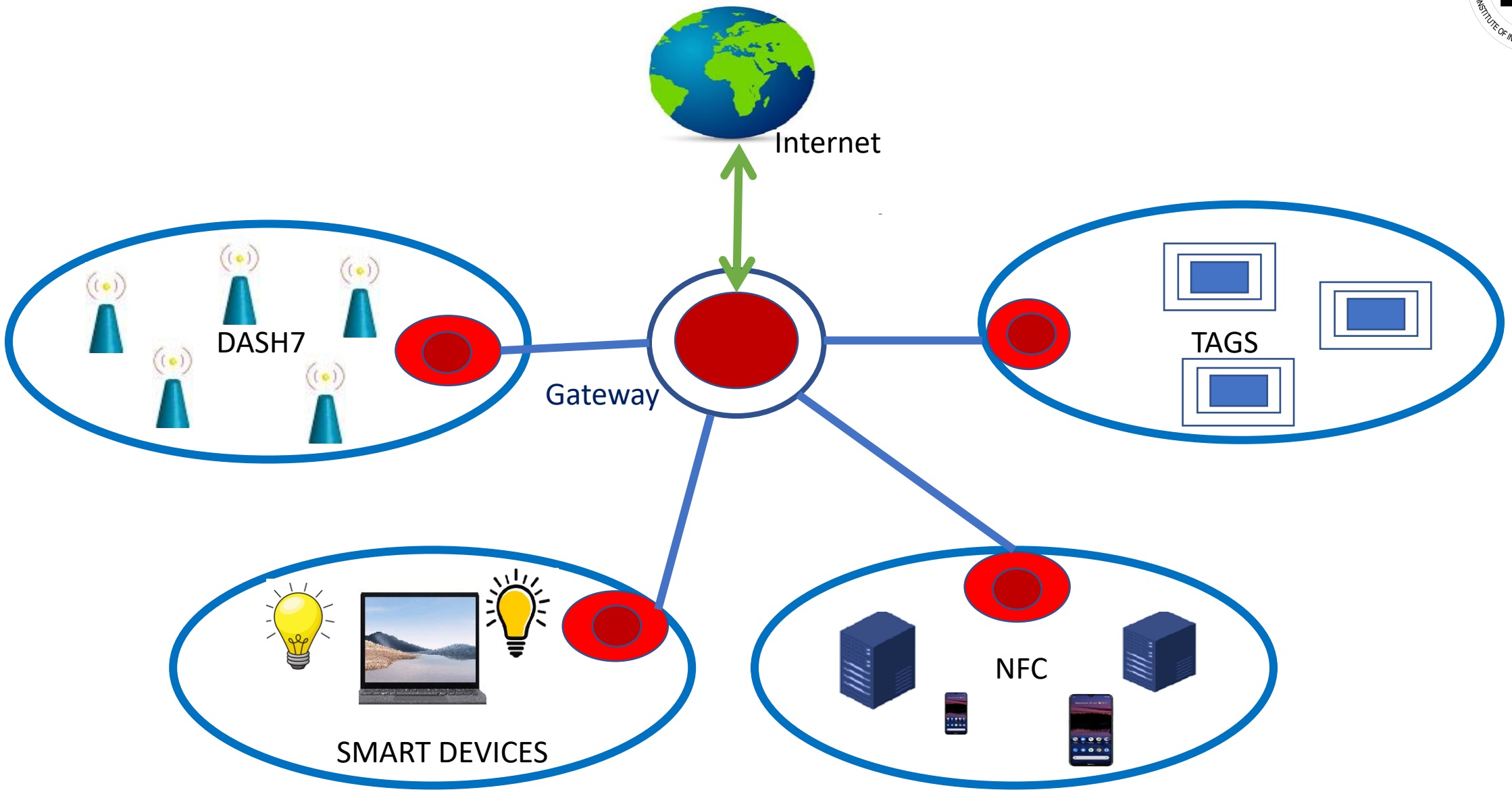
- It is based on an active RFID standard.
- It operates on 433MHz frequency band.
- Frequency shift keying (FSK) is used for modulating messages transmission over the channel.
- It uses 433.92 MHz operational band to enable communication with NFC devices.

DASH7

Application

- Agriculture
- Vehicles
- Mobiles
- Consumer electronics related applications

The DASH7 Communication Architecture



The DASH7 Protocol stack in comparison to the OSI Stack

	OSI Stack	Dash Stack
Host Layer	Application Layer	Application Layer
	Presentation Layer	Presentation Layer
	Session Layer	Session Layer
	Transport Layer	Transport Layer
Media Layer	Network Layer	Network Layer Services
		Network
	Data Link Layer	Logical Link Control
		Media access Control
	Physical Layer	Physical Layer

DASH7

- Dash7 protocol has a fully defined and complete OSI stack.
- Physical layer is made adaptable with Lora or Sigfox.
- It supports cheap processing systems by virtue of its integrated file system.
- DASH7 Gateways can query devices in proximity to it without waiting for predefined time-slots to listen to its end device beacons.

DASH7

Features

- It supports very dense deployments.
- It has low memory footprints.
- It acts as a bridge between NFC and IoT communication system.
- It enables tag to tag communication without needing the tags to pass their messages through a base station or a tag reader.

DASH7

Features

- It is synonymous with the multi node hopping mesh network in ZigBee and Z-wave.
- Transmission range is between 1 to 10km.
- Latency is 1 to 10 seconds.

Z-Wave

Z-Wave

Introduction

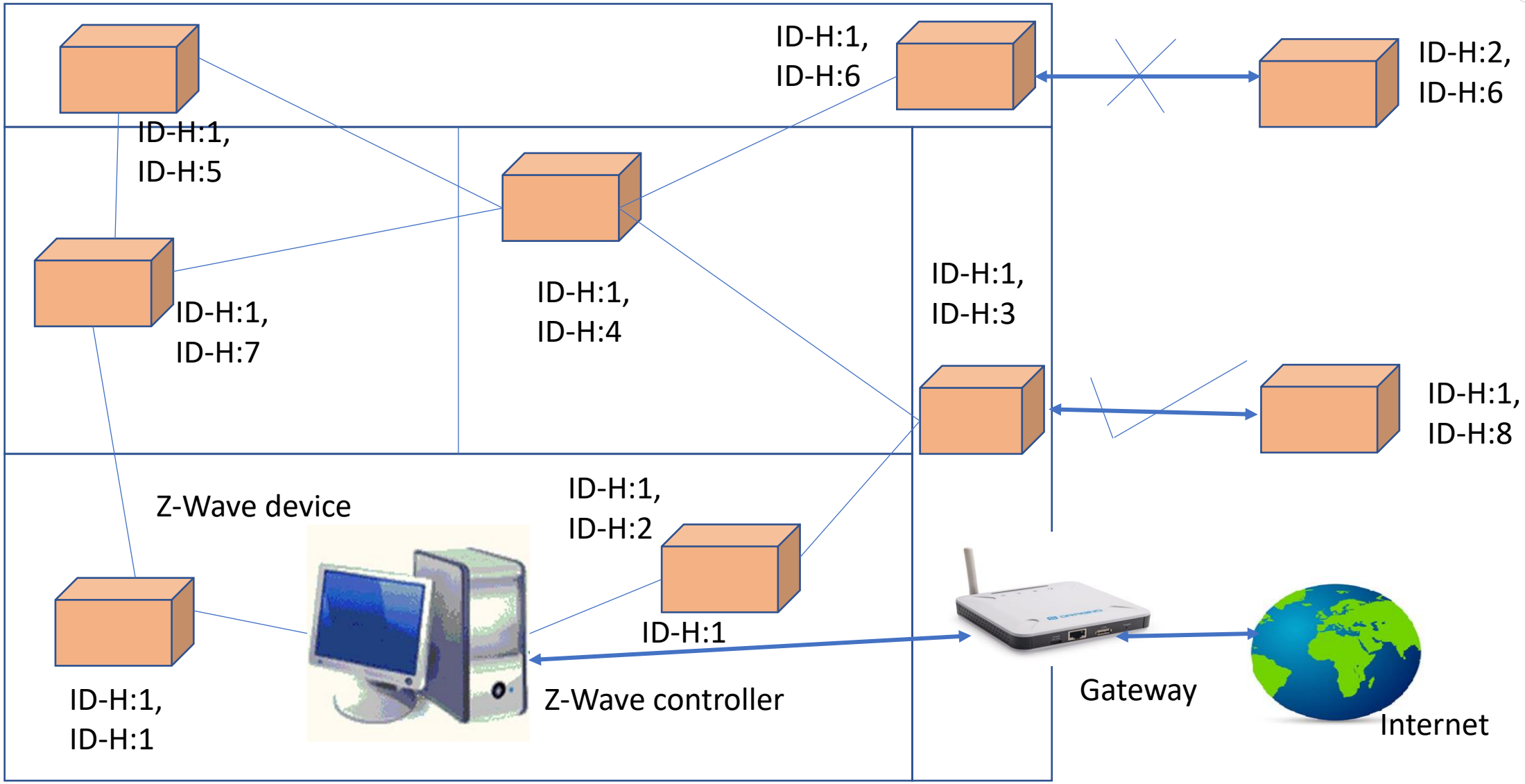
- It is an economical and less complicated alternative to Zigbee.
- It was developed by Zensys for home automation solutions.
- Power consumption is lower than Wi-Fi.
- Transmission Range is greater than Bluetooth.
- Z-Wave integrated sensors are present in locks, home power distribution system, appliances, and heating system.

Z-Wave

Z-Wave Specification

- Operational frequency range is 800-900MHz.
- Gaussian frequency shift keying (GFSK) Modulation scheme is used.
- Manchester channel encoding is used for preparing the data for transmission over the channel.
- Each Z-Wave network ID is 4Bytes long, and the node ID length is 1Bytes long.

Z-Wave Deployment and Communication Architecture



Z-Wave

Components of a Z-Wave Network

- Z-Wave node
- Z-Wave controller
- Gateway
- Internet

Z-Wave

Z-Wave Network

- Z-Wave controller is a central network controller device which set up and manages the Z-Wave network.
- Each network have a logical ID.
- Each logical ID contains a home network ID and multiple node IDs for the devices present within it.
- Z-wave nodes with different home IDs can not communicated with each other.
- The central hub is connected to Internet through Gateway.

Z-Wave

Z-Wave Network

- One central hub is present in a home.
- A home can contain multiple devices which can communicate with central hub through Z-wave.
- The device can not connect to the Internet directly.
- A hub can contain maximum 232 devices.
- It uses a source routed static network.
- Mobile devices are excluded from the network.

Z-Wave

Z-Wave Network

- Z-Wave devices are connected to the home based routers and access points.
- Z-Wave routers or access points are responsible for forwarding Z-Wave messages to a central hub.
- Z-Wave devices can communicate directly with central hub if it is within its range.
- Z-Wave routing strictly follow a source routed mesh network topology.

Z-Wave

Message Healing

- When Z-Wave devices are not in the range of central Z-Wave hub, the messages are routed through different nodes to bypass obstructions created by household appliances or layouts.
- This process of avoiding radio dead spots is done using a message.
- This message is called message healing.

The Z-Wave Protocol Stack

Application

Security

Transport

Network

Physical

Weightless

Weightless

Introduction

- It is a low-power wide area network.
- It is useful for low power, low throughput, moderate to high latency applications supporting either or both public or private networks.
- Operating frequency is sub GHz bands.
- Weightless has *three* standards.
  - ✓ Weightless P
  - ✓ Weightless N
  - ✓ Weightless W

Weightless

- Weightless P supports bidirectional communication over both licensed and unlicensed ISM bands.

- Weightless N is a LWPAN uplink only technology.

- Weightless W is designed to make use of the TV whitespace frequencies for communications.

Weightless

Features

- Weightless P is most adopted and accepted standard among three standards.
- Weightless P is also known as Weightless Protocol.
- It provides bidirectional and reliable communications.
- Each message transaction is validated using an acknowledgement frame.
- It is used for densely deployed low complexity IoT end devices.

Weightless

Features

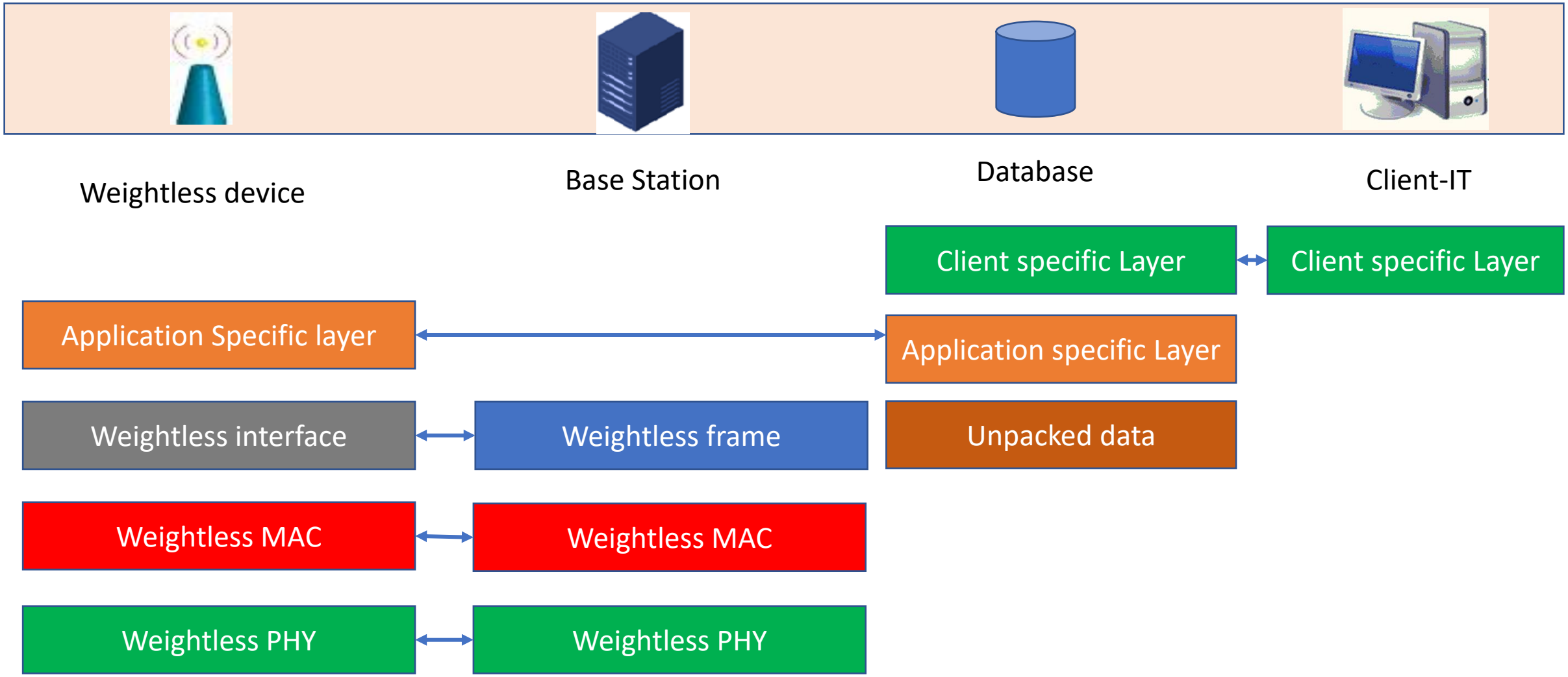
- Payload size is less than 48 bytes.
- It has ultra low power consumption status compared to cellular network.
- Data rate is 0.625 kbps to 100kbps.
- Network cost and latency is very low compared to cellular network.

Weightless

Architecture

- It has three components.
  - ✓ End Device
  - ✓ Base station
  - ✓ Base station network

Typical components of the Weightless standard and its protocols



Weightless

End Device

- These are the leaf nodes of the network.
- Low complexity and low cost devices.
- Duty cycle is very low.
- Transmitting power is 14 dBm to 30 dBm.

Weightless

Base station

Central co-ordinating node in each cell.

Star topology is used to connect the end devices to the base station.

Transmitting power is 27 dBm to 30 dBm.

Weightless

Base station network

- It connects all base station to the single network.
- It manages the allocation and scheduling of radio sources across the network.
- The task includes address authentication, roaming, scheduling responsibilities.

Sigfox

Sigfox

Introduction

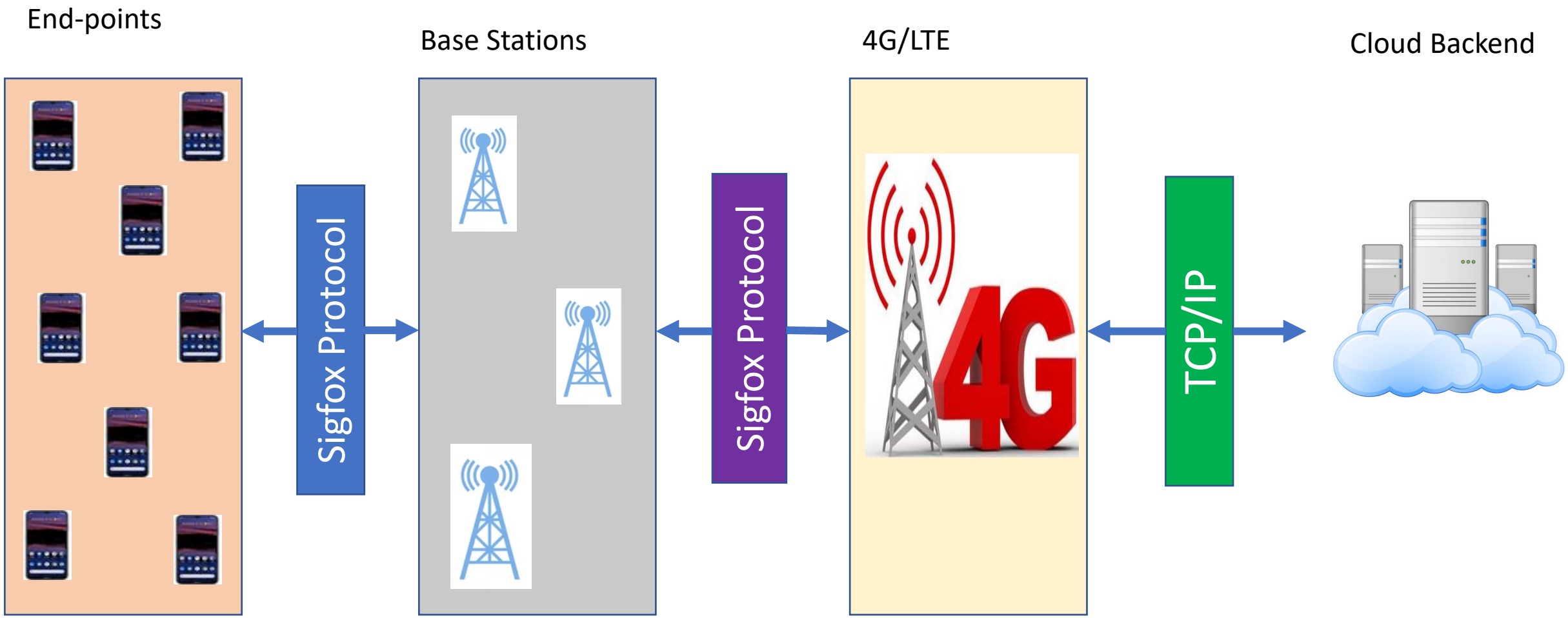
- It is a low power connectivity solution.
- It is used in
  - ✓ Home automation and security system(Within a building)
  - ✓ Smart metering
  - ✓ Agriculture
- It uses ultra narrow band technology (192kHz) for accessing and communicating through the radio spectrum.
- Data rate is 100-600 bps.
- BPSK is used for encoding

Sigfox

Introduction

- In Europe, Sigfox uses 868 and 868.2 MHz spectrum.
- In other countries, it uses 902 and 928MHz spectrum.
- It less prone to noise as receiver has to access only a very tiny part of the spectrum for receiving messages.
- This standard is resilient as it can communicate in presence of jamming signals.
- It supports random access message forwarding principle which ensures high quality of services.

The Sigfox Communication architecture



The Sigfox Communication Architecture

Sigfox end devices

- Sigfox end device uses time frequency diversity method to transmit and receive the messages.

- Time frequency diversity method

  Each Sigfox device emits a message at an arbitrary frequency and simultaneously send two replies of the same message at different frequency.

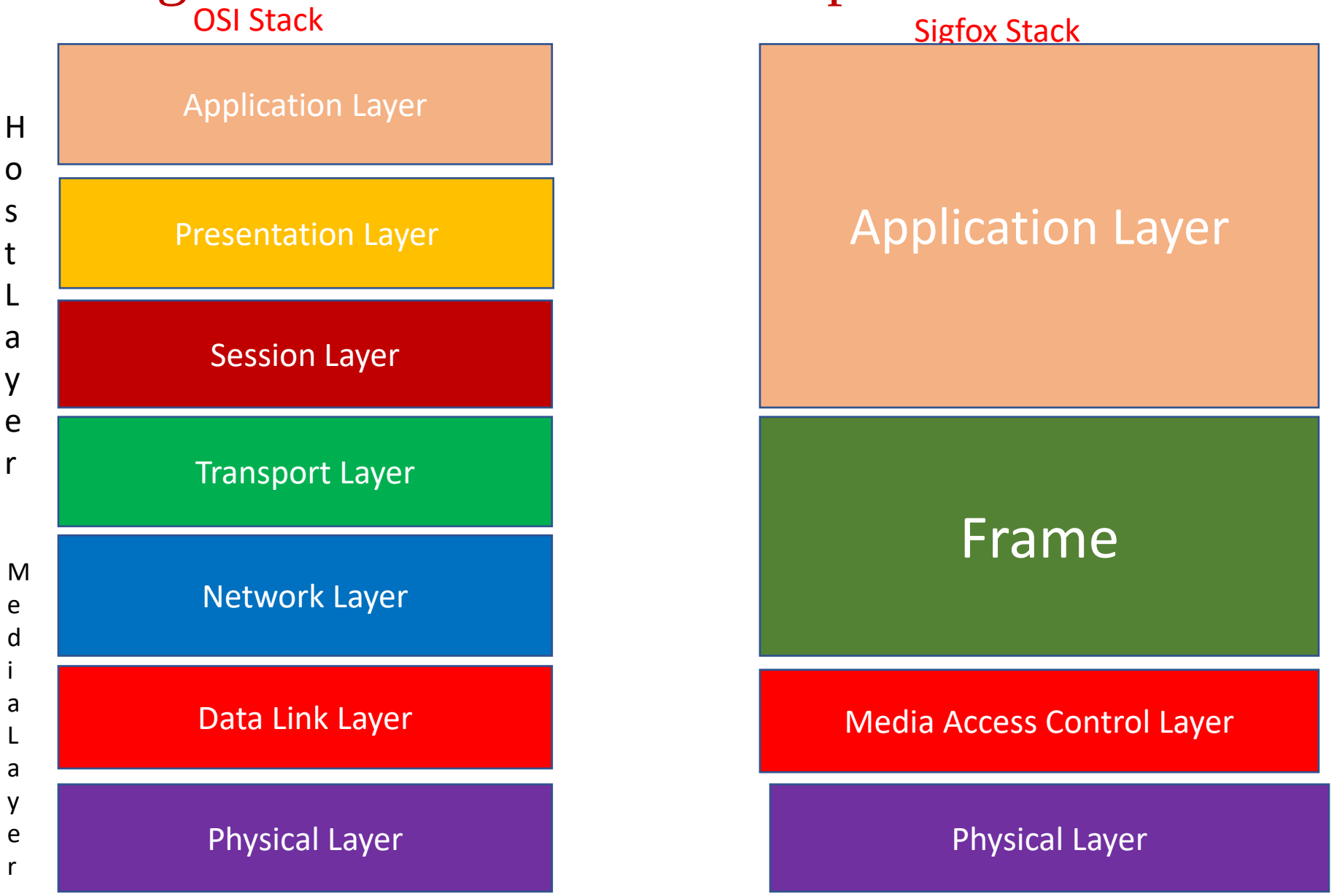
- Sigfox end devices are less complicated.

Sigfox

Sigfox Base Station

- It uses cooperative reception principle.
- Sigfox end devices uses the principle of spatial diversity to send the messages to Sigfox base station.
- principle of spatial diversity
  The messages are not attached to any base station and any base station in the vicinity of the device can receive the messages from it.
- It provides excellent quality of services as it uses the principle of time, frequency, spatial diversity.
- The base stations are more complicated than end devices as it monitor whole 192kHz spectrum looking for UNB(Ultra narrow band) transmissions for demodulation.

Sigfox Protocol stack in comparison to the OSI Stack



Sigfox

- The communication is bi-directional and asynchronous.
- Message length (payload) of this protocol is 0 to 12 bytes.
- Payload includes simultaneous transfer of sensor data, status of event/alert, GPS co-Ordinator, and application data.
- AES is used for security purpose.
- It supports authentication, integrity, anti-reply on message transmission through the network.

Sigfox

- It is a low-power and resilient standard.
- It is widely used in the application requiring infrequent communication with small bursts of data.
- It supports both dense and wide node deployment applications.
- It is more suitable for indoor applications.
- Mobility is not supported by this protocol.

LoRa

LoRa

Introduction

- LoRa or Long Range
- Developed by Grenoble, France.
- It supports cellular type communications aimed to provide connectivity to M2M and IoT solutions.
- It uses 169MHz, 433MHz, 868MHz, 915MHz frequency bands.

LoRa

Introduction

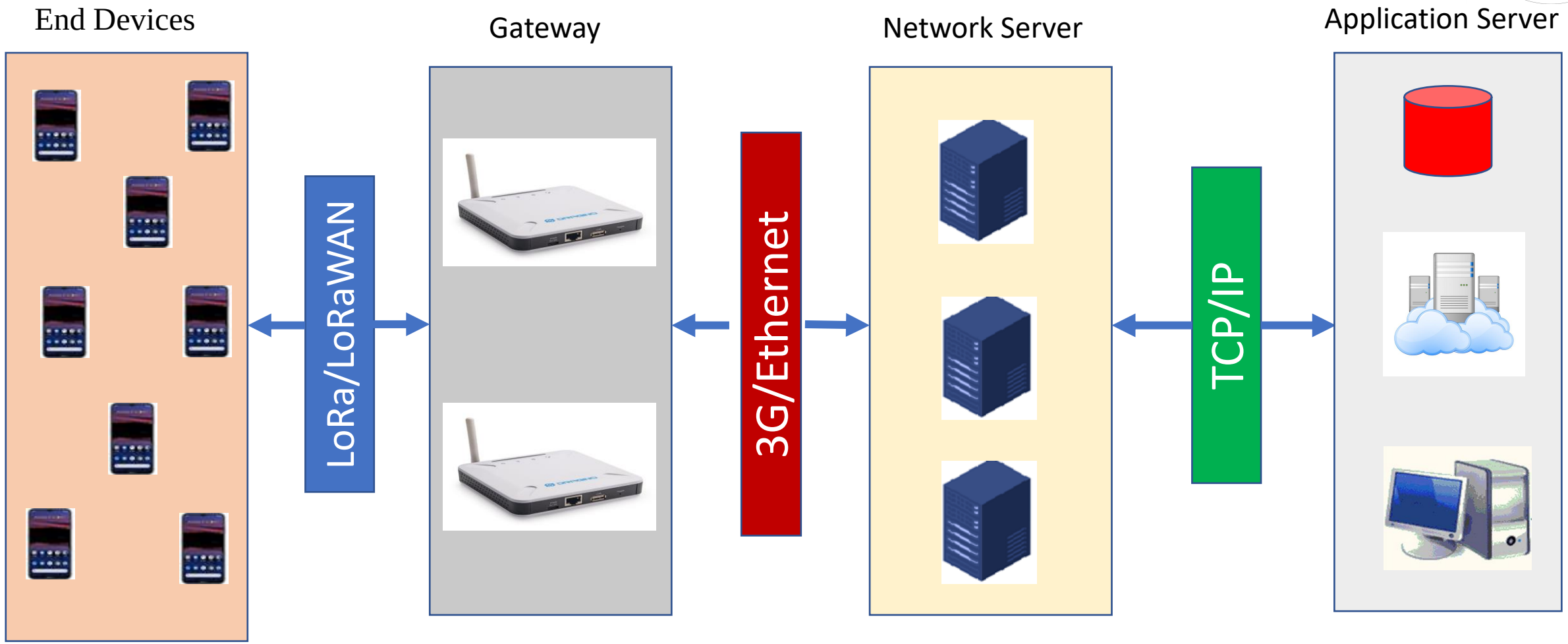
- Bidirectional communication links symmetrically and a spread spectrum with 125 kHz wideband for operating.
- Widely used for electric grid monitoring application.
- Transmission range is from 15Km to 20 Km.
- Supports millions of Devices.

LoRa

Specifications

- It is a spread spectrum technology with a boarder band (125kHz).
- It achieves high receiver sensitivity by utilizing frequency modulation chirp coding gain.
- It supports mobility of the end devices.
- Widely used in asset tracking and asset management applications.
- Higher battery life.
- Low data rates (27 to 50 kbps).
- Longer latency times.
- Supports both wired and wireless communications.

LoRa Deployment and communication architecture



LoRa Network Architecture

LoRa network follows *four* entities.

- End points/nodes
- Gateways
- Network Server
- A remote computer

LoRa Entities

- The end devices deals with all sensing and control solutions.
- The gateways forwards messages from end nodes to a backhaul network.
- The gateways are connected to the network server by using IP addresses.
- Network server is responsible for scheduling message acknowledgements, modifying data rates, removing message redundancies.
- Remote computers have control over the end devices and act as data sinks for data originating from these nodes.

LoRaWAN

- The network formed by LoRa devices are called LoRaWAN.
- Routing of messages between end devices and destination node is done through LoRaWAN Gateway.
- LoRaWAN has a boarder spectrum which results Interference, can be solved by coding gain of chirp signals.
- LoRaWAN end devices and base stations are inexpensive.
- It uses WAN communication and is an architecture that makes use of LoRa.
- Messages transmitted over LoRaWAN is received by all base stations in proximity to the device, which makes message redundancy in the network.
- The resilience of the network is enhanced by ensuring more messages are successfully delivered between entities in the network.

LoRa Protocol Stack

Application Layer

MAC

PHY

RF

Security in LoRa

- Unique *network key* is used to provide security in network layer.
- Unique *application key* ensures end to end security in application layer.
- Unique *device specific key* ensures security at device level

NB-IOT

NB-IOT

Introduction

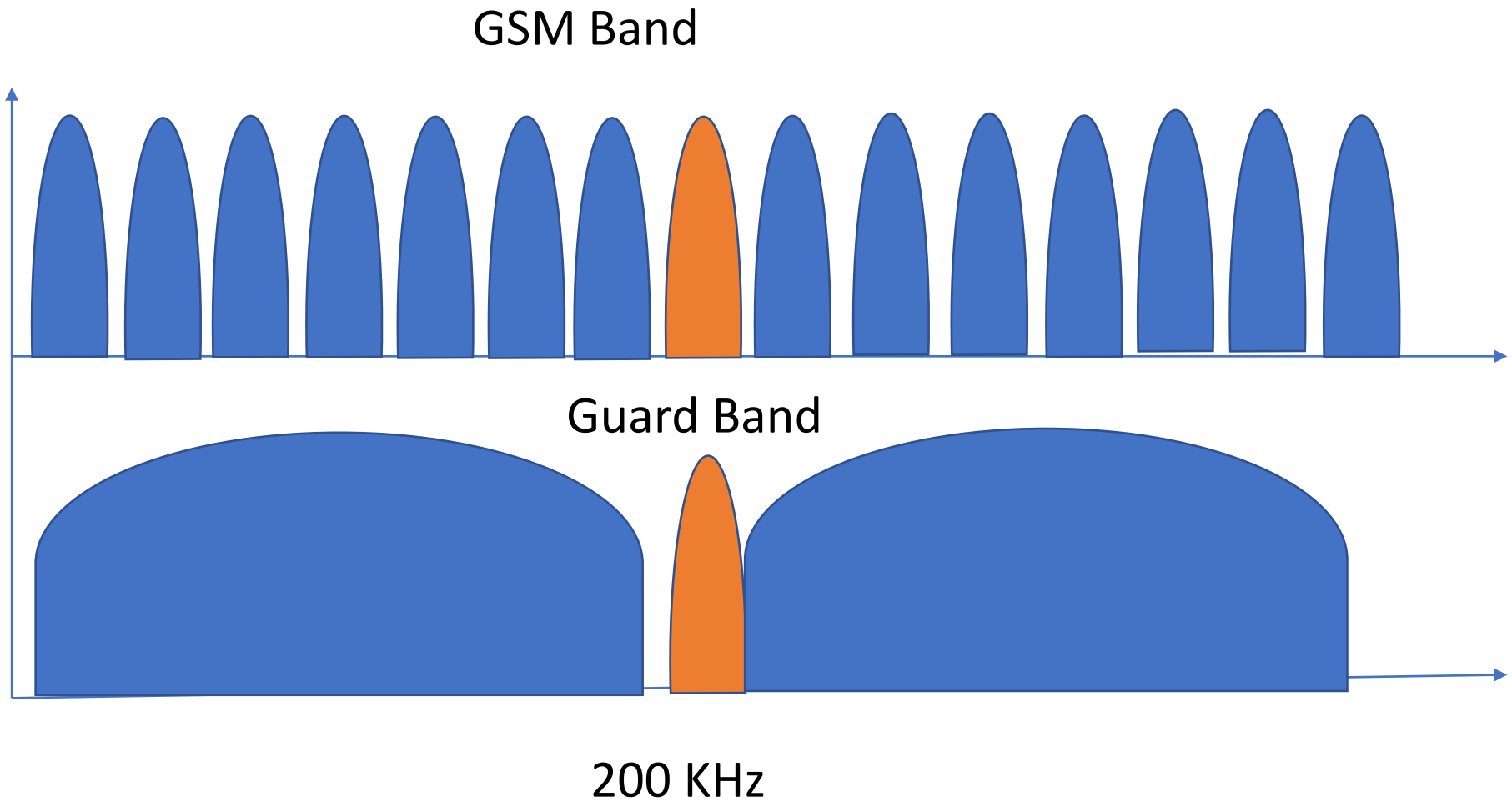
- Narrow Band Internet of Things
- It is an initiative of Third Generation Partnership Project (3GPP) to develop cellular standard.
- It coexists with cellular system.
- It consumes minimum power.
- Battery Life is up to 10 years.

NB-IOT

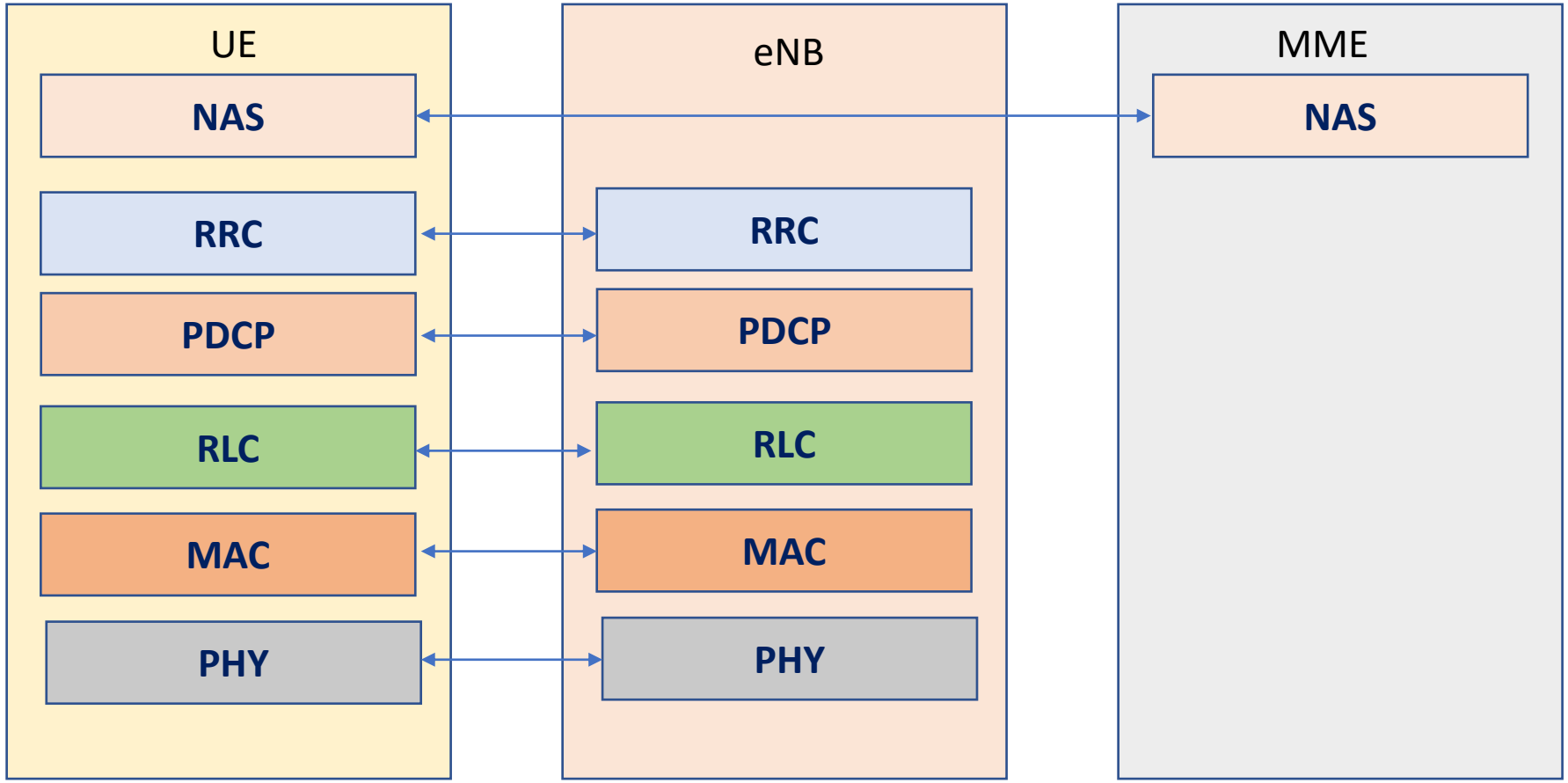
Introduction

- It improves the reliability, spectrum efficiencies, and system capability.
- It uses orthogonal frequency division multiplexing (OFDM) which enhances the system capacity and increase spectrum efficiency.
- Device complexity is quite high.
- It provides support for security, confidentiality, authentication, integrity.

A location of NB-IOT band within the LTE spectrum



The NB-IOT protocol stack with respect to its entities



PDCP - packet data convergence protocol
RRC - radio resource control
RLC – radio link control
NAS– Non access stratum

eNB - e node B
MME – Mobility Management Entity

NB-IOT

- The coverage of NB-IoT supports deployments in indoor environments as well as in dense urban areas.
- It provides high quality of services as well as reduced latencies.
- It can not transfer large amount of messages.
- It supports static network.
- It uses 200 kHz GSM band.
- It can transfer tens to hundred bytes of data per device daily.

Wi-Fi

Wi-Fi

Introduction

- Its base protocol is IEEE 802.11.
- It is a wireless technology for wireless local area networking of devices.
- It uses 2.4GHz ultra high frequency band or 5.8 GHz super high frequency ISM radio bands.
- It uses time sharing based TDMA multiplexing.
- It uses CSMA/CA for channel access.
- Popular versions of IEEE 802.11 is a/b/g/n.

Wi-Fi

IEEE 802.11a

- Data Rate-54 Mbps
- Bandwidth-5GHz

OFDM modulation scheme for communication.

IEEE 802.11g

- Data Rate-54 Mbps
- Bandwidth-2.4GHz

OFDM modulation scheme for communication.

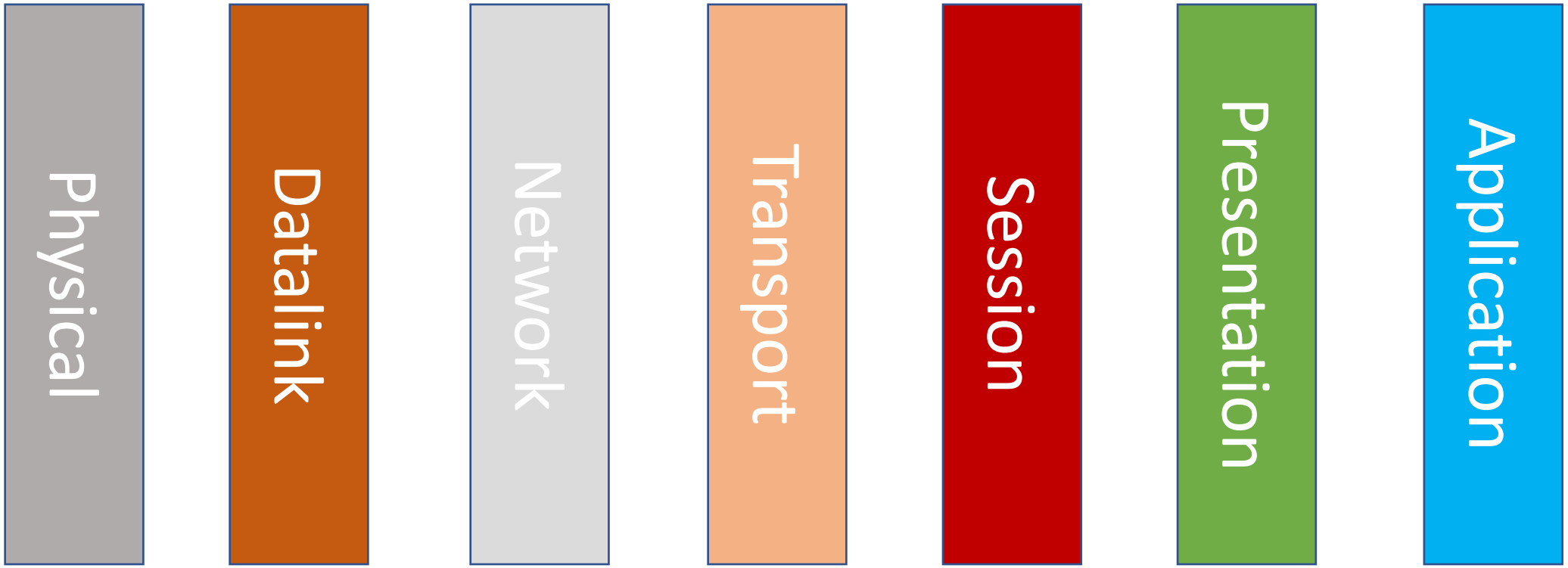
IEEE 802.11b

- Data Rate-11 Mbps
- Bandwidth-2.4 GHz
- OFDM modulation scheme for communication.

IEEE 802.11b

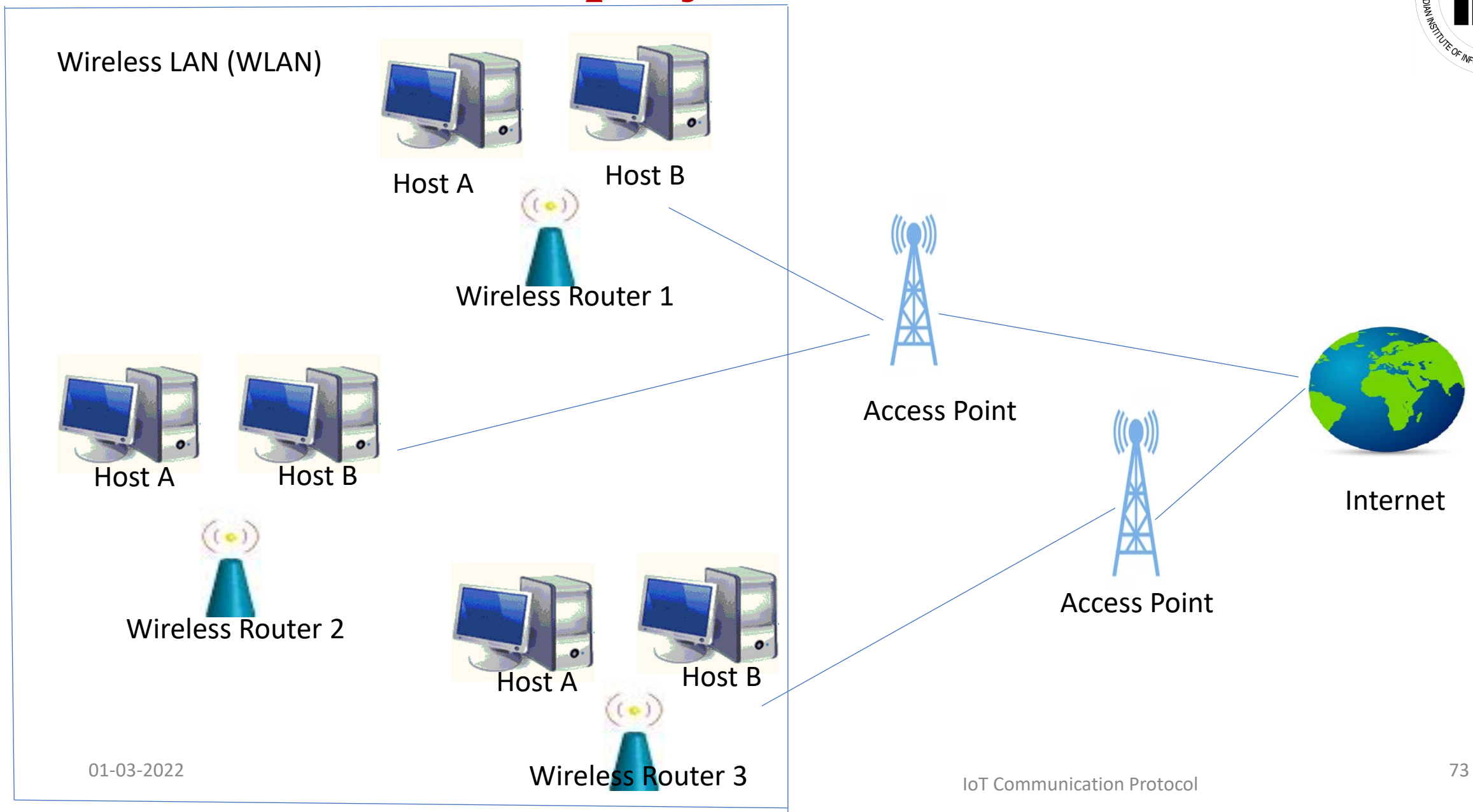
- Data Rate-140 Mbps
- Bandwidth-5 GHz
- OFDM modulation scheme for communication.

The IEEE 802.11 Wi-Fi Stack



IEEE 802.11

Wi-Fi Deployment Architecture



Bluetooth

Bluetooth

Introduction

- It is defined by IEEE 802.15.1 standard.
- It is a short range wireless communication technology operating at low power to enable communication among two or more Bluetooth enabled devices.
- Intended for replacing cables connecting portable units (Smartphones, Laptops).
- It allows the transmission of data and voice over short distances.
- Maintains high levels of security.
- Bluetooth technology is based on **Ad-hoc technology** also known as **Ad-hoc Piconets.**

Bluetooth

Features

- Bluetooth technology operates in the unlicensed industrial, scientific and medical (ISM) band at 2.4 to 2.485 GHZ.
- Uses spread spectrum hopping, full-duplex signal at a nominal rate of 1600 hops/sec.
- Bluetooth supports 1Mbps data rate for version 1.2 and 3Mbps data rate for Version 2.0 combined with Error Data Rate.
- Transmission range is approximately 10m.
- The transmission of data is done through FHSS, which reduces interference caused by other devices.

Bluetooth

Features

- The data is divided into packets before transmitted by Bluetooth.
- The packets are transmitted over 79 designated channels, each 1MHZwide in 2.4 GHz band.
- Adaptive frequency hopping enable this standard to perform 800 hops per second over these channels.
- Initial version-GFSK(Gaussian frequency shift keying) modulation having data rate 1 Mbps.
- Next version-$\pi/4$ DQPSK(Differential Quadrature Phase Shift Keying) modulation with data rate 2 Mbps.
- Next version-8-DPSK(Differential Phase Shift Keying) modulation with data rate 3 Mbps.

Bluetooth

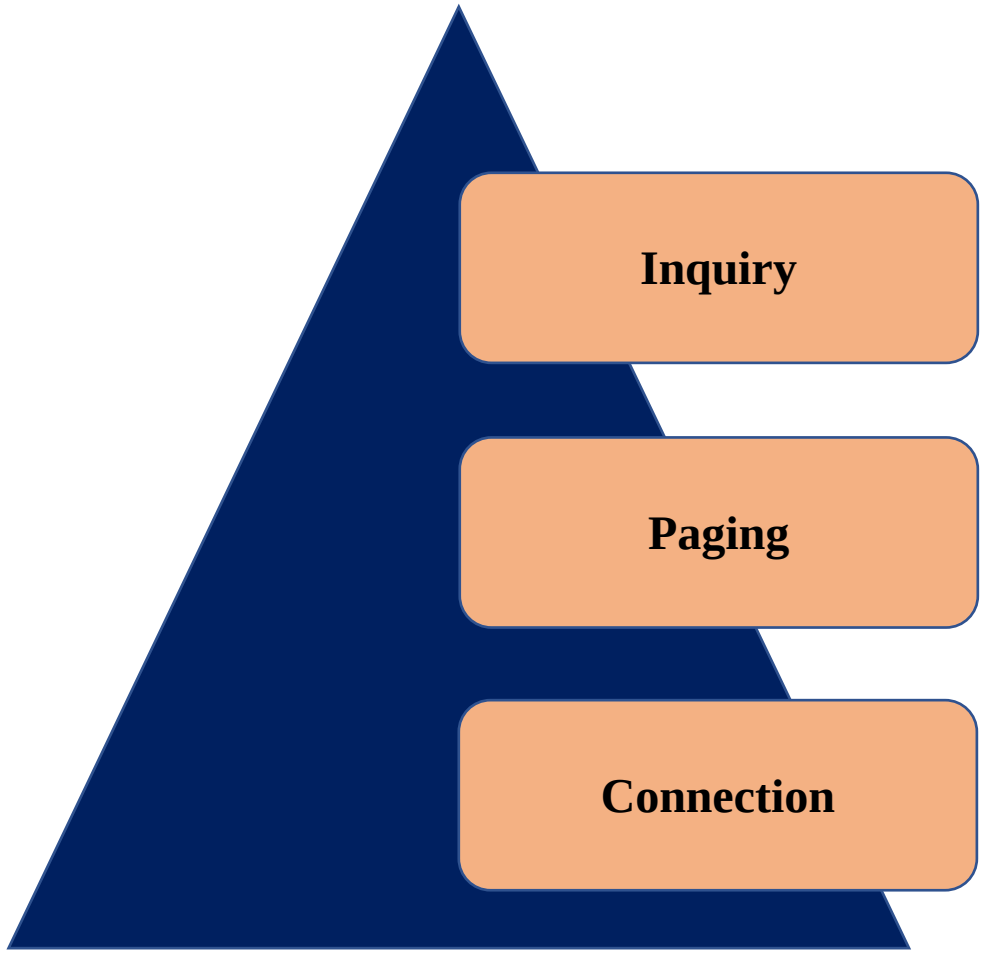
Features

Bluetooth operating range depends on the device:

- **Class 3** radios have a range of up to 1 meter or 3 feet.
- **Class 2** radios are most commonly found in mobile devices have a range of 10 meters or 30 feet.
- **Class 1** radios are used primarily in industrial use cases have a range of 100 meters or 300 feet.

Bluetooth

Connection Establishment



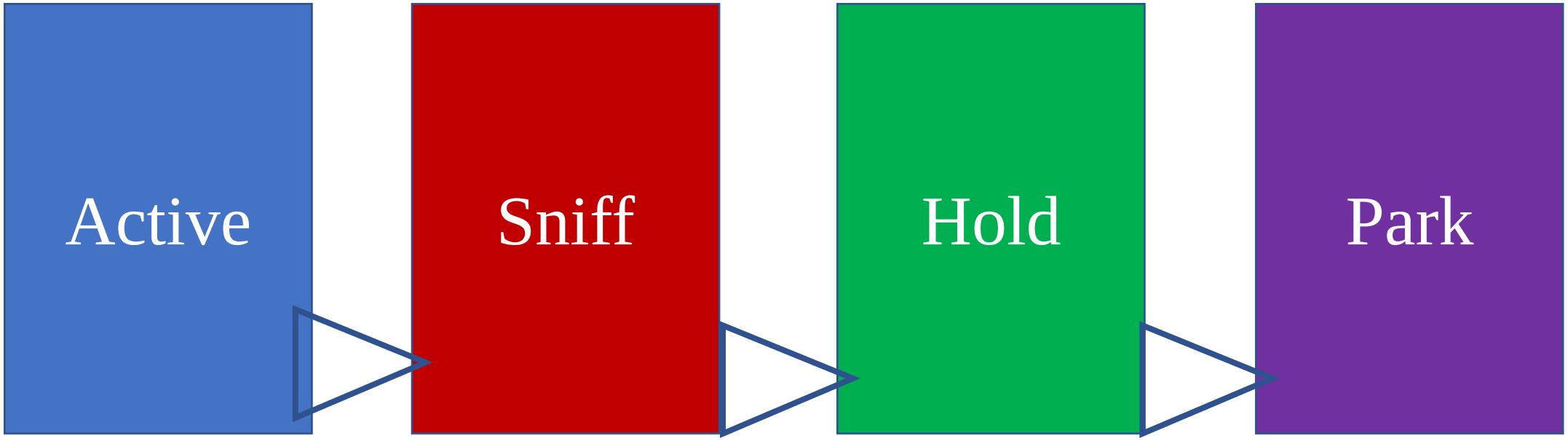
Inquiry run by one Bluetooth device to try to **discover other devices near it.**

Process of **forming a connection** between two Bluetooth devices.

A device either actively **participates** in the network or enters a low-power sleep mode.

Bluetooth

Modes



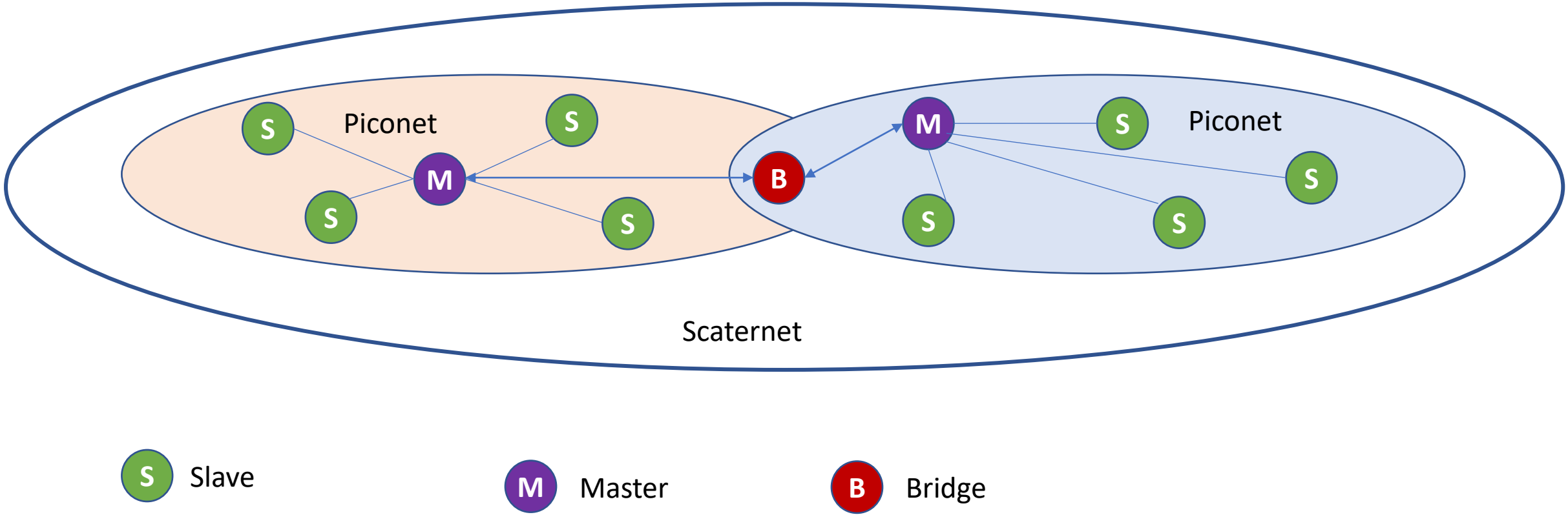
Actively transmitting or receiving data.

Sleeps and only listens for transmissions at a set interval .

Power-saving mode where a device sleeps for a defined period and then returns back to active mode .

Slave will become inactive until the master tells it to wake back up.

The Bluetooth device network Architecture



Bluetooth

Piconets

- Bluetooth enabled electronic devices connect and communicate wirelessly through short range networks known as **Piconets**.
- Bluetooth devices exist in small ad-hoc configurations with the ability to act either as master or slave.
- Provisions are in place, which allow for a **master** and a **slave** to switch their roles.
- The simplest configuration is a point to point configuration with one master and one slave.

Bluetooth

- When more than two Bluetooth devices communicate with one another, it is called a **PICONET**.
- A Piconet can contain up to *seven slaves* clustered around a single master.
- The device that initializes establishment of the Piconet becomes the **master**.
- The master is responsible for transmission control by dividing the network into a series of time slots amongst the network members, as a part of **time division multiplexing** scheme.

Bluetooth

Features of Piconet

- Within a Piconet, the clock and unique **48-bit address** of master determines the timing of various devices and the frequency hopping sequence of individual devices.
- Each Piconet device supports 7 simultaneous connections to other devices.
- Each device can communicate with several piconets simultaneously.
- Piconets are established dynamically and automatically as Bluetooth enabled devices enter and leave piconets.

Bluetooth

Features of Piconet

- There is no direct connection between the slaves.
- All connections are either master-to-slave or slave-to-master.
- Slaves are allowed to transmit once these have been polled by the master.
- Transmission starts in the slave-to-master time slot immediately following a polling packet from the master.
- A device can be a member of two or more Piconets.

Bluetooth

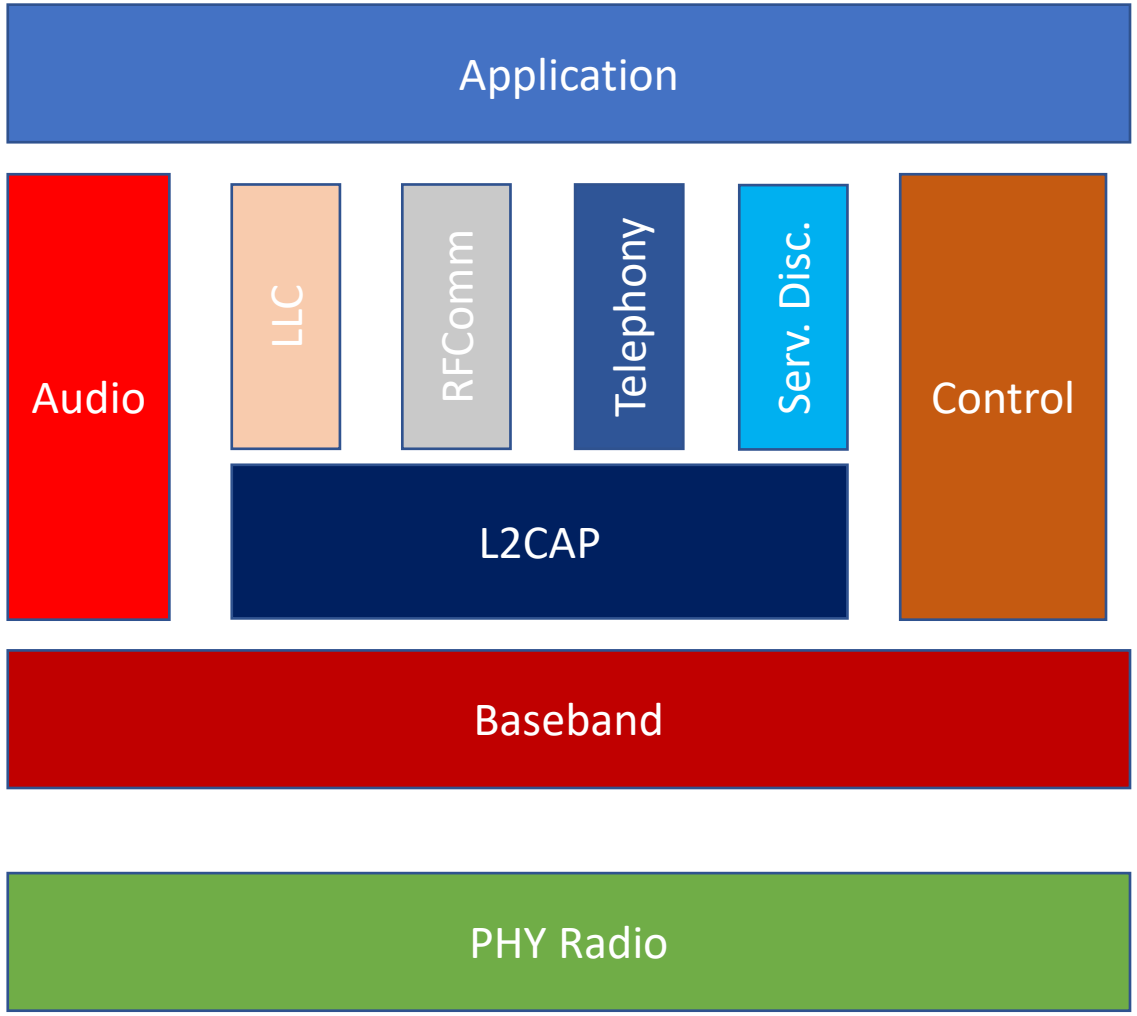
Features of Piconet

- A device can be a slave in one Piconet and master in another. It however cannot be a master in more than once Piconets.

- Devices in adjacent Piconets provide a bridge to support inner-Piconet connections, allowing assemblies of linked Piconets to form a physically extensible communication infrastructure known as **Scatternet**.

The Bluetooth Protocol Stack

Bluetooth Stack



The Bluetooth Protocol Stack

Bluetooth standard consist of *four* parts.

1. Core Protocol
2. Cable replacement protocol
3. Telephony control protocol
4. Adapted protocol
5. Link Manager Protocol (LMP), Logical Link Control and Adaptation Protocol ((L2CAP) , Host Controller Interface (HCI), Radio Frequency Communication (RFCOMM), and Service Discovery Protocol (SDP) protocols are associated with Bluetooth.

The Bluetooth Protocol Stack

Baseband

- Physical layer of the Bluetooth.
- Manages physical channels and links.
- Other services include:
  - ✓ Error correction
  - ✓ Data whitening
  - ✓ Hop selection
  - ✓ Bluetooth security
  - ✓ Manages asynchronous and synchronous links.
  - ✓ Handles packets, paging and inquiry.

The Bluetooth Protocol Stack

Link Manager Protocol (LMP)

- It manages the establishment, authentication, and link configuration.

- LMPs consists of some protocol data units (PDUs) between which transmission occurs for availing services such as name request, link address request, connection establishment, connection authentication, mode negotiation, and data transfer.

The Bluetooth Protocol Stack

Host Controller Interface

- It enables access to hardware status and control registers and connects the controller with the link manager.

- The automatic discovery of Bluetooth devices in its proximity is one of the essential tasks of HCL.

The Bluetooth Protocol Stack

L2CAP

- The Logical Link Control and Adaptation Protocol (L2CAP).
- Layered over the Baseband Protocol and resides in the data link layer.
- Used to multiplex multiple logical connections between two devices.
- Provides connection-oriented and connectionless data services to upper layer protocols.
- Provides:
  - ✓ Protocol multiplexing capability
  - ✓ Segmentation and reassembly operation
  - ✓ Group abstractions

The Bluetooth Protocol Stack

Service Discovery Protocol (SDP)

- Enables applications to discover available services and their features.
- Addresses the unique characteristics of the Bluetooth environment such as, dynamic changes in the quality of services in RF proximity of devices in motion.
- Can function over a reliable packet transfer protocol.
- Uses a request/response model.

The Bluetooth Protocol Stack

RFComm

- Radio Frequency Communications (RFCOMM).
- It is a cable replacement protocol used for generating a virtual serial data stream.
- RFCOMM provides for binary data transport.
- Emulates EIA-232 (formerly RS-232) control signals over the Bluetooth baseband layer, i.e. it is a serial port emulation.
- RFCOMM provides a simple reliable data stream to the user, similar to TCP.
- Supports up to 60 simultaneous connections between two BT devices.

The Bluetooth Protocol Stack

Telephony Control Protocol – Binary (TCS BIN)

- It is a bit oriented protocol to control call signaling prior to initiation of voice or data communication between devices.

Bluetooth

Applications

- Audio players
- Home automation
- Smartphones
- Toys
- Hands free headphones
- Sensor networks

Problem - 1

Let there be a task of 480 TB from a host machine that needs to be processed in the cloud. The service provider has three data centers(DC) namely DC1, DC2, DC3 which are capable of processing tasks. The capacity of different data centers are given in the following table.

Parameters	DC1	DC2	DC3
Available Storage(TB)	1043	560	1095
Processing Speed(Gbps)	875	950	865
Distance from the host(Km)	380	101	356

To which of the DCs do you think it best to allocate the task? Justify your answer.

Problem-2

The power required to transmit a bit in Zigbee is 180 μW/bit. An implementation has 200 Zigbee slave nodes (where each node is attached to four sensors), each of which periodically transmits data to the master node at interval of 120 seconds. The packet from each node consist of a 64 bit node identifier and a 64 bit destination identifier, 8 bit sensor values and 8 bit sensor identifier from each sensor. How much power will be consumed by the implementation (except the master node) for 1 hour of operation.

Problem-3

Thread is based on IEEE802.15.4 2006 specifications. It transmits 127 byte packets with data rate of 250kbps over the 2.4GHz band. Out of the 127 bytes, the payload occupies a maximum of 63 bytes. A thread router alternatively transmits sensor value of 9 bytes and 40 bytes per second to the boarder router. Considering ideal transmission and full throughput, what is the total volume of data transmitted through this thread network in an hour.

THANK YOU

Problem-1

Let there be a task of 480 TB from a host machine that needs to be processed in the cloud. The service provider has three data centers (DC) namely DC1, DC2, DC3 which are capable of processing tasks. The capacity of different data centers is given in the following table.

Parameters	DC1	DC2	DC3
Available Storage (TB)	1043	560	1095
Processing Speed (Gbps)	875	950	865
Distance from the host (Km)	380	101	356

To which of the DCs do you think it best to allocate the task? Justify your answer.

Problem - 1

A task came from host machine need to be processed in cloud - 480 TB

Service provider have three data centers

	Available storage (TB)	Processing speed (Gbps)	Dist. from host (Km)
DC_1	1043	875	380
DC_2	560	950	101
DC_3	1095	865	356

Our task size is 480 TB

Out of three DC, our task can be stored in any one of the DC.

If we store it in DC_2, then less memory will wasted.

As processing speed of DC_2 is high, then processing latency reduces.

As distance from host is less in DC_2 then network latency is less if we choose DC_2. By considering all the above three factors, assigning task to DC_2 is suitable.

Problem-2

The power required to transmit a bit in Zigbee is 180 µW/bit. An implementation has 200 Zigbee slave nodes (where each node is attached to four sensors), each of which periodically transmits data to the master node at interval of 120 seconds. The packet from each node consist of a 64 bit node identifier and a 64 bit destination identifier, 8 bit sensor values and 8 bit sensor identifier from each sensor. How much power will be consumed by the implementation (except the master node) for 1 hour of operation.

Problem-2

The power required to transmit a bit – 180 µW/bit

Total number of Zigbee nodes – 200

Each Zigbee node have sensors – 4

Slave sends data to master in interval of – 120 seconds

We need to calculate data transmission in 1 hour.

So, number of transmission required –

$$\frac{\cancel{3600}^{30}\ \text{seconds}}{\cancel{120}} = 30 \text{ times}$$

Each slave node sends its data to master 30 times in 1 hour.

Packet =

64 bit source identifier	64 bit destination identifier	8 bit sensor value	8 bit sensor identifier

Total packet size is $= 64 + 64 + 8 + 8$

$= 128 + 16 = 144$ bit packet length.

Power required by one node – $180 \times 10^{-6} \frac{W}{bit} \times 144\ bit \times 30$

Power required by 200 node –

$$200 \times 180 \times 144 \times 30 \times 10^{-6}\ W$$

$$= 15552 \times 10^{4} \times 10^{-6}\ W$$

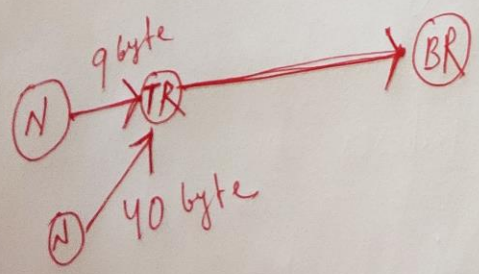
$$= 155.52\ W$$

Problem-3

Thread is based on IEEE802.15.4 2006 specifications. It transmits 127 byte packets with data rate of 250kbps over the 2.4GHz band. Out of the 127 bytes, the payload occupies a maximum of 63 bytes. A thread router alternatively transmits sensor value of 9 bytes and 40 bytes per second to the boarder router. Considering ideal transmission and full throughput, what is the total volume of data transmitted through this thread network in an hour.

Problem - 3

Thread transmits - 127 byte packet
with data rate - 250 kbps
and band width - 2.4 GHZ
Payload — 63 byte
Header - 127 - 63 = 64 byte.



Total volume of data transmitted from TR to BR is

9 X 30 = 270

40 X 30 = 1200

1470 bytes of data