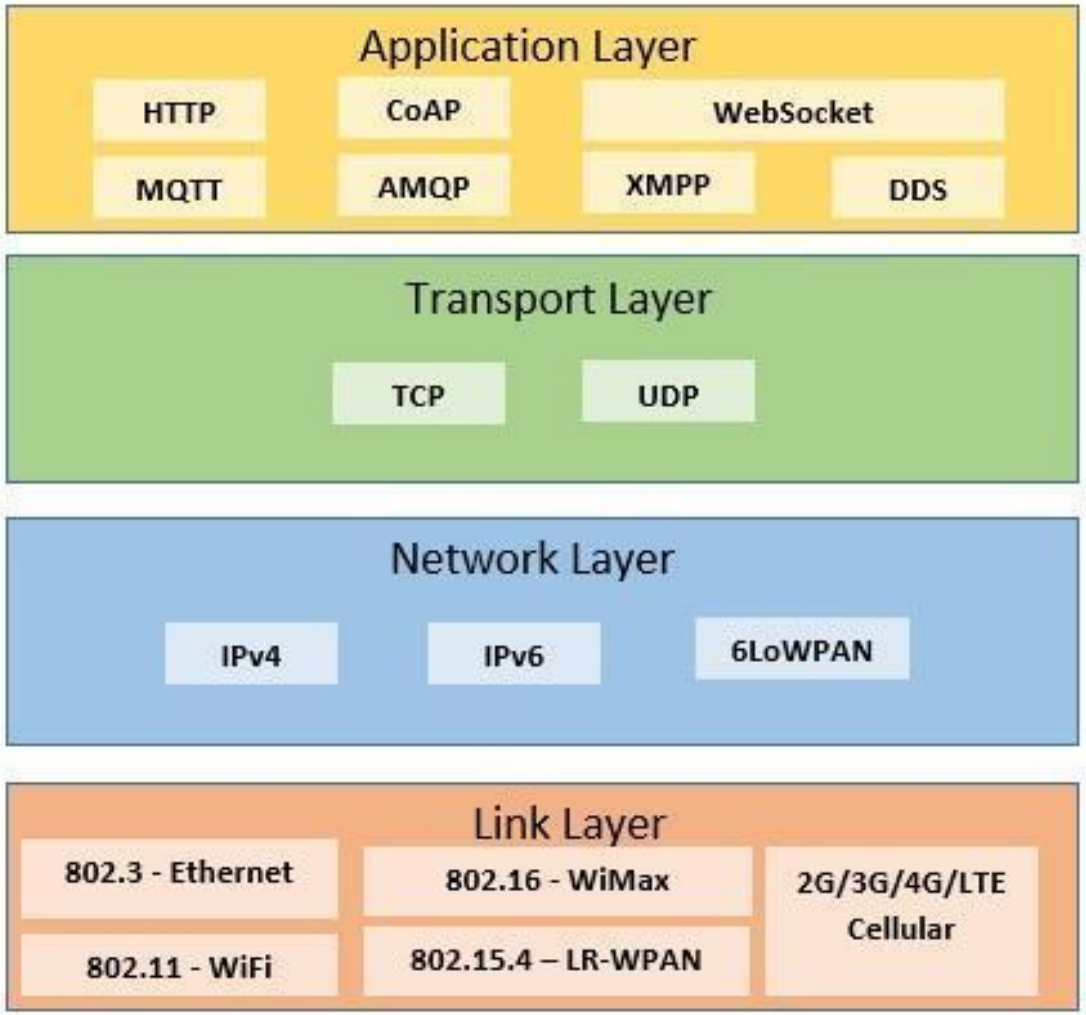
National Forensic Sciences University
Knowledge | Wisdom | Fulfilment
An Institution of National Importance
(Ministry of Home Affairs, Government of India)

Protocol Stack & Connecting Technologies

Dr. Madhavi Dave
Assistant Professor
SCSDF, NFSU Gandhinagar

IoT Protocol Stack



IoT Protocol for Each Layer

Session		MQTT, SMQTT, CoRE, DDS, AMQP , XMPP, CoAP, …	Security	Management
Network	Encapsulation	6LowPAN, 6TiSCH, 6Lo, Thread, …	TCG, Oath 2.0, SMACK, SASL, ISASecure, ace, DTLS, Dice, …	IEEE 1905, IEEE 1451, …
	Routing	RPL, CORPL, CARP, …		
Datalink		WiFi, Bluetooth Low Energy, Z-Wave, ZigBee Smart, DECT/ULE, 3G/LTE, NFC, Weightless, HomePlug GP, 802.11ah, 802.15.4e, G.9959, WirelessHART, DASH7, ANT+, LTE-A, LoRaWAN, …		

IoT Protocol

Application and Session Layer Protocol	MQTT	MQTT is a commonly used light-weight communication protocol for communication among clients and servers.
	SMQTT	A secure MQTT provides encryption for message transfer.
	MQTT-SN	MQTT-SN is an extension of MQTT for sensor networks.
	CoAP	CoAP is a web transfer protocol for constrained networks of IoT.
	DDS	DDS is a data connectivity protocol among IoT nodes and API.
	XMPP	XMPP is a client-server communication protocol using XML elements.
	RESTful/HTTP	RESTful/HTTP is a web connection protocol with state information.
	Websocket	Websocket is a communication protocol for data transmission among multiple nodes.
	SOAP	SOAP is a communication protocol used with HTTP and XML.

IoT Protocol

Transport Layer Protocol	TCP	TCP is a connection-oriented transport protocol with optimal functionality used for MQTT operations.
	UDP	UDP is a web connectionless transport protocol for resource-constrained devices.
Network Layer Protocol	IPv4	IPv4 is used to provide a unique identity to each connected node.
	IPv6	IPv6 is used to provide multiple identities to each connected node.
	6LoWPAN	6LoWPAN is used for the connection of wireless IoT devices.
Data Link Layer Protocol	802.3 – Ethernet	It provides a connection to the stationary IoT devices.
	802.16 – WiMax	802.3 - Ethernet is used for the high-speed data rate wireless connection of IoT devices.
	802.11 –WiFi	802.11 -WiFi provides a wireless LAN connection to IoT nodes.
	802.15.4 -LR-WPAN	802.15.4 -LR-WPAN is used for wireless sensor networks that have IPv6 addresses.
	Wifi	Wifi uses radio frequency to communicate among IoT nodes.

IoT Protocol

Data Link Layer Protocol	Bluetooth Low Energy (BLE)	BLE is used for IoT devices to communicate with other connected nodes.
	ZigBee	ZigBee is a wireless technology for local communication.
	Z-Wave	Z-Wave is a wireless technology for communication in the M2M network.
	WirelessHART	WirelessHART provides synchronization of connected devices of the network using TDMA.
	DASH7	DASH7 provides bi-directional communication for the sensor-actuator network.

IoT Protocol List

- **Connectivity** (6LowPAN, RPL)
- **Identification** (EPC, uCode, IPv6, URIs)
- **Communication / Transport** (WiFi, Bluetooth, LPWAN)
- **Discovery** (Physical Web, mDNS, DNS-SD)
- **Data Protocols** (MQTT, CoAP, AMQP, Websocket, Node)
- **Device Management** (TR-069, OMA-DM)
- **Semantic** (JSON-LD, Web Thing Model)
- **Multi-layer Frameworks** (Alljoyn, IoTivity, Weave, Homekit)

6LoWPAN

- 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 devices to connect to the Internet.
- Created by the Internet Engineering Task Force (IETF) - RFC 5933 and RFC 4919.

Features of 6LoWPAN

- 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 re-formatted to fit the IEEE 802.15.4 packet format.
- Uses include IoT, Smart grid, and M2M applications.

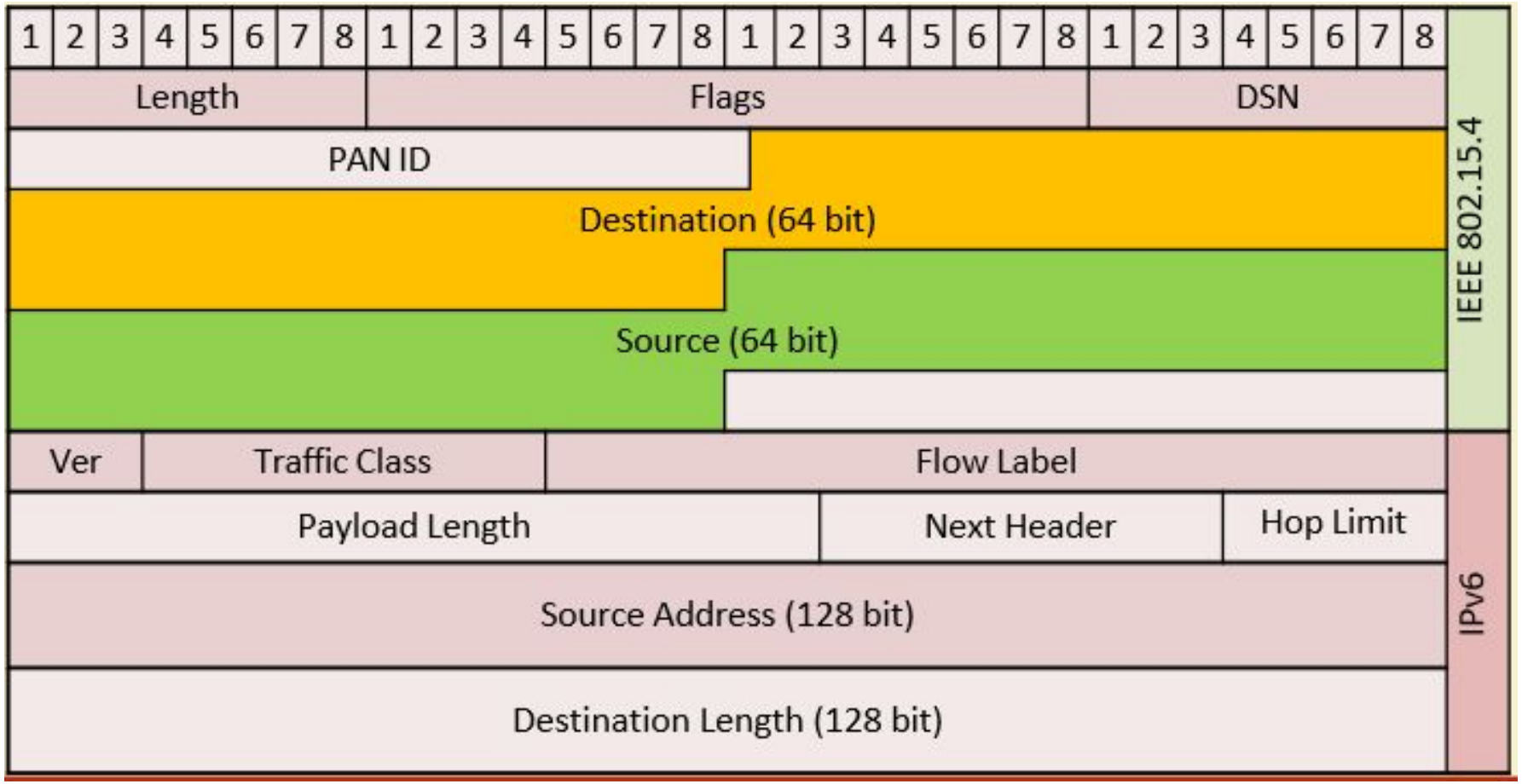
6LoWPAN Routing & Addressing

- Mesh routing within the PAN space.
- Routing between IPv6 and the PAN domain
- Routing protocols in use:
  - LOADng
  - RPL
- Addressing
  - 64-bit addresses: globally unique
  - 16 bit addresses: PAN specific; assigned by PAN coordinator
  - IPv6 multicast not supported by 802.15.4
  - IPv6 packets carried as link layer broadcast frames

6LoWPAN Routing & Addressing

- Mesh routing within the PAN space.
- Routing between IPv6 and the PAN domain
- Routing protocols in use:
  - LOADng
  - RPL
- Addressing
  - 64-bit addresses: globally unique
  - 16 bit addresses: PAN specific; assigned by PAN coordinator
  - IPv6 multicast not supported by 802.15.4
  - IPv6 packets carried as link layer broadcast frames

6LoWPAN Packet Format



RFID

- RFID is an acronym for “radio-frequency identification”
- 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 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.

RFID Applications

- Inventory management
- Asset tracking
- Personnel tracking
- Controlling access to restricted areas
- ID badging
- Supply chain management
- Pharmaceutical industry

MQTT

- **Message Queue Telemetry Transport.**
- ISO standard (ISO/IEC PRF 20922).
- It is a publish-subscribe-based lightweight messaging protocol for use in conjunction with the TCP/IP protocol.
- MQTT was introduced by IBM in 1999 and standardized by OASIS in 2013.
- Designed to provide connectivity (mostly embedded) between applications and middle-wares on one side and networks and communications on the other side.

MQTT (cont..)

- A message broker controls the publish-subscribe messaging pattern.
- A topic to which a client is subscribed is updated in the form of messages and distributed by the message broker.
- Designed for:
  - Remote connections
  - Limited bandwidth
  - Small-code footprint

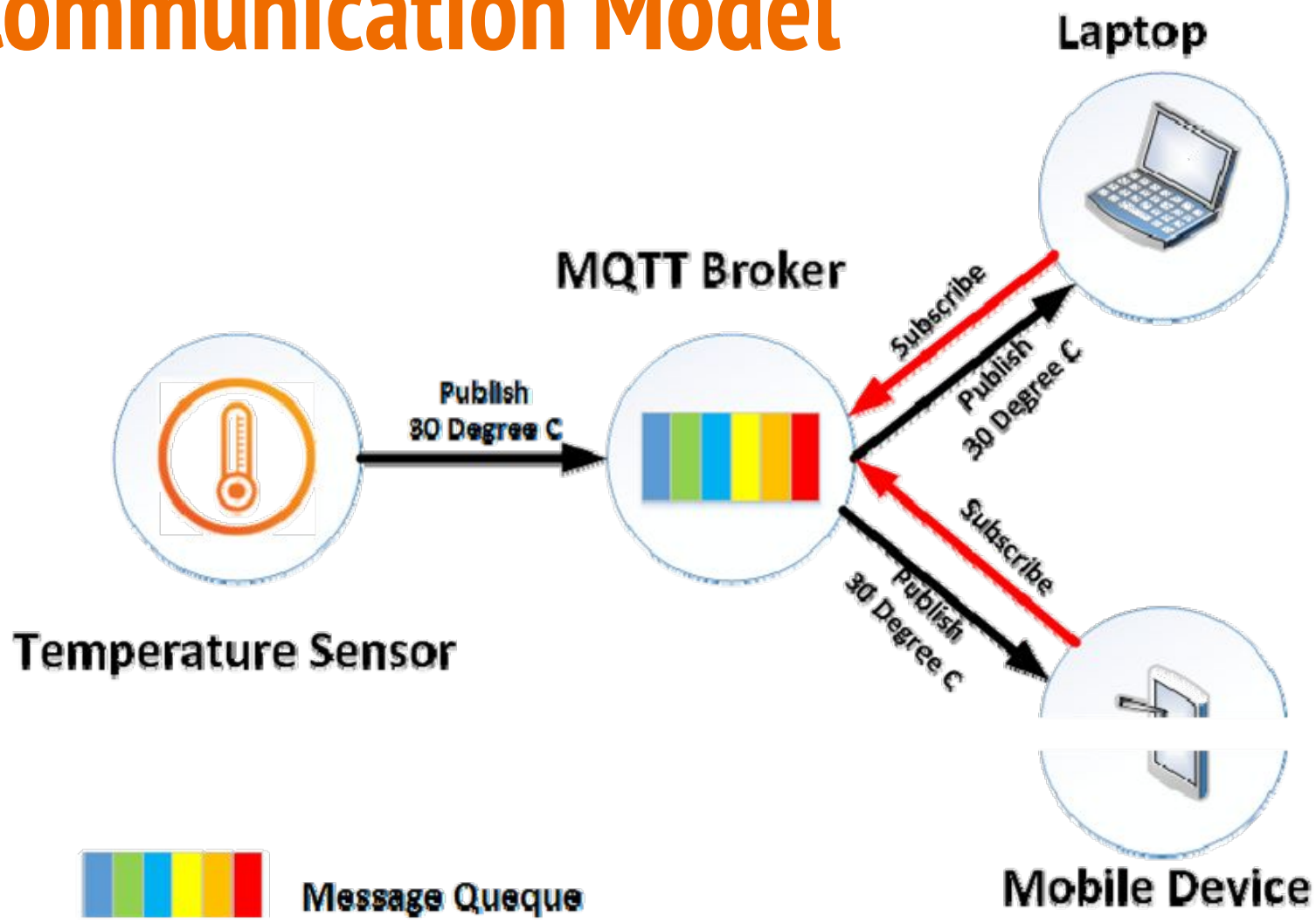
MQTT Components

- Publishers
  - Lightweight sensors
- Subscribers
  - Applications interested in sensor data
- Broker
  - Connect publishers and subscribers
  - Classify sensor data into topics

MQTT Methods

- Connect
- Disconnect
- Subscribe
- Unsubscribe
- Publish

MQTT Communication Model



MQTT Communication

- The protocol uses a **publish/subscribe** architecture (HTTP uses a request/response paradigm).
- Publish/subscribe is **event-driven** and enables messages to be pushed to clients.
- The central **communication point is the MQTT broker**, which is in charge of dispatching all messages between the senders and the rightful receivers.
- Each client that publishes a message to the broker, includes a **topic** into the message. The **topic is the routing information for the broker.**

MQTT Communication (cont..)

- Each client that wants to receive messages subscribes to a certain topic and the broker delivers all messages with the matching topic to the client.
- Therefore the clients don’t have to know each other. They only communicate over the topic.
- This architecture enables highly scalable solutions without dependencies between the data producers and the data consumers.

MQTT Topics

- A topic is a **simple string** that can have more hierarchy levels, which are separated by a slash.
- A sample topic for sending temperature data of the living room could be *house/living-room/temperature*.
- On one hand the client (e.g. mobile device) can subscribe to the exact topic or on the other hand, it can use a **wildcard**.

MQTT (cont..)

- The subscription to *house/+/temperature* would result in all messages sent to the previously mentioned topic *house/livingroom/ temperature,* as well as any topic with an arbitrary value in the place of living room, such as *house/kitchen/temperature*.
- The plus sign is a **single level wild card** and only allows arbitrary values for one hierarchy.
- If more than one level needs to be subscribed, such as, the entire sub-tree, there is also a **multilevel wildcard** (#).
- It allows to subscribe to all underlying hierarchy levels.
- For example *house/#* is subscribing to all topics beginning with *house*.

Applications

- **Facebook Messenger** uses MQTT for online chat.
- **Amazon Web Services** use Amazon IoT with MQTT.
- **Microsoft Azure** IoT Hub uses MQTT as its main protocol for telemetry messages.
- The **EVRYTHNG IoT platform** uses MQTT as an M2M protocol for millions of connected products.
- **Adafruit** launched a free MQTT cloud service for IoT experimenters called Adafruit IO.

SMQTT

- **Secure MQTT** is an extension of MQTT which uses encryption based on lightweight attribute.
- The main advantage of using such encryption is the broadcast encryption feature, in which one message is encrypted and delivered to multiple other nodes, which is quite common in oT applications.
- In general, the algorithm consists of four main stages: setup, encryption, publish and decryption.

SMQTT (cont..)

- In the setup phase, the subscribers and publishers register themselves to the broker and get a master secret key according to their developer's choice of key generation algorithm.
- When the data is published, it is encrypted and published by the broker which sends it to the subscribers, which is finally decrypted at the subscriber end having the same master secret key.
- The key generation and encryption algorithms are not standardized.
- SMQTT is proposed only to enhance MQTT security features.

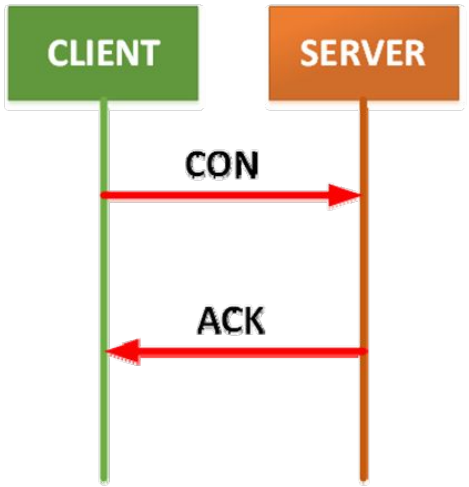
CoAP

- CoAP – **Constrained Application Protocol**.
- **Web transfer protocol** for use with constrained nodes and networks.
- **Designed for Machine to Machine** (M2M) applications such as smart energy and building automation.
- Based on **Request-Response model** between end-points
- Client-Server interaction is **asynchronous over a datagram oriented transport protocol** such as UDP

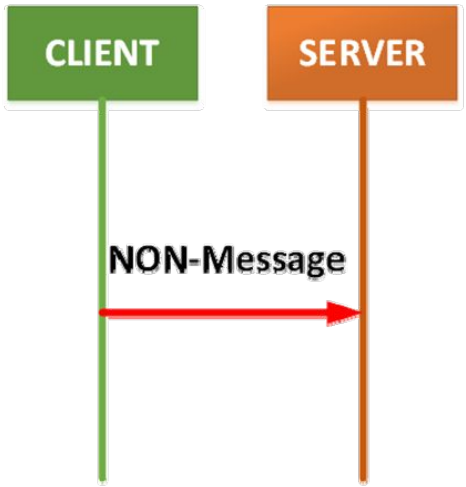
- The Constrained Application Protocol (CoAP) is a session layer protocol designed by IETF Constrained RESTful Environment (CoRE) working group to provide lightweight RESTful (HTTP) interface.
- Representational State Transfer (REST) is the standard interface between HTTP client and servers.
- Lightweight applications such as those in IoT, could result in significant overhead and power consumption by REST.
- CoAP is designed to enable low-power sensors to use RESTful services while meeting their power constraints.

- Built over UDP, instead of TCP (which is commonly used with HTTP) and has a light mechanism to provide reliability.
- CoAP architecture is divided into two main sub-layers:
  - Messaging
  - Request/response.
- The messaging sub-layer is responsible for reliability and duplication of messages, while the request/response sublayer is responsible for communication.
- CoAP has four messaging modes:
  - Confirmable
  - Non-confirmable
  - Piggyback
  - Separate

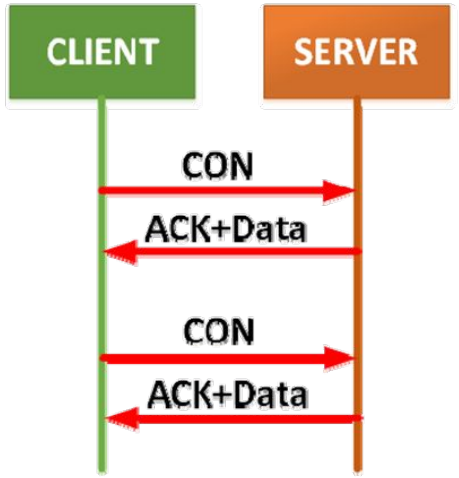
CoAP Request-Response Model



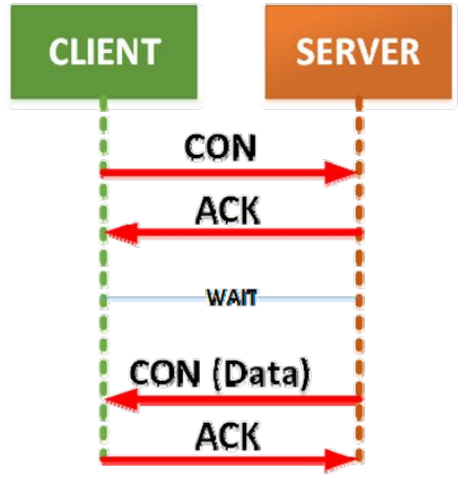
Confirmable Message



Non-Confirmable Message



Piggyback Message



Separate Message

Features

- Reduced overheads and parsing complexity.
- URL and content-type support.
- Support for the discovery of resources provided by known CoAP services.
- Simple subscription for a resource, and resulting push notifications.
- Simple caching based on maximum message age.

XMPP

- **XMPP – Extensible Messaging and Presence Protocol.**
- A communication protocol for **message-oriented middleware** based on XML (Extensible Markup Language).
- Real-time exchange of structured data.
- It is an open standard protocol.

XMPP (cont..)

- XMPP uses a **client-server architecture**.
- As the model is **decentralized**, no central server is required.
- XMPP provides for the **discovery of services** residing locally or across a network, and the **availability information** of these services.
- Well-suited for cloud computing where virtual machines, networks, and firewalls would otherwise present obstacles to alternative service discovery and presence-based solutions.
- Open means to support machine-to-machine or peer-to-peer communications across a diverse set of networks.

XMPP Highlights

- Decentralization – No central server; anyone can run their own XMPP server.
- Open standards – No royalties or granted permissions are required to implement these specifications
- Security – Authentication, encryption, etc.
- Flexibility – Supports interoperability

Application

- Publish-subscribe systems
- Signaling for VoIP
- Video
- File transfer
- Gaming
- Smart grid
- Social networking services

Weakness

- Does not support QoS.
- Text based communications induces higher network overheads.
- Binary data must be first encoded to base64 before transmission.

AMQP

- **Advanced Message Queuing Protocol.**
- **Open standard for passing business messages** between applications or organizations.
- Connects between systems and business processes.
- It is a binary application layer protocol.
- Basic unit of data is a *frame*.
- ISO standard: **ISO/IEC 19464**

Features

- Security
- Reliability
- Interoperability
- Routing
- Queuing
- Open standard

QoS

- *At-most-once*
  - each message is delivered once or never
- *At-least-once*
  - each message is certain to be delivered, but may do so multiple times
- *Exactly-once*
  - message will always certainly arrive and do so only once

Application

- Monitoring and global update sharing.
- Connecting different systems and processes to talk to each other.
- Allowing servers to respond to immediate requests quickly and delegate time consuming tasks for later processing.
- Distributing a message to multiple recipients for consumption.
- Enabling offline clients to fetch data at a later time.
- Introducing fully asynchronous functionality for systems.
- Increasing reliability and uptime of application deployments.

Communication at DataLink Layer

- IEEE 802.15.4
- Zigbee
- 6LoWPAN
- Wireless HART
- Z-Wave
- ISA 100
- Bluetooth
- NFC
- RFID

IEEE 802.15.4

- Well-known standard for low data-rate WPAN.
- Developed for low-data-rate monitoring and control applications and extended-life low-power-consumption uses.
- 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

Bluetooth

- Bluetooth wireless technology is a short range communications technology.
- Intended for replacing cables connecting portable units
- Maintains high levels of security.
- Bluetooth technology is based on Ad-hoc technology also known as Ad-hoc Piconets.

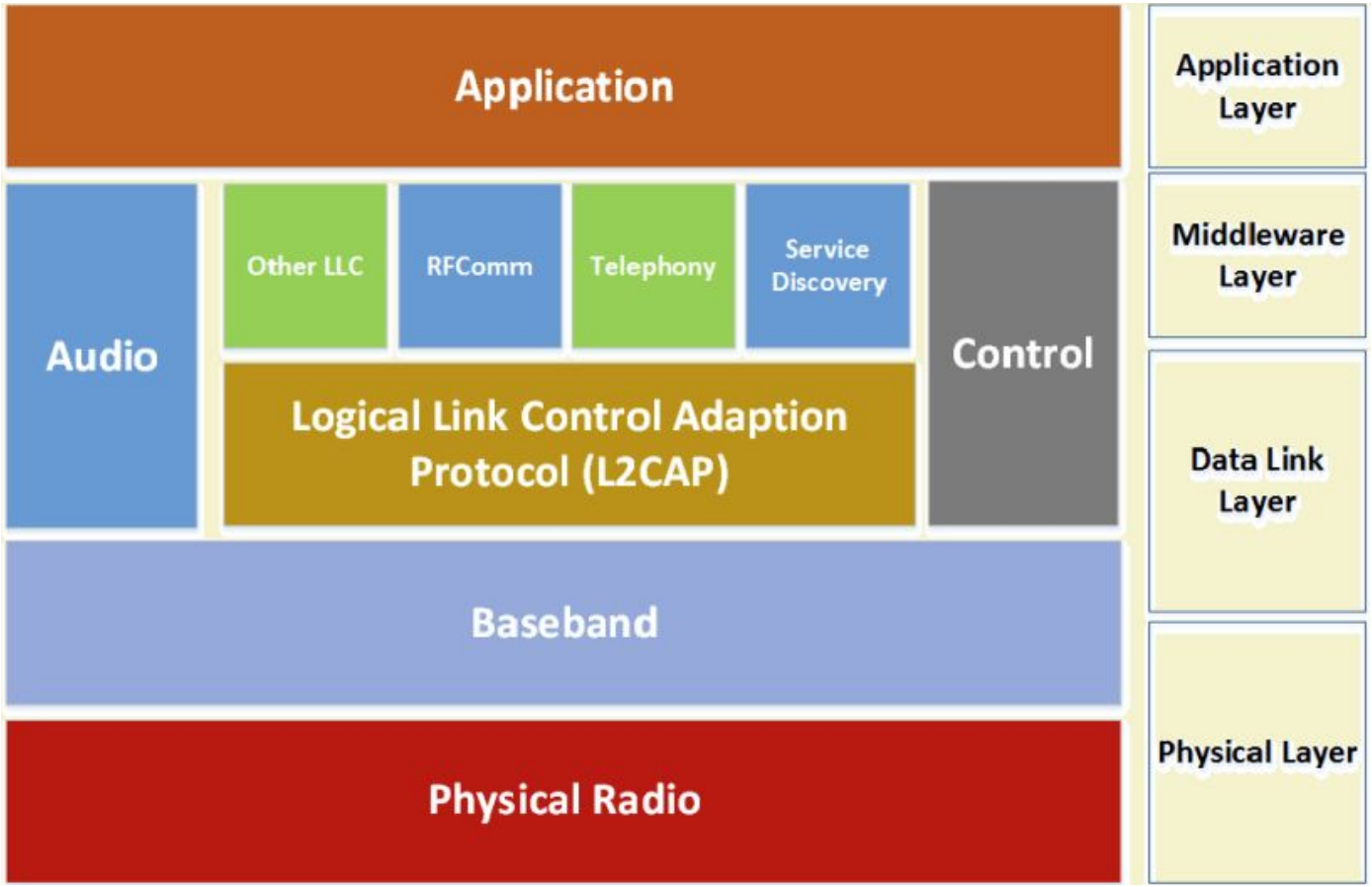
Bluetooth Features

- 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 nominalrate 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.
- 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.

Connection Establishment

- Inquiry:
  - Inquiry run by one Bluetooth device to try to discover other devices near it.
- Paging:
  - Process of forming a connection between two Bluetooth devices.
- Connection:
  - A device either actively participates in the network or enters a low-power sleep mode.
- Modes of Connection:
  - Active: Actively transmitting or receiving data.
  - Sniff: Sleeps and only listens for transmissions at a set interval
  - Hold: Power-saving mode where a device sleeps for a defined period and then returns back to active mode
  - Park: Slave will become inactive until the master tells it to wake back up.

Bluetooth Protocol Stack



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.
- 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

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 .
  - RFCOMM provides a simple reliable data stream to the user, similar to TCP.
  - Supports up to 60 simultaneous connections between two devices.
- 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.

Bluetooth Protocol Stack

- 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.
  - 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.
  - There is no direct connection between the slaves.
  - A device can be a member of two or more Piconets.

Zigbee

- 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.
- The most popular use of ZigBee is wireless sensor networks using the mesh topology.

Zigbee 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

Z Wave

- Zwave is a protocol for communication among devices used for home automation.
- It uses RF for signaling and control.
- Mesh network topology is the main mode of operation, and can support 232 nodes in a network.
- A central network controller device sets-up and manages a Zwave network.
- Each logical Zwave network has 1 Home (Network) ID and multiple node IDs for the devices in it.
- Nodes with different Home IDs cannot communicate with each other.
- Network ID length=4 Bytes, Node ID length=1 Byte.

Z Wave (cont..)

- Uses source routed network mesh topology using 1 primary controller.
- Devices communicate with one another when in range.
- When devices are not in range, messages are routed through different nodes to bypass obstructions created by household appliances or layout.
- This process of bypassing radio dead-spots is done using a message called Healing.
- As Zwave uses a source routed static network, mobile devices are excluded from the network and only static devices are considered.

Zwave vs. Zigbee

Zwave	Zigbee
• User friendly and provides a simple system that users can set up themselves. • Ideal for someone with a basic understanding of technology who wants to keep their home automation secure, efficient,simple to use, and easy to maintain. • Expensive. • Nine out of ten leading security and communication companies in the U.S. use ZWave in their smart home solutions	• Requires so little power that devices can last up to seven years on one set of batteries. • Ideal for technology experts who want a system they can customize with their preferences and install themselves. • Cheaper than Zwave. • ZigBee Alliance consists of nearly 400 member organizations that use, develop, and improve ZigBee's open-standard wireless connection