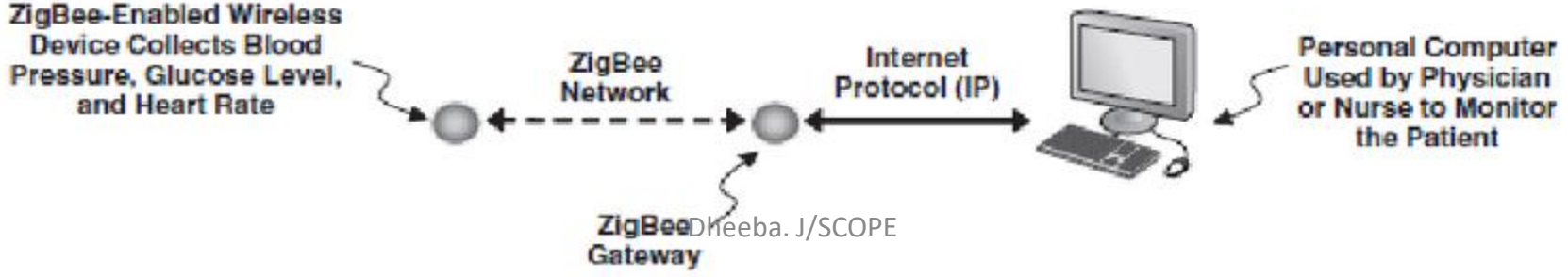
Module 2

Components in IoT

Communication Protocol – Zigbee

- Communication protocol -> for low-data-rate short-range wireless networking.
- ZigBee-based wireless devices operate in 868 MHz, 915 MHz, and 2.4 GHz frequency bands.
- Zigbee devices are capable of being operational for several years -> the device spends most of its time in a power-saving mode, also known as sleep mode
- A simple Zigbee application -> in-patient monitoring system



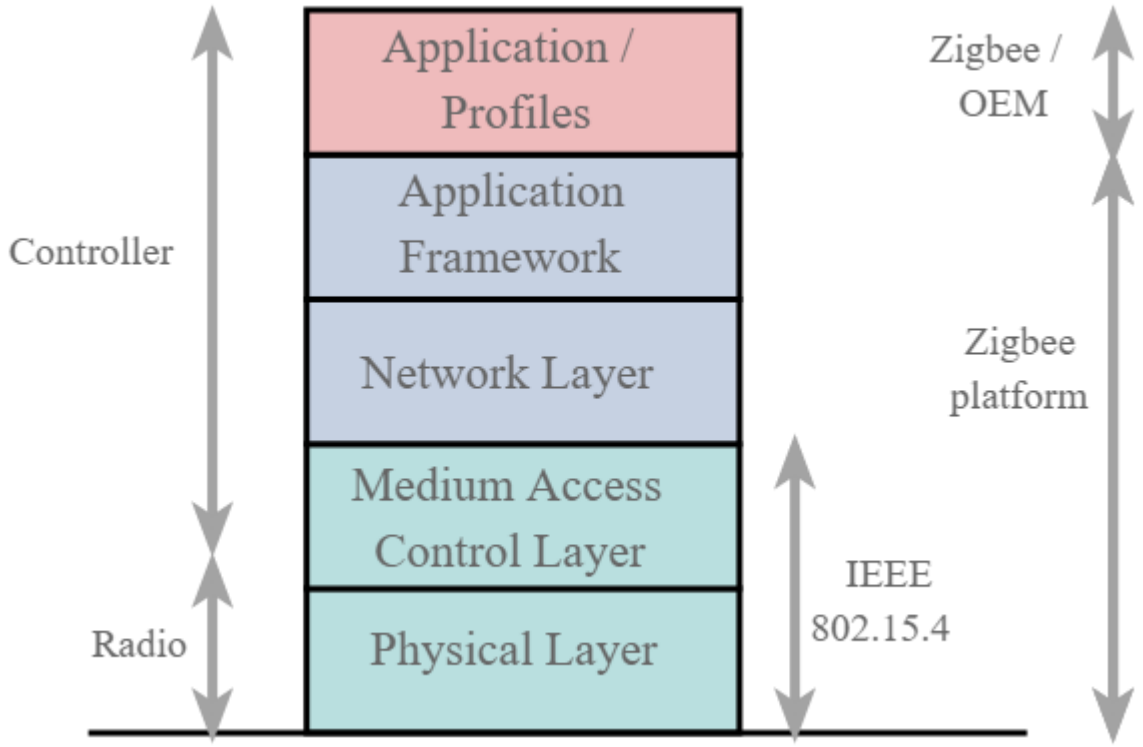
- This standard uses only the first two layers (PHY, MAC) plus the logical link control (LLC) and service specific convergence sub-layer (SSCS) additions to communicate with all upper layers.
- Comparison

	Data Rate	Typical Range	Application Examples
ZigBee	20 to 250 Kbps	10–100 m	Wireless Sensor Networks
Bluetooth	1 to 3 Mbps	2–10 m	Wireless Headset Wireless Mouse
IEEE 802.11b	1 to 11 Mbps	30–100 m	Wireless Internet Connection

Zigbee can be used if you want to transmit and receive simple commands and/or gather information from sensors such as temperature or humidity sensors.

- In many ZigBee applications, the devices have duty cycles of less than 1% to ensure years of battery life.
  - duty cycle is the ratio of the time the device is active to the total time
  - if a device wakes up every minute and stays active for 60 ms
  - Then duty cycle, 0.06/60 = 0.001 (0.1%)

- Protocol stack – Zigbee
- Uses direct sequence spread spectrum (DSSS) modulation.
- Highly tolerant of noise and interference and offers link reliability improvement mechanisms.
- Uses carrier sense multiple access with collision avoidance (CSMA-CA) for channel access.

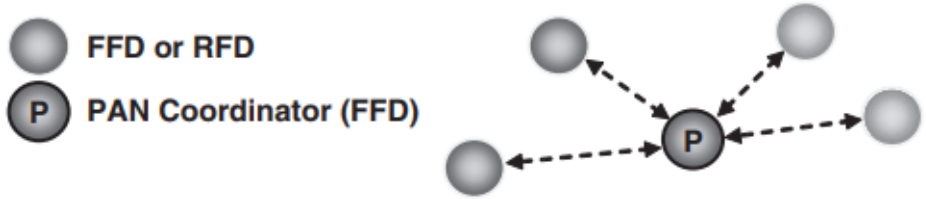


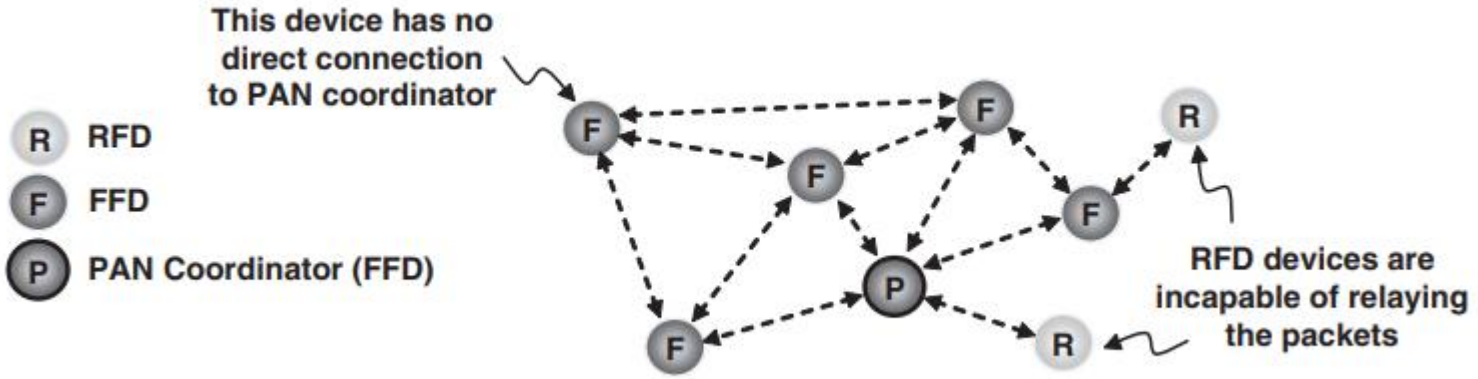
- ZigBee-based devices must be able to interact with each other regardless of the manufacturing origin – interoperability
- Two types of devices in an IEEE 802.15.4 wireless network: full-function devices (FFDs) and reduced-function devices (RFDs).
- FFD
  - capable of taking any role and does all functionalities of IEEE 802.15.4.
- RFD
  - can talk only with an FFD device.
  - intended for very simple applications such as turning on or off a switch
  - Processing power and memory are less compared to FFD

- FFD device can take three different roles
  - Zigbee router -> FFD device that is capable of relaying messages.
  - Zigbee coordinator -> If the coordinator is also the principal controller of a personal area network (PAN), it is called a PAN coordinator .
  - Zigbee end device -> If a device is not acting as a coordinator, it is simply called a device .

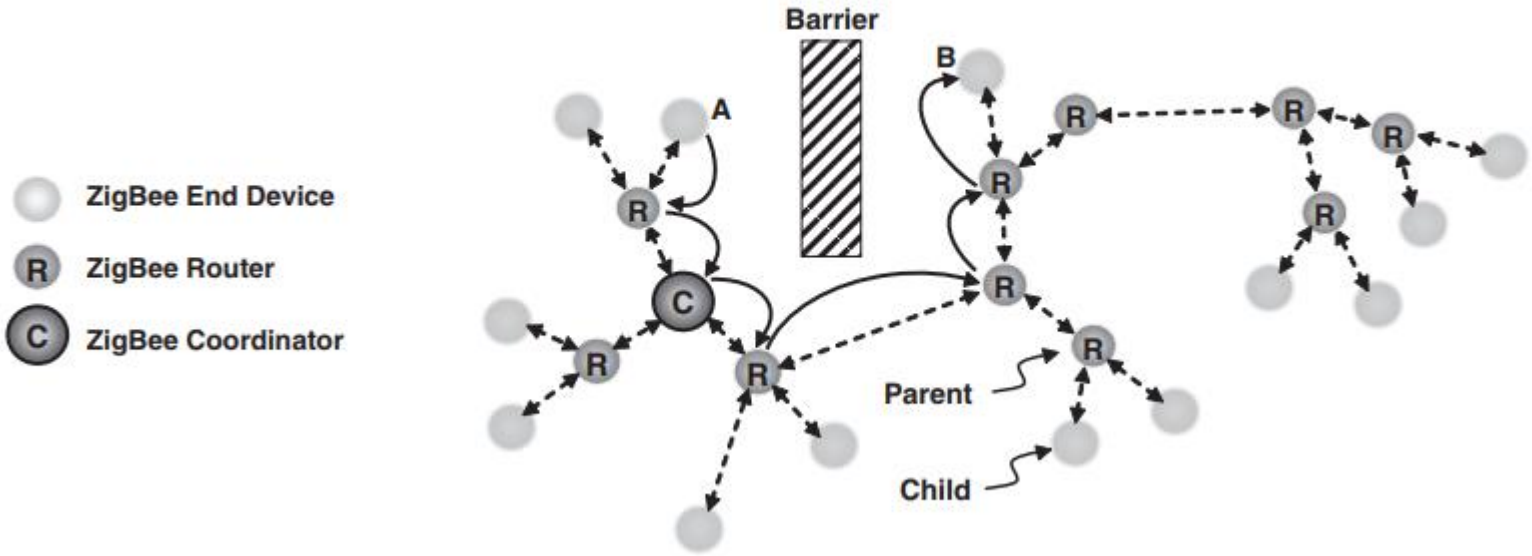
ZigBee Networking Topologies

- Star topology
- Every device in the network can communicate only with the PAN coordinator.
- PAN coordinator is activated and starts establishing its network.
- Select a unique PAN identifier that is not used by any other network in its radio sphere of influence —the region around the device in which its radio can successfully communicate with other radios.





- Peer to Peer
  - Each device can communicate directly with any other device if the devices are placed close enough together to establish a successful communication link.
  - Any FFD in a peer-to-peer network can play the role of the PAN coordinator.
  - One way to decide which device will be the PAN coordinator is to pick the first FFD device that starts communicating as the PAN coordinator.
  - In a peer-to-peer network, all the devices that participate in relaying the messages are FFDs because RFDs are not capable of relaying the messages.
  - However, an RFD can be part of the network and communicate only with one particular device (a coordinator or a router) in the network.
  - peer-to-peer network is known as a mesh topology

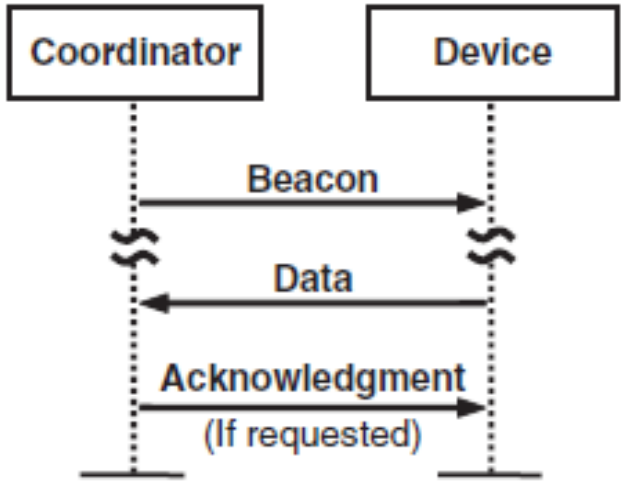


- Tree topology
  - ZigBee coordinator (PAN coordinator) establishes the initial network.
  - ZigBee routers form the branches and relay the messages.
  - ZigBee end devices act as leaves of the tree and do not participate in message routing.
- PAN coordinator role (regardless of topology used)
  - Allocate a unique address (16-bit or 64-bit) to each device in the network.
  - Initiate, terminate, and route the messages throughout the network.
  - Selects an unique PAN identifier for the network.

Communication in Zigbee

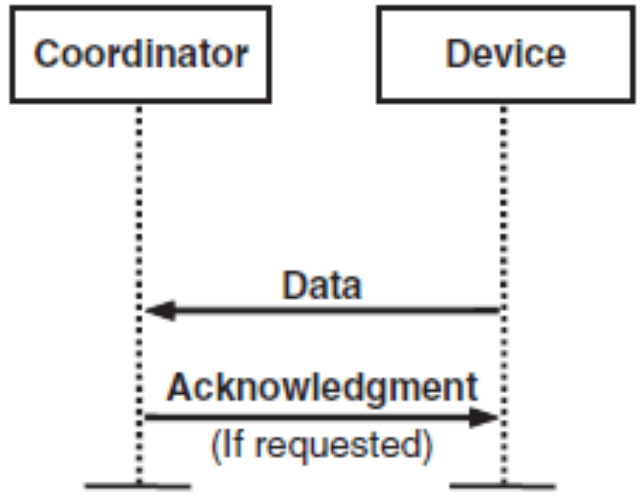
- CSMA-CA
  - In CSMA-CA, anytime a device wants to transmit, it first performs a clear channel assessment (CCA) to ensure that the channel is not in use by any other device.
  - Then the device starts transmitting its own signal.
  - Carrier sense (CS) -> analyse the type of the occupying signal and, if this signal is an IEEE 802.15.4 signal, then the device may decide to consider the channel busy
  - If the channel is not clear, the device backs off for a random period of time and tries again.
  - The random back-off and retry are repeated until either the channel becomes clear or the device reaches its user-defined maximum number of retries.

- Beacon-Enabled vs. Nonbeacon Networking
  - Channel access: contention based or contention free
  - Contention-based channel access , all the devices that want to transmit in the same frequency channel use the CSMA-CA mechanism, and the first one that finds the channel clear starts transmitting.
  - In the contention-free method, the PAN coordinator dedicates a specific time slot to a particular device -> **Guaranteed time slot (GTS).**
  - Therefore, a device with an allocated GTS will start transmitting during that GTS without using the CSMA-CA mechanism

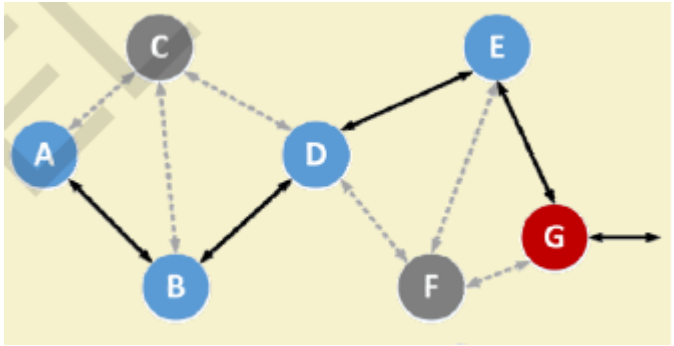


- To provide a GTS, the PAN coordinator needs to ensure that all the devices in the network are synchronized.
- Beacon is a message with specific format that is used to synchronize the clocks of the nodes in the network.
- A coordinator has the option to transmit beacon signals to synchronize the devices attached to it -> beacon-enabled PAN
- Disadvantage -> all the devices in the network must wake up on a regular basis, listen for the beacon, synchronize their clocks, and go back to sleep.
- Battery life of a device in a beacon enabled network is normally less than a network with no beaconing.

- A network in which the PAN coordinator does not transmit beacons is known as a nonbeacon network .
- A nonbeacon network cannot have GTSs and no contention free periods because the devices cannot be synchronized with one another.
- The battery life in a nonbeacon network can be noticeably better than in a beacon-enabled network because in a nonbeacon network, the devices wake up less often.



Network formation



- **Self-forming networks**
  - ZigBee network starts its formation as soon as devices become active.
  - the first FFD device that starts communicating can establish itself as the ZigBee coordinator, and other devices then join the network by sending association requests.
- **Self healing networks**
  - In a mesh network there is normally more than one way to relay a message from one device to another.
  - Naturally, the most optimized way is selected to route the message.
  - However, if one of the routers stops functioning due to exhaustion of its battery or if an obstacle blocks the message route, the network can select an alternative route.
  - This is an example of the self-healing characteristic of ZigBee mesh networking

Security

- In a wireless network, the transmitted messages can be received by any nearby device, including an intruder. There are two main security concerns in a wireless network -> Data confidentiality
- The intruder device can gain sensitive information by simply listening to the transmitted messages.
- Encrypting the messages before transmission will solve the confidentiality problem.
- An encryption algorithm modifies a message using a string of bits known as the *security key,* and only the intended recipient will be able to recover the original message.
- The IEEE 802.15.4 standard supports the use of Advanced Encryption Standard (AES) to encrypt their outgoing messages.

- Intruder device may modify and resend one of the previous messages even if the messages are encrypted.
- Data authentication
- One of the main constraints in implementing security features in a ZigBee wireless network is limited resources.
- Nodes with tamper resistance -> erase the sensitive information, including the security keys, if tampering is detected

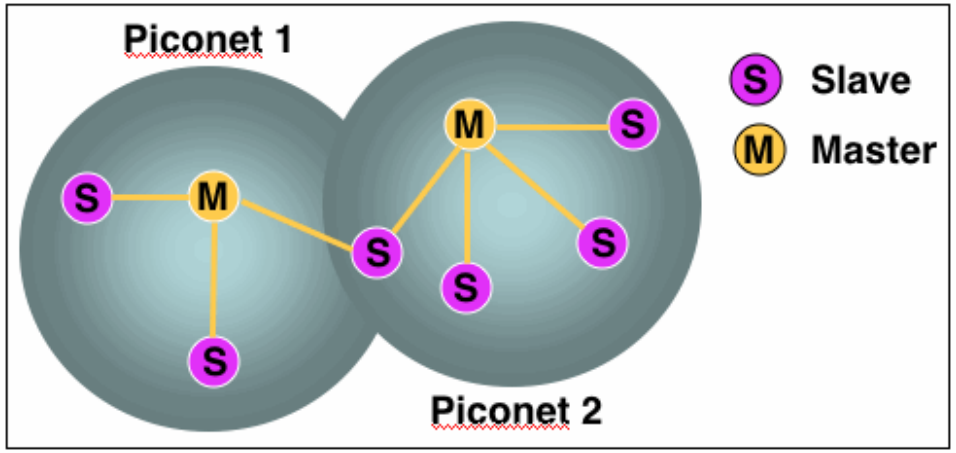
Bluetooth

- Bluetooth provides short-range, low-cost connectivity between portable devices.
- Characteristics -> low power, short range, and medium transmission speed.
- low power consumption makes Bluetooth ideal for small, battery-powered devices like mobile phones and pocket PCs
- Originally used for telephony applications such as wireless headsets for cell phones.
- Bluetooth's short range (10 m) is ideal for the concept of "personal operating space"
- Bluetooth technology operates in the unlicensed industrial, scientific and medical (ISM) band at 2.4 to 2.485 GHZ.

- Bluetooth WPAN involves up to eight devices, located within a 10-m radius personal operating space.
- *Ad hoc networking* -> exchange information or share services is done spontaneously according to immediate need.
- For example, one could use the Bluetooth-enabled mobile phone at a Bluetooth-enabled vending machine to charge one's account and buy a drink.
- Bluetooth typically hops faster and uses shorter packets.
- Short packets and fast hopping limit the impact of interference from other radio systems that use the same frequency band.
- Application -> mobile computers, bar code laser scanners, cash registers, vending machines, GPS receivers, slide projectors, printers, digital cameras, digital camcorders, test and measurement equipment, and LAN access points

Basic Definitions

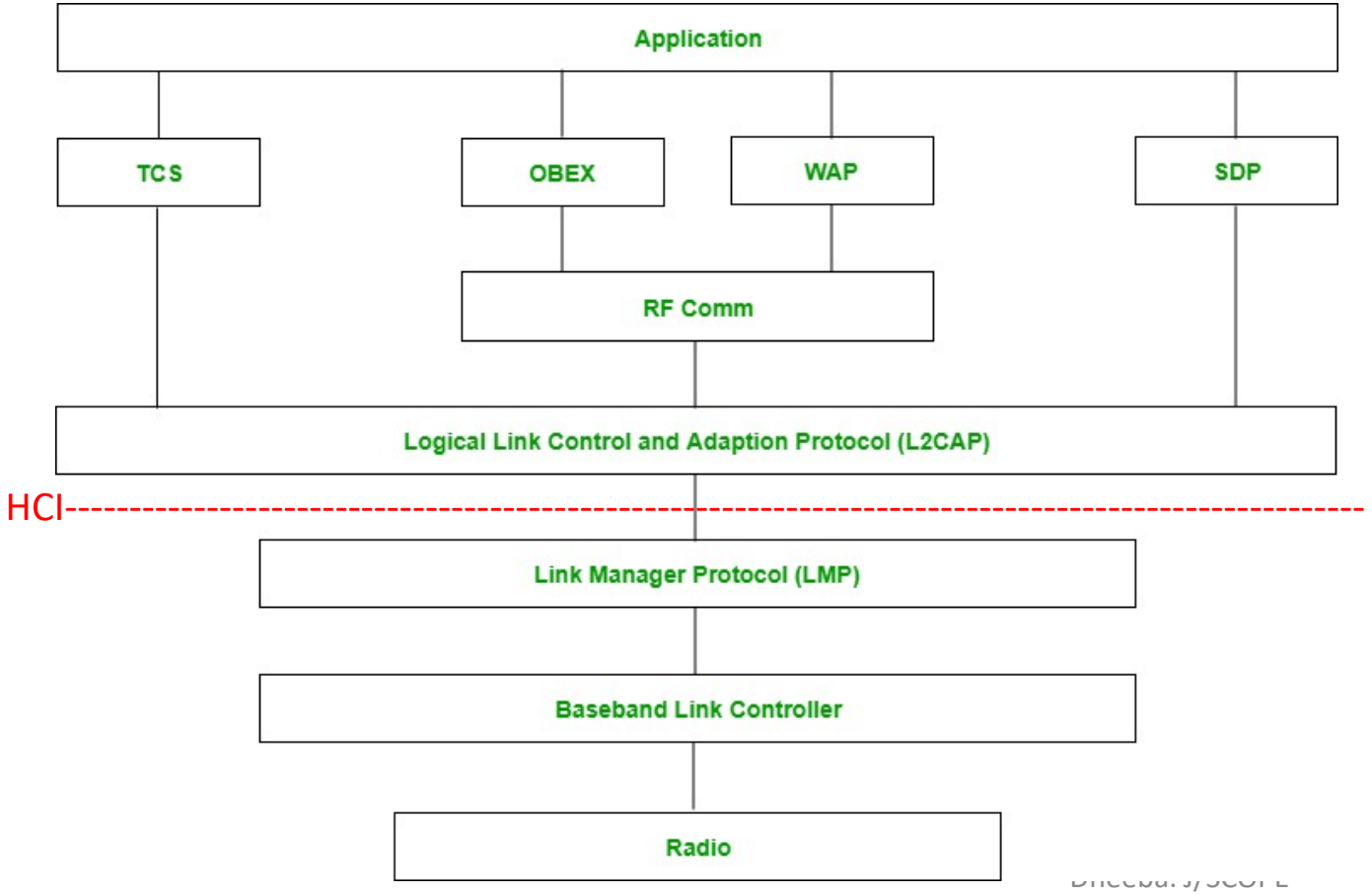
- **Piconet.**
  - A collection of devices connected via Bluetooth technology in an ad hoc fashion.
  - A piconet starts with two connected devices, such as a PC and cellular phone, and may grow to eight connected devices. (7 slaves + 1 master)
  - When establishing a piconet, one unit will act as a master for synchronization purposes, and the other(s) as slave(s) for the duration of the piconet connection.
- **Scatternet.**
  - Two or more independent and nonsynchronized piconets that communicate with each other.
  - A slave as well as a master unit in one piconet can establish this connection by becoming a slave in the other piconet.

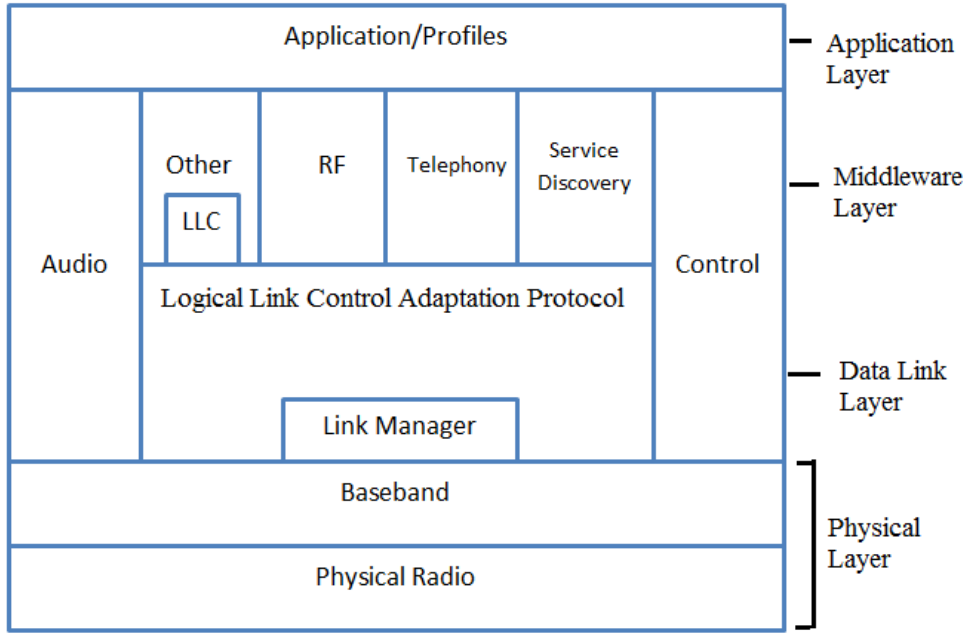


- **Master unit.** The device in the piconet whose clock and hopping sequence are used to synchronize all other devices in the piconet.
- **Slave units.** All devices in a piconet that are not the master (up to seven active units for each master).
- **MAC address.** A 3-bit medium access control address used to distinguish between units participating in the piconet.
- **Parked units.** Devices in a piconet which are time-synchronized but do not have MAC addresses.
- **Sniff and hold mode.** Devices that are synchronized to a piconet, and which have temporarily entered power-saving mode in which device activity is reduced.

Bluetooth Protocol Stack

- Bluetooth protocol stack can be placed into three groups:
  - Transport protocol group
  - Middleware protocol group
  - Application group





- **Transport Protocol Group**
  - Designed to allow Bluetooth devices to locate and connect to each other.
  - These protocols carry audio and data traffic between devices and support both synchronous and asynchronous transmission.
  - Audio traffic is treated with high priority in Bluetooth (goes directly to the baseband layer)
  - Responsibility -> Managing the physical and logical links between the devices
  - **Logical link control and adaptation protocol (L2CAP) layer**
    - 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

- **Link manager layer (LML)**
  - Responsible for negotiating the properties of the Bluetooth air interface between them.
  - Supervise device pairing -> creation of a trust relationship between the devices by generating and storing an authentication key for future device authentication
- **Baseband and radio layers**
  - Responsible for the process of searching for other devices and establishing a connection with them
  - Assigns the master and slave roles.
  - Controls bluetooth unit's synchronization and transmission frequency hopping sequence
- **Host controller interface (HCI) layer**
  - It has been developed to serve the purpose of interoperability between host devices and Bluetooth modules
  - The HCI provides a command interface to the baseband controller and link manager, and access to hardware status and control registers. Essentially this interface provides a uniform method of accessing the Bluetooth baseband capabilities.

- **Middleware Protocol Group**
  - Third party and industry standard protocols and protocols developed specifically by the Special Interest Group (SIG)
  - **RFCOMM layer**
    - Provides a virtual serial port to applications
    - Advantage -> easy for applications designed for cabled serial ports to migrate to Bluetooth
  - **Service discovery protocol (SDP) layer**
    - Two devices can start communicating on the spur of the moment.
    - Once a connection is established there is a need for the devices to find and understand the services the other devices have to offer.
    - Responsibility -> discover and learn about the services offered by the other device

- **Object exchange (OBEX) protocol.**
  - IrOBEX (in short, OBEX) is a session protocol developed by the Infrared Data Association to exchange objects in a simple and spontaneous manner.
  - Uses client-server model (similar to http but in a light weigh fashion)
- **Infrared data association (IrDA) interoperability protocols.**
  - The SIG has adopted some IrDA protocols to ensure interoperability between applications.
- **Networking layers**
  - Bluetooth wireless communication uses a peer-to-peer network topology rather than an LAN type topology.
  - Dial-up networking uses the attention (AT) command layer (accessed is an IP network)
- **Telephone control specifi cation (TCS) layer and audio**
  - Support telephony functions, which include call control and group management
  - Audio traffic is treated separately in Bluetooth.
  - Isochronous -> audio traffic has a time element associated with it. It is routed directly to the baseband.

- **Application Group**
  - This group consists of actual applications that make use of Bluetooth links and refers to the software that exists above the protocol stack.
  - The software uses the protocol stack to provide some function to the user of the Bluetooth devices.
  - Bluetooth-SIG does not define any application protocols nor does it specify any API.
  - Bluetooth profiles are developed to establish a base point for use of a protocol stack to accomplish a given usage case.

Bluetooth Link Types

- Supports two link types:
  - Synchronous connection oriented (SCO) type (used primarily for voice)
  - Asynchronous connectionless (ACL) type (used primarily for packet data).
- The SCO link is symmetric and typically supports time-bounded voice traffic.
- SCO packets are transmitted over reserved intervals.
- Once the connection is established, both master and slave units may send SCO packets without being polled.
- The SCO link type supports circuit-switched, point-to-point connections and is used often for voice traffic.
- The data rate for SCO links is 64 kbps.

- The ACL link is packet oriented and supports both symmetric and asymmetric traffic.
- The master unit controls the link bandwidth and decides how much piconet bandwidth is given to each slave, and the symmetry of the traffic.
- Slaves must be polled before they can transmit data.
- The ACL link also supports broadcast messages from the master to all slaves in the piconet.

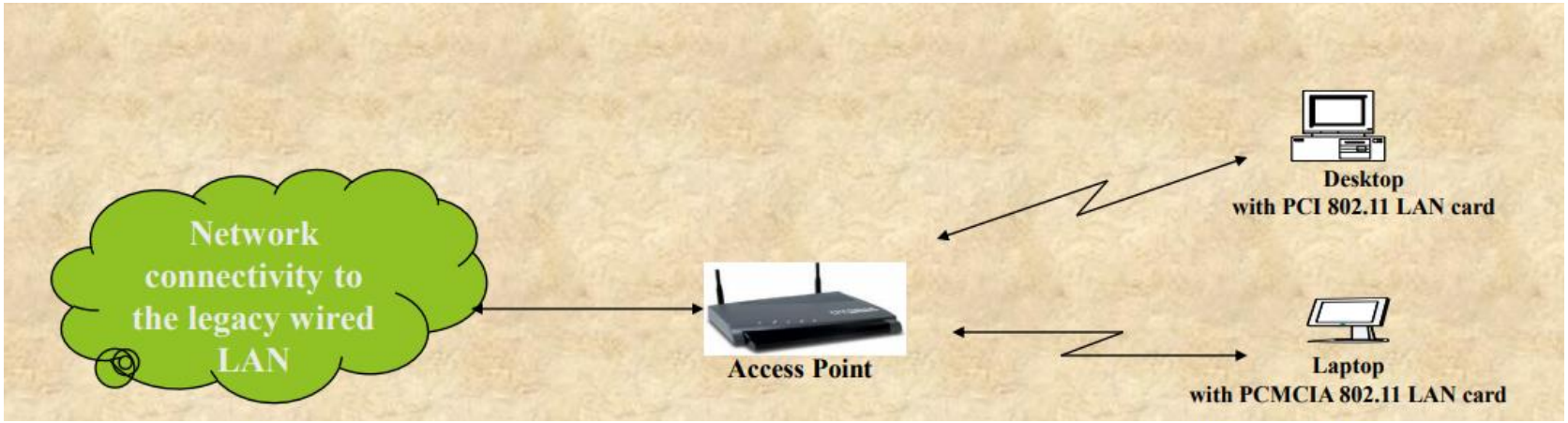
WiFi

- WiFi is primarily a local area networking (LAN) technology designed to provide in-building broadband coverage.
- It is based on IEEE 802.11 specification.
- WiFi stands for **Wi**reless **Fi**delity.
- Present scenario - supports a peak physical-layer data rate of 54 Mbps and typically provide indoor coverage over a distance of 100 feet.
- Fixed channel bandwidth of 25 MHz for 802.11b and 20 MHz for either 802.11a or g networks.

Radio Signals

- radio signals transmitted from WiFi antennas are picked up by WiFi receivers, i.e computers and cell phones that are equipped with WiFi cards.
- the WiFi card reads the signals and thus creates an internet connection between the user and the network without the use of a physical cable.

- Provides network connectivity over wireless media
- An Access Point (AP) is installed to act as Bridge between Wireless and Wired Network
- The AP is connected to wired network and is equipped with antennae to provide wireless connectivity



- Range (Distance between Access Point and WLAN client) depends on structural hindrances and RF gain of the antenna at the Access Point
- To service larger areas, multiple APs may be installed with a 20-30% overlap
- A client is always associated with one AP and when the client moves closer to another AP, it associates with the new AP (Hand-Off)

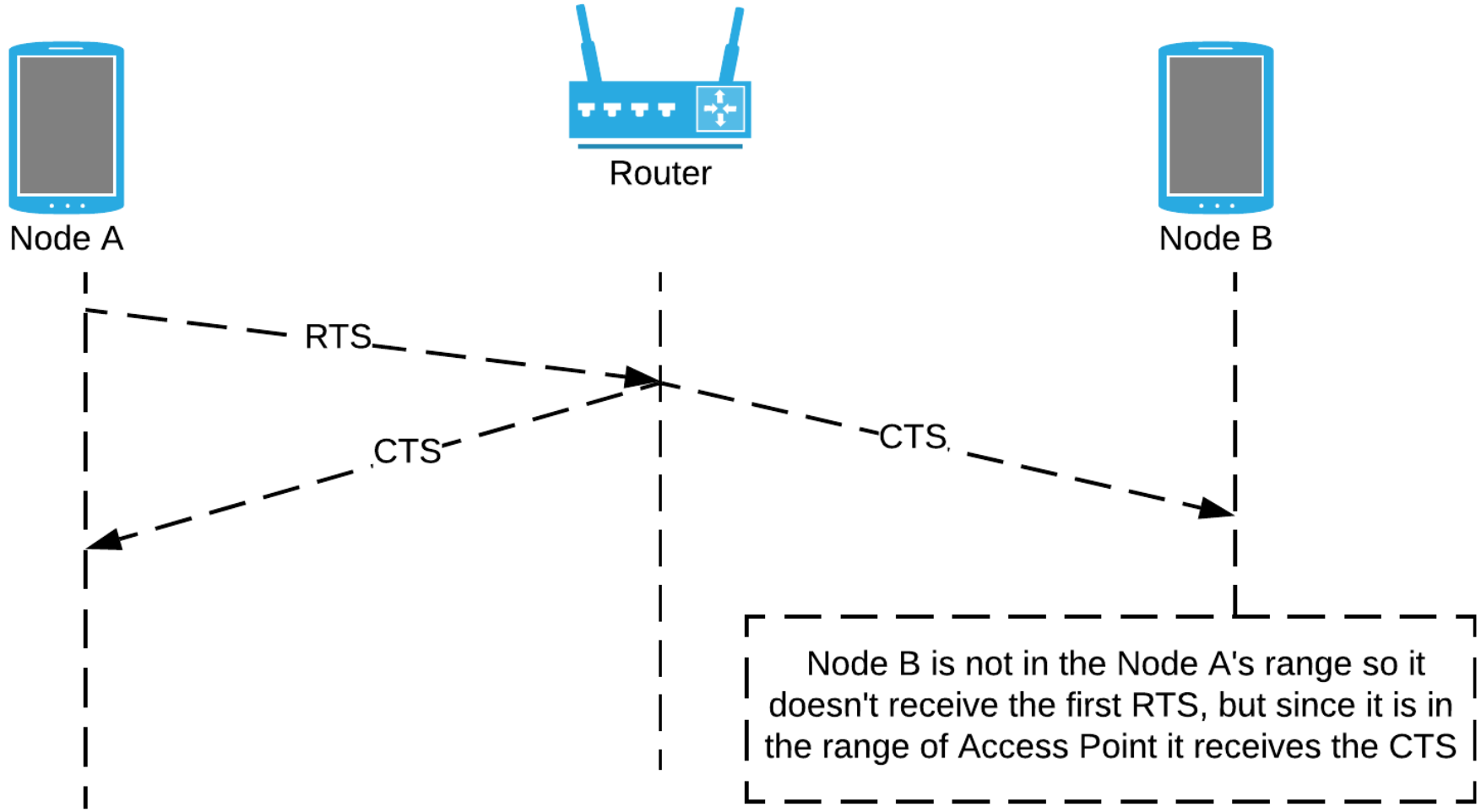
802.11 family

- **802.11** – This pertains to wireless LANs and provides 1 - or 2-Mbps transmission in the 2.4-GHz band using either frequency-hopping spread spectrum (FHSS) or direct-sequence spread spectrum (DSSS).
- **802.11a** – This is an extension to 802.11 that pertains to wireless LANs and goes as fast as 54 Mbps in the 5-GHz band. 802.11a employs the orthogonal frequency division multiplexing (OFDM) encoding scheme.
- **802.11b** – The 802.11 high rate WiFi is an extension to 802.11 that pertains to wireless LANs and yields a connection as fast as 11 Mbps transmission in the 2.4-GHz band. The 802.11b specification uses only DSSS
- **802.11g** – This pertains to wireless LANs and provides 20+ Mbps in the 2.4-GHz band.

Wi-Fi - Access Protocols

- Wireless LANs use a media access control protocol called Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA).
- WiFi systems are the half duplex - all stations transmit and receive on the same radio channel.
- fundamental problem of a radio system is that a station cannot *hear* while it is sending - impossible to detect a collision
- collision avoidance mechanism called the **Distributed Control Function** (DCF).
  - WiFi station will transmit only when the channel is clear
  - All transmissions are acknowledged
  - if a station does not receive an acknowledgement, it assumes a collision occurred and retries after a random waiting interval.

- The method of CSMA/CA is −
  - When a frame is ready, the transmitting station checks whether the channel is idle or busy.
  - If the channel is busy, the station waits until the channel becomes idle.
  - If the channel is idle, the station waits for an Inter-frame gap (IFG) amount of time and then sends the frame.
  - After sending the frame, it sets a timer.
  - The station then waits for acknowledgement from the receiver. If it receives the acknowledgement before expiry of timer, it marks a successful transmission.
  - Otherwise, it waits for a back-off time period and restarts the algorithm.



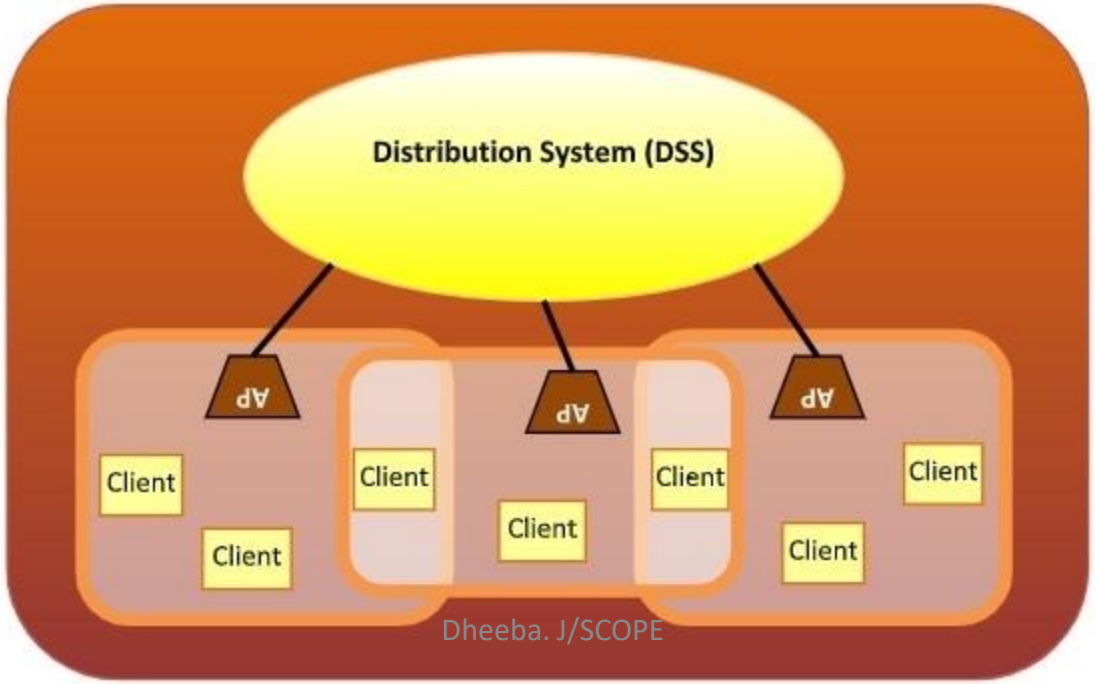
the base station sends to the receiver a Request To Send (RTS) which contains the MAC address of the transmitter and receiver + *Duration* field

Co-ordination Functions in 802.11 MAC Sublayer

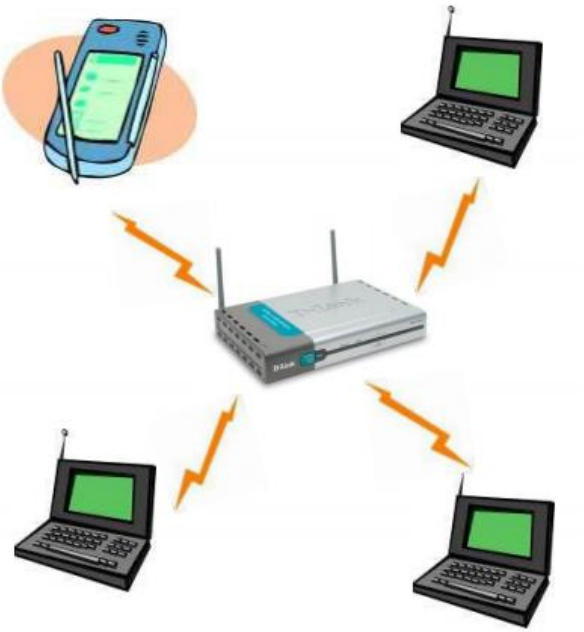
- two co-ordination functions for collision avoidance before transmission
  - **Distributed Coordination Function (DCF)**
    - It is a mandatory function used in CSMA/CA.
    - It is used in distributed contention-based channel access.
    - It is deployed in both Infrastructure BSS (basic service set) as well as Independent BSS.
  - **Point Coordination Function (PCF)**
    - It is an optional function used by 802.11 MAC Sublayer.
    - It is used in centralized contention-free channel access.
    - It is deployed in Infrastructure BSS only.

Configuration of Wireless LANs

- Each station in a Wireless LAN has a wireless network interface controller. (Stations – STA)
  - **Wireless Access Point (WAP)** – WAPs or simply access points (AP) are generally wireless routers that form the base stations or access points.
  - **Client** – Clients are workstations, computers, laptops, printers, smart phones, Sensors etc. They are around tens of metres within the range of an AP.



- **Basic Service Set (BSS) -** A basic service set is a group of stations communicating at physical layer level.
- depending upon mode of operation – 2 categories
  - **Infrastructure BSS –** Here, the devices communicate with other devices through access points.
  - **Independent BSS –** Here, the devices communicate in peer-to-peer basis in an ad hoc manner.



- **Extended Service Set (ESS) –** It is a set of all connected BSS
- **Distribution System (DS) –** It connects access points in ESS.

Frame Format of IEEE 802.11

- Main fields of a frame of wireless LANs
  - **Frame Control** – It is a 2 bytes starting field composed of 11 subfields. Contain control information of the frame.
  - **Duration** – It is a 2-byte field that specifies the time period for which the frame and its acknowledgment occupy the channel.
  - **Address fields** – There are three 6-byte address fields containing addresses of source, immediate destination, and final endpoint respectively.
  - **Sequence** – It a 2 bytes field that stores the frame numbers.
  - **Data** – This is a variable-sized field that carries the data from the upper layers. The maximum size of the data field is 2312 bytes.
  - **Check Sequence** – It is a 4-byte field containing error detection information.

Application

- WiFi can be good for IoT applications that don’t have to worry about power drain (e.g. devices that are plugged into an outlet), that need to send a lot of data (e.g. video), and that don’t need high range. A good example would be a home security system.

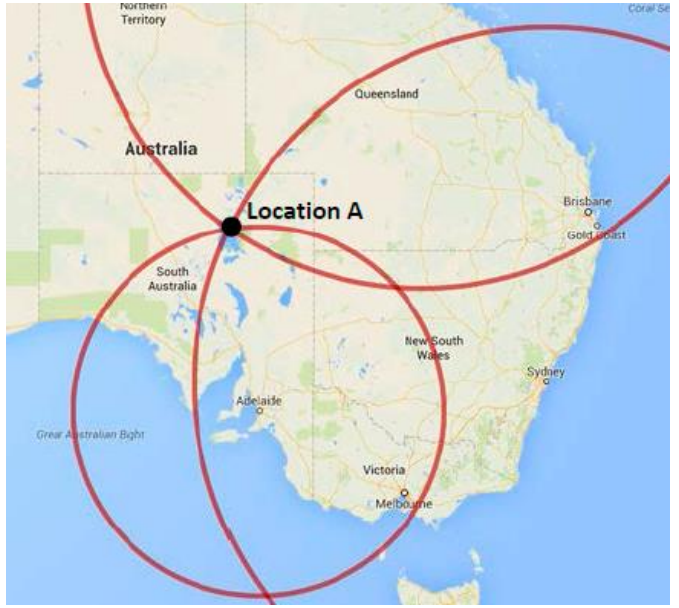
GPS

GPS

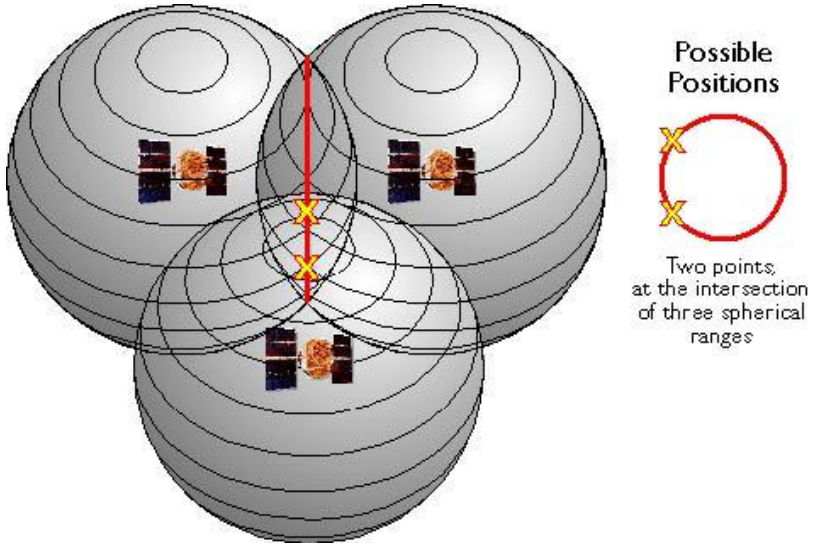
- GPS or Global Positioning System is a satellite navigation system that furnishes location and time information in all climate conditions to the user.
- The system gives critical abilities to military and civilian users around the globe.
- GPS provides continuous real-time, 3-dimensional positioning, navigation and timing worldwide.
- founded by the United States Department of Defense in 1973 to track objects on Earth in real time.
- It uses 24 active satellites known as the Global Navigation Satellite System, and eight backup satellites in case an active satellite fails.
- **NavIC** is India's own navigation system, similar to the U.S.' GPS (IRNSS)

How Does GPS Work?

- GPS uses satellites to track the position of any object with a GPS tracking chip, including vehicles, people, and pets.
- At least three satellites -- positioned to be in the sky over any area at any given time -- are used to **triangulate** the position of a tracking chip.
- Satellites use microwaves to collect information in three dimensions and calculate position from their intersecting spheres.
- 4 satellites = elimination of the second possible location



Trilateration



- In order to make this calculation, every GPS receiver must know the following things:
  - The location of at least four GPS satellites above it and;
  - The distance between the receiver and each of those GPS satellites (calculated by knowing the time it took to reach the receiver)
- A GPS receiver determines its own location by measuring the time it takes for a signal to arrive at its location from at least four satellites.
- Because radio waves travel at a constant speed, the receiver can use the time measurements to calculate its distance from each satellite.

- How is the distance to the satellite determined with the desirable accuracy? – in theory
  - by measuring the arrival time of the signal from the GPS satellite.
  - This signal carries timing information from the atomic clock on-board the satellite and the measured time delay thus indicates the distance (multiplying the time delay by the speed of light gives the distance).

  Assuming that the distance between a GPS satellite and the GPS receiver is 24,000 km. What is the time delay that would be measured? (The speed of light is 300,000 km/sec)

- If the clocks are perfect sync the satellite range will intersect at a single point.
- But if imperfect the four satellite will not intersect at the same point.
- The receiver looks for a common correction that will make all the satellite intersect at the same point

GPS and IoT

- IoT can collect and quantify large amounts of data for everything from personal health to vehicles; GPS tracking is needed to provide location information for these objects.
- For example,
  - IoT could sense when a driver ends up in a crash or stranded due to vehicle malfunction, but GPS tracking provides the location information that emergency vehicles will need to respond in time.
  - Your house pet may run out the front door without you noticing, but a GPS-capable tag may detect the animal is in distress, so you can quickly locate your pet and bring it back home.

Working

- The GPS consists of three segments:
  - The space segment: the GPS satellites
  - The control system,
  - The user segment, which includes both military and civilian users and their GPS equipment.

User segment

- It consists of receivers that decode the signals from the satellites.
- The receiver performs following tasks:
  - Selecting one or more satellites
  - Acquiring GPS signals
  - Measuring and tracking
  - Recovering navigation data

Control segment

- The control segment of the Global Positioning System is a network of ground stations that monitors the shape and velocity of the satellites' orbits.
- The accuracy of GPS data depends on knowing the positions of the satellites at all times.
- **Monitor Stations** are very precise GPS receivers installed at known locations. They record discrepancies between known and calculated positions caused by slight variations in satellite orbits.

Space segment

- Composed of satellites that transmit signals from space, on the basis of which time and position of the user is measured.
- Set of satellites is called as constellation.
- GPS uses two satellite constellations i.e. NAVSTAR and GLONASS.
- NAVSTAR (Navigation satellite timing and ranging)
- They orbit at altitudes of about 20,200km each.
- Each satellite contains four precise atomic clocks, only one of which is in used at a time.

Threats

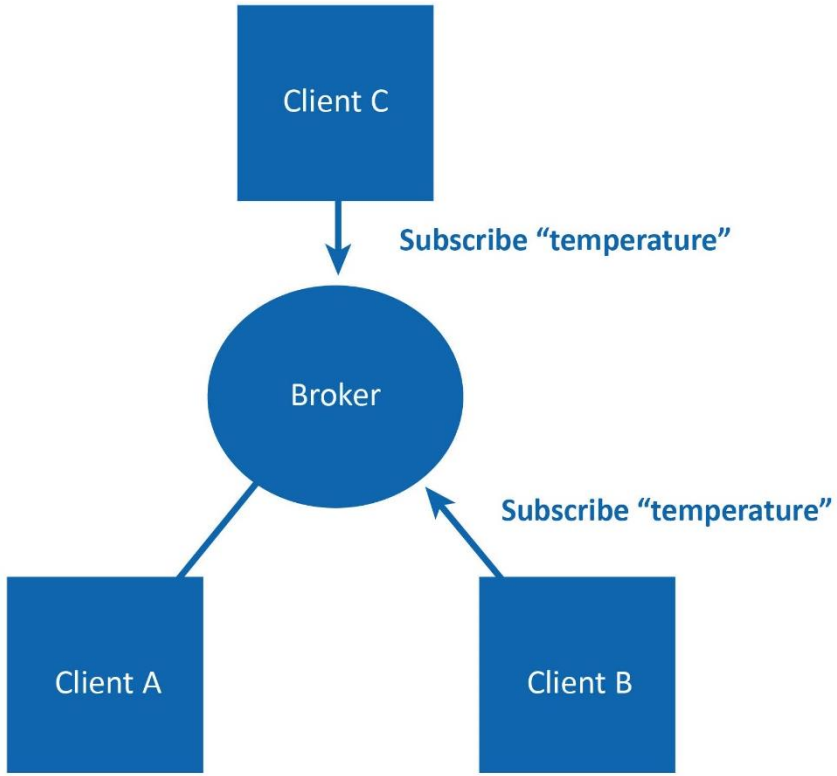
Intentional signal degradation

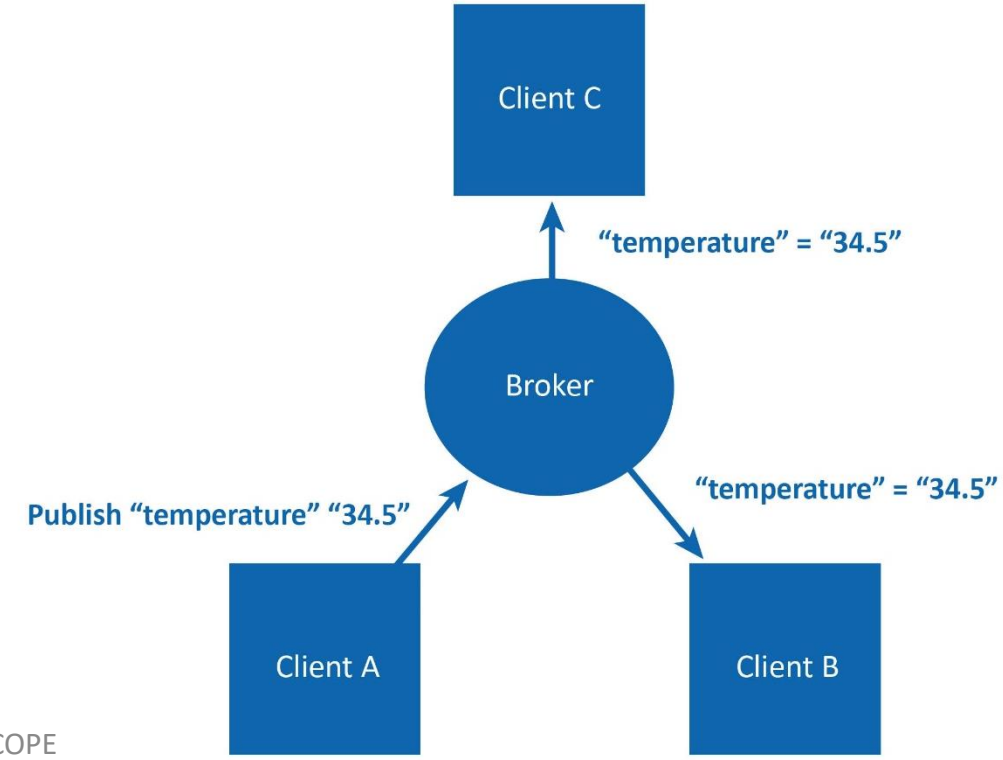
- Selective availability
  - Two components
    - Dither : manipulation of the satellite clock freq
    - Epsilon: errors imposed within the ephemeris data (determine a satellite's position and gives important information about the health of a satellite, current date and time) sent in the broadcast message
- Spoofing
  - Here the P code (code that identifies which satellite is transmitting information) is made un gettable by converting it into the Y code.

MQTT

- MQTT (Message Queuing Telemetry Transport) has gained a lot of prominence in the context of IoT devices.
- MQTT uses the broker–client model.
- MQTT is a lightweight messaging protocol on top of TCP/IP protocol
- MQTT is designed for constrained devices (devices with low memory and network bandwidth) and wireless networks with varying levels of latency due to unreliable connection.
- At the heart of MQTT is the central communication point known as MQTT broker.
- It is responsible for dispersing messages to rightful clients.

- Each client which publishes a message to the MQTT broker includes the routing information, known as topic.
- Clients may subscribe to multiple topics.
- The clients don’t have to know each other to receive information; they just have to subscribe to relevant topics.
- The publisher-subscriber architecture of MQTT makes it a highly scalable solution, without creating dependencies between data producers and consumers.





Topics

- In MQTT, the word topic refers to an UTF-8 string that the broker uses to filter messages for each connected client.
- The topic consists of one or more topic levels.
- Each topic level is separated by a forward slash

- **Topics are case-sensitive.**

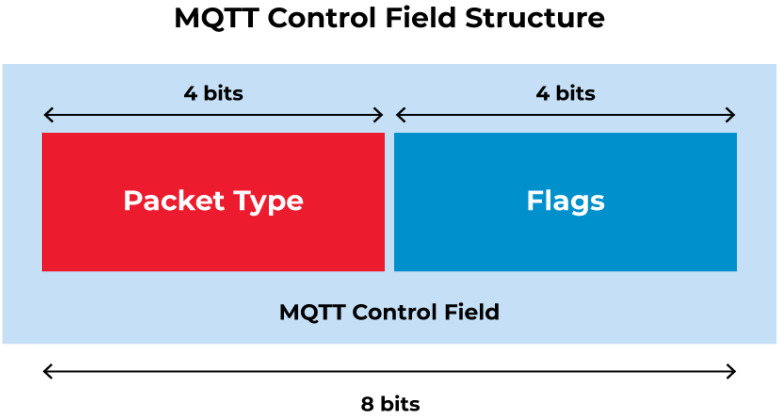
- Wildcards
  - When a client subscribes to a topic, it can subscribe to the exact topic of a published message or it can use wildcards to subscribe to multiple topics simultaneously.
  - A wildcard can only be used to subscribe to topics, not to publish a message.
  - *single-level*

multi-level

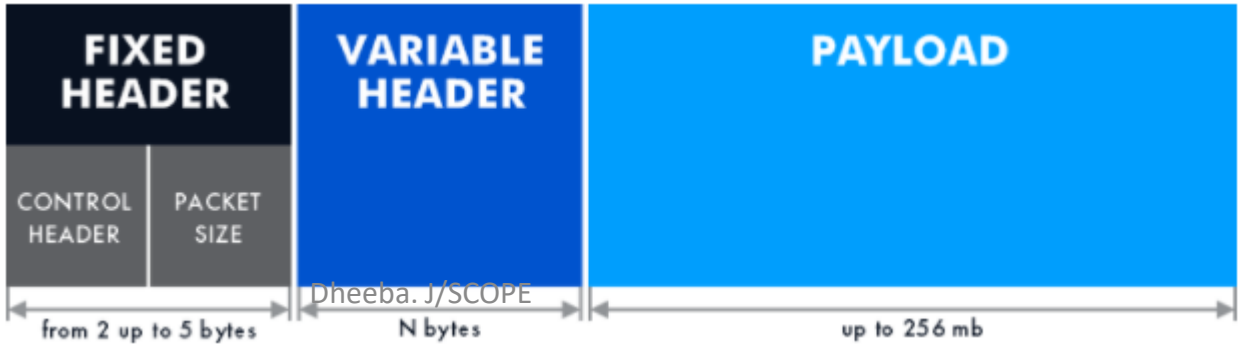
The $-symbol topics are reserved for internal statistics of the MQTT broker. Clients cannot publish messages to these topics.
$SYS/broker/clients/connected
$SYS/broker/messages/sent
$SYS/broker/uptime

Message format of MQTT protocol

- All the messages of MQTT have a small code footprint, hence it is popular as a lightweight messaging protocol.
  - Fixed header (2 bytes) [Control + remaining length]
  - Optional variable header
  - Message payload (<= 256MB)
  - Quality of Service (QoS) level



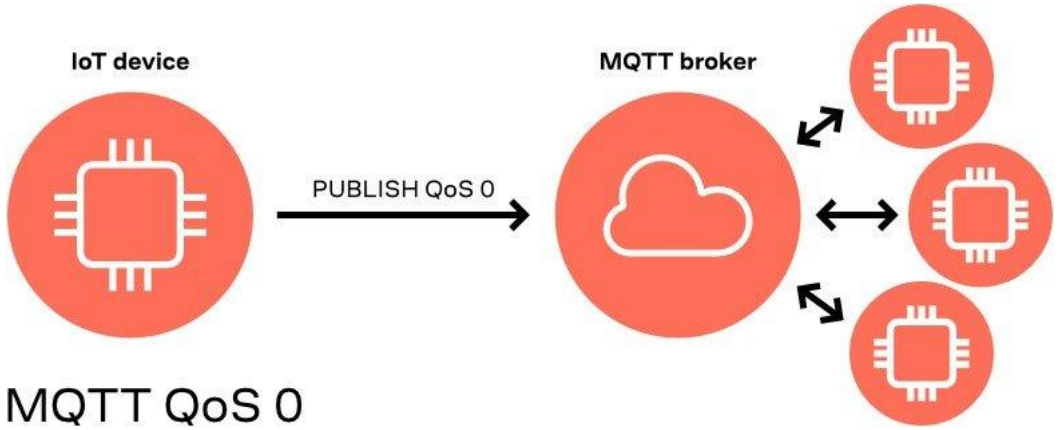
- MQTT supports one-to-one, one-to-many, and many-to-many communication



Quality of Service

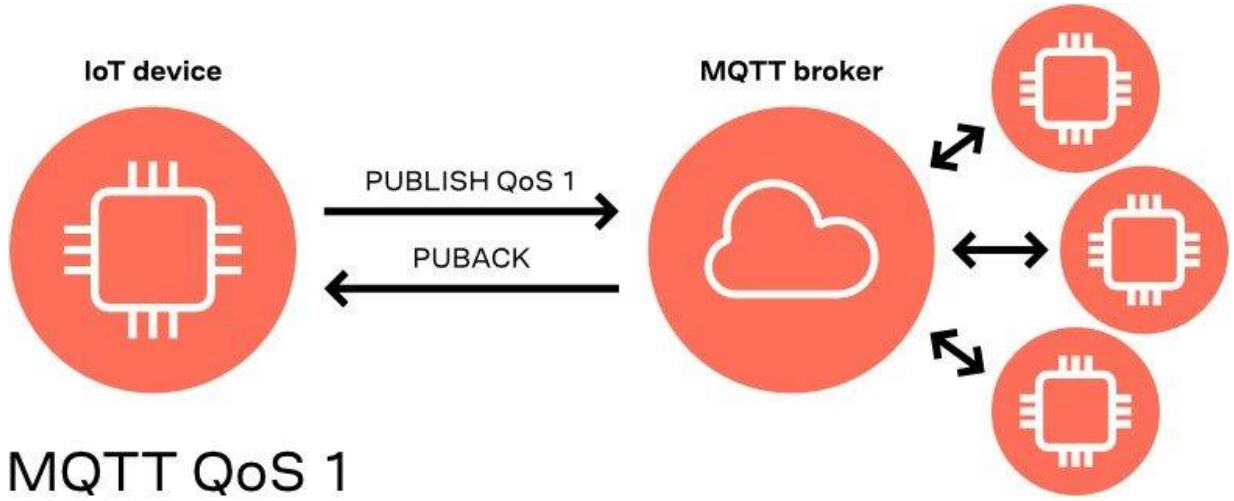
- The **Quality of Service** (QoS) level is an agreement between the sender of a message and the receiver of a message that defines the guarantee of delivery for a specific message.
- There are 3 QoS levels in MQTT:
  - *At most once* (0)
  - *At least once* (1)
  - *Exactly once* (2).
- When you talk about QoS in MQTT, you need to consider the two sides of message delivery:
  - Message delivery form the publishing client to the broker.
  - Message delivery from the broker to the subscribing client.

- The client that publishes the message to the broker defines the QoS level of the message when it sends the message to the broker.
- The broker transmits this message to subscribing clients using the QoS level that each subscribing client defines during the subscription process.
- **QoS 0 - at most once**
  - This service level guarantees a best-effort delivery.
  - There is no guarantee of delivery.
  - The recipient does not acknowledge receipt of the message and the message is not stored and re-transmitted by the sender.
  - QoS level 0 is often called “fire and forget”

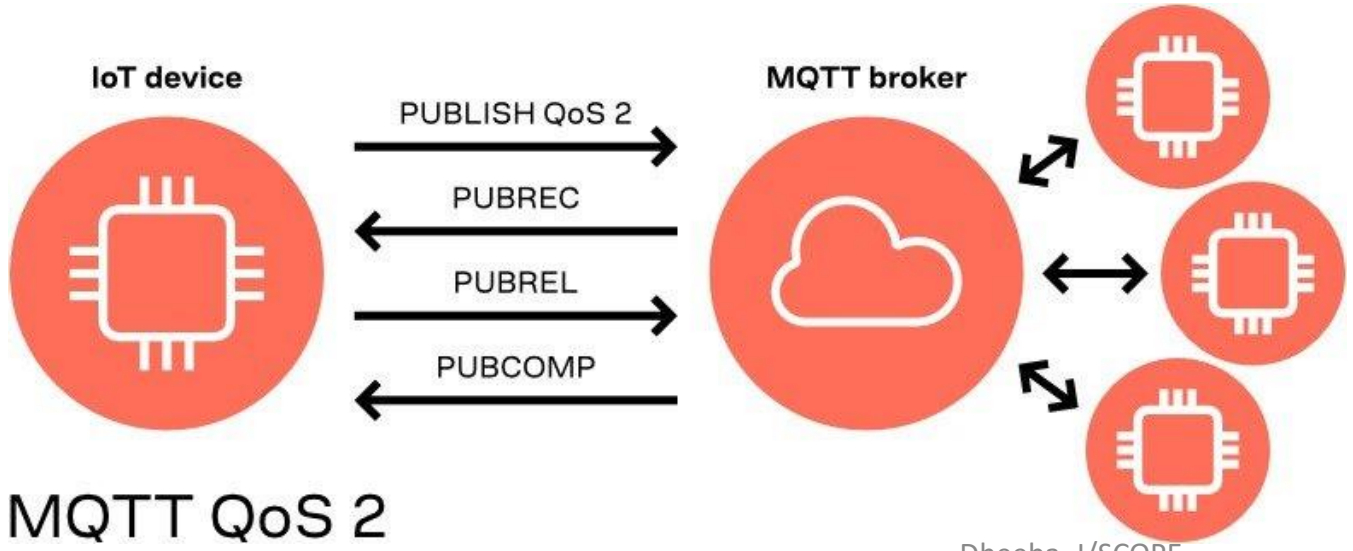


MQTT QoS 0

- **QoS 1 - at least once**
  - QoS level 1 guarantees that a message is delivered at least one time to the receiver.
  - The sender stores the message until it gets a **PUBACK (Publish acknowledgement)** packet from the receiver that acknowledges receipt of the message.
  - It is possible for a message to be sent or delivered multiple times.



- **QoS 2 - exactly once**
  - QoS 2 is the highest level of service in MQTT.
  - This level guarantees that each message is received only once by the intended recipients.
  - QoS 2 is the safest and slowest quality of service level.
  - The guarantee is provided by at least two request/response flows (a four-part handshake) between the sender and the receiver.
  - The sender and receiver use the packet identifier of the original PUBLISH message to coordinate delivery of the message.



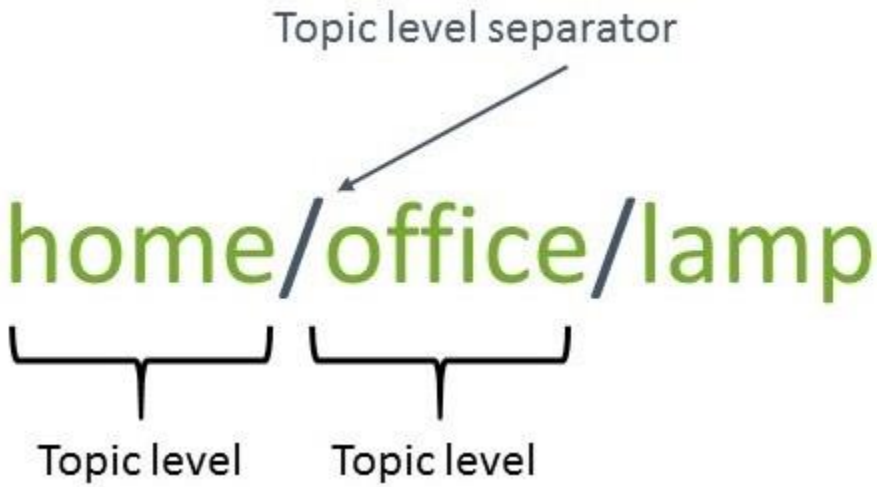
PUBREC - Publish received

PUBREL - Publish release

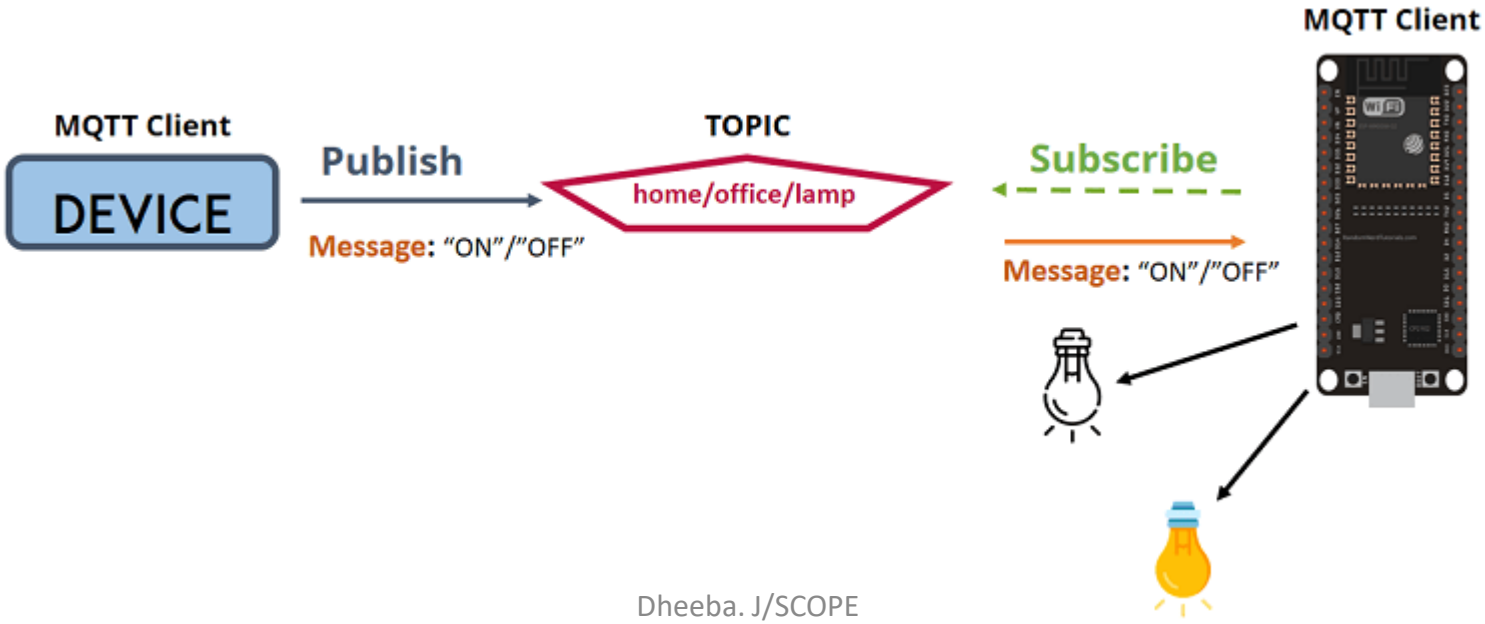
PUBCOMP - Publish Complete

Example

- **MQTT – Topics**
  - **Format**



- You have a device that publishes “on” and “off” messages on the **home/office/lamp** topic.
- You have a device that controls a lamp (it can be an ESP32, ESP8266, or any other board). The ESP32 that controls your lamp, is subscribed to that topic: **home/office/lamp**.
- So, when a new message is published on that topic, the ESP32 receives the “on” or “off” message and turns the lamp on or off.



Why not http?

- HTTP is slower, more overhead and power consuming protocol than MQTT. So, let’s get into each one separately:
- Slower: because it uses bigger data packets to communicate with the server.
- Overhead: HTTP request opens and closes the connection at each request, while MQTT stays online to make the channel always open between the broker “server” and clients.
- Power consuming: since it takes a longer time and more data packets, therefore it uses much power.

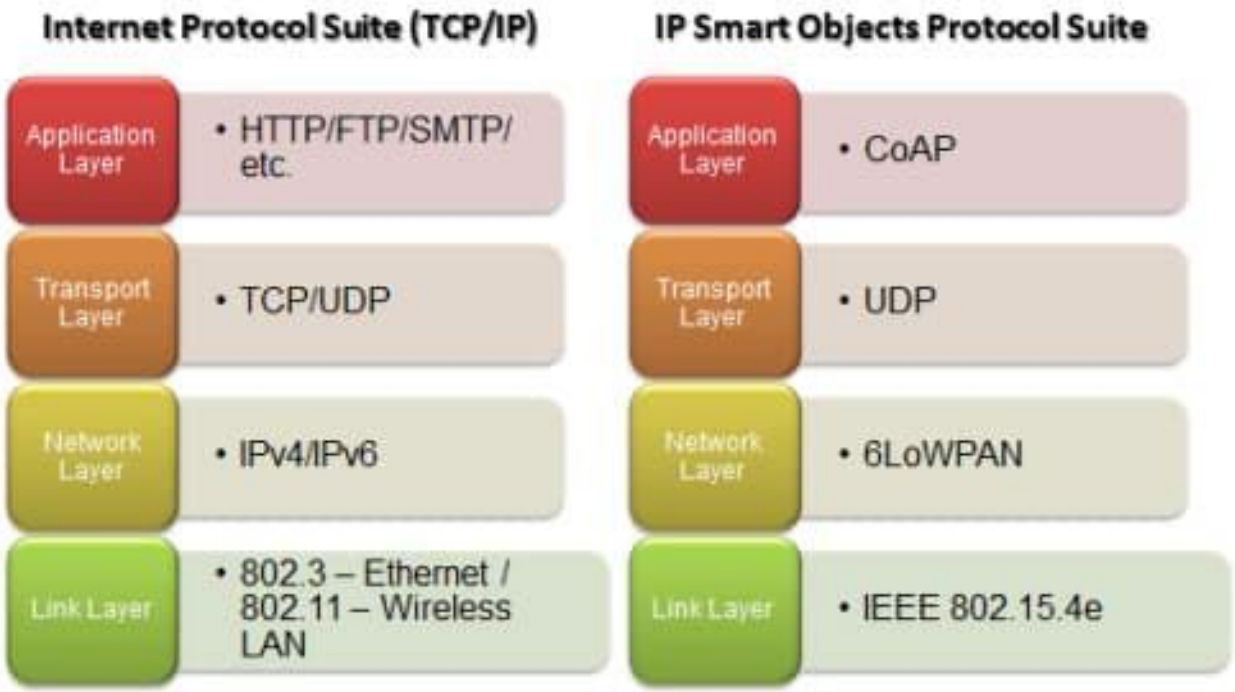
- Cloud-based Mosquitto brokers are many, like:
  - ThingMQ
  - ThingStudio
  - MQTT.io
  - Heroku
  - CloudMQTT

CoAP

- CoAP is an IoT protocol that has interesting features specifically designed for constrained devices.
- CoAP stands for Constrained Application Protocol, and it is defined in RFC 7252.
- CoAP is a simple protocol with low overhead specifically designed for constrained devices (such as microcontrollers) and constrained networks.
- This protocol is used in M2M data exchange and is very similar to HTTP

Features of CoAP protocols

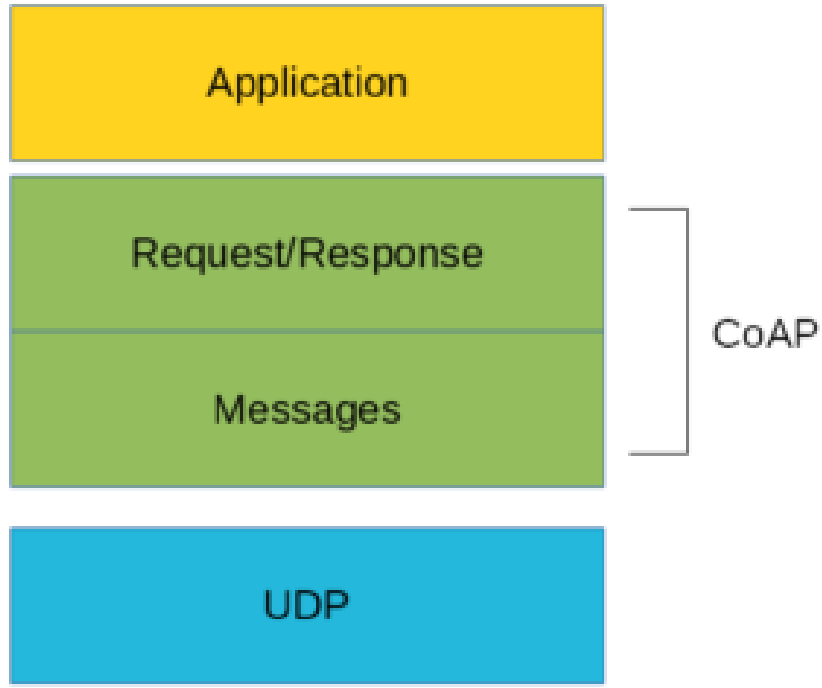
- Web protocol used in M2M with constrained requirements
- Asynchronous message exchange
- Low overhead and very simple to parse
- URI and content-type support
- Proxy and caching capabilities



CoAp protocol: Messages and Request/Response.

- The Messages layer deals with UDP and with asynchronous messages.
- The Request/Response layer manages request/response interaction based on request/response messages.

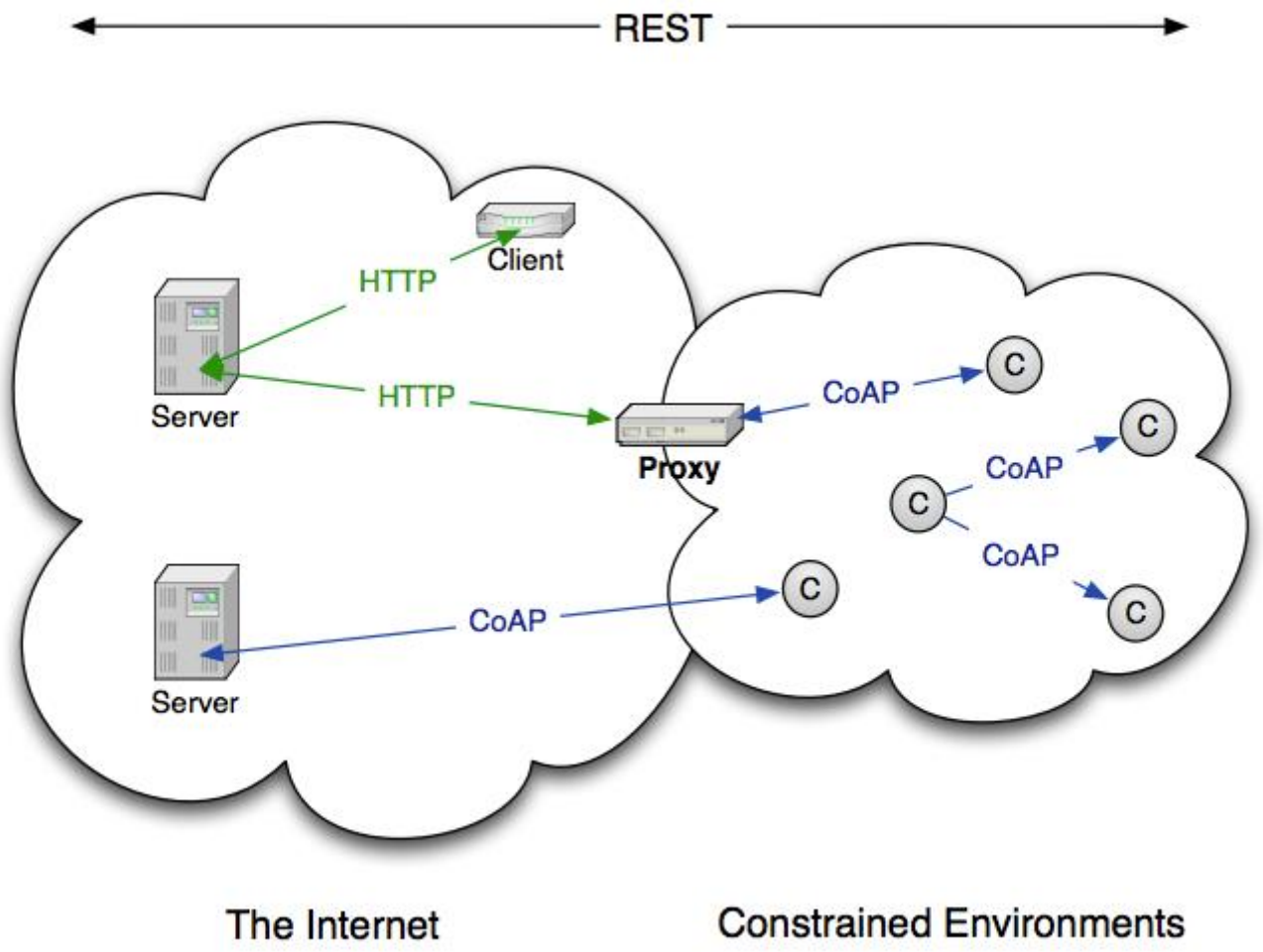
Abstraction protocol layer, CoAP can be represented as

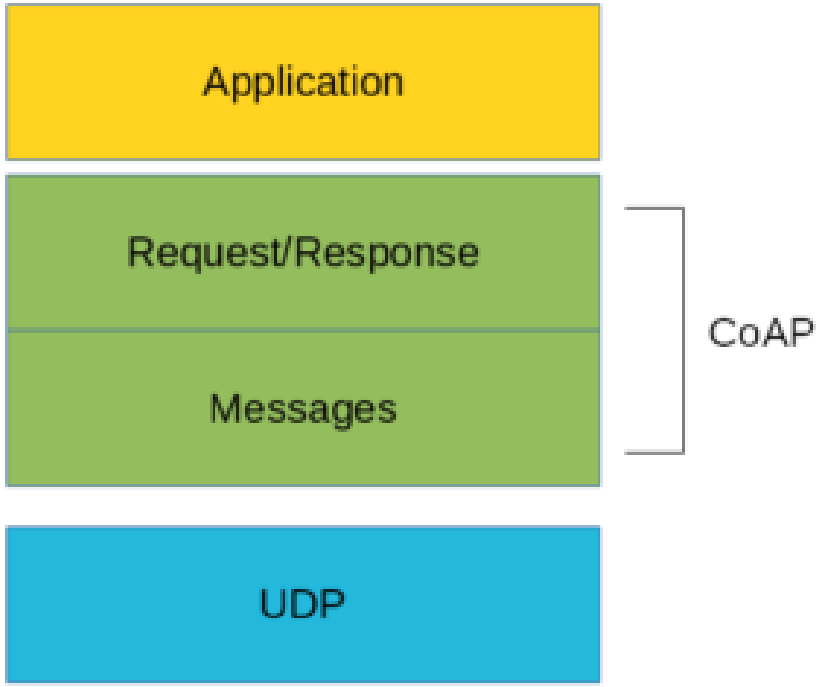


Terminology

- **Endpoint**: An entity that participates in the CoAP protocol. Usually, an Endpoint is identified with a host
- **Sender**: The entity that sends a message
- **Recipient**: The destination of a message
- **Client**: The entity that sends a request and the destination of the response
- **Server**: The entity that receives a request from a client and sends back a response to the client

Architecture

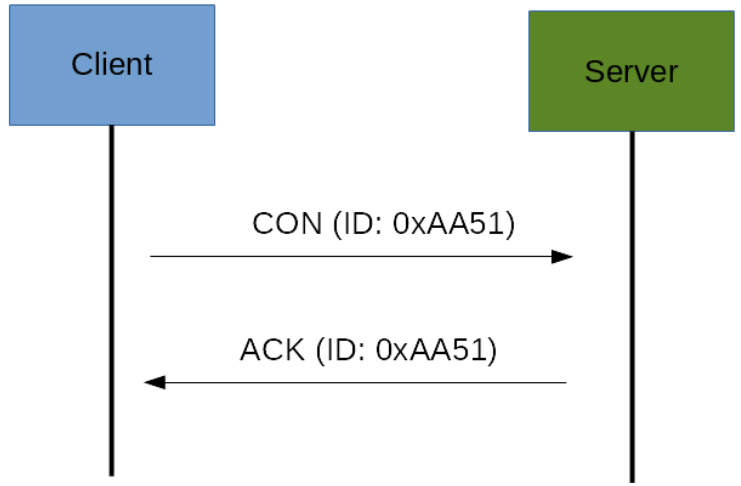




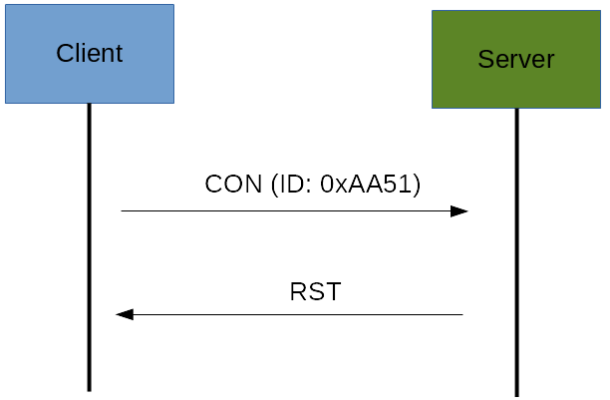
- CoAP supports four different message types:
  - Confirmable
  - Non-confirmable
  - Acknowledgment
  - Reset
- This is the lowest layer of CoAP, Deals with UDP exchanging messages between endpoints.
- CoAP message has a unique ID; this is useful to detect message duplicates.
  - A binary header
  - A compact options
  - Payload

CoAP Messages Model

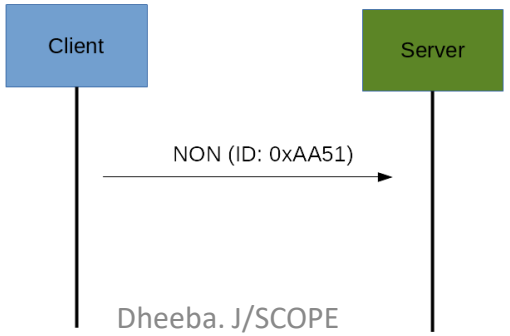
- A confirmable message (CON) is a reliable message. When exchanging messages between two endpoints, these messages can be reliable.
- Using this kind of message, the client can be sure that the message will arrive at the server.
- A Confirmable message is sent again and again until the other party sends an acknowledge message (ACK). The ACK message contains the same ID of the confirmable message (CON).



- If the server has troubles managing the incoming request, it can send back a Reset message (RST) instead of the Acknowledge message (ACK).



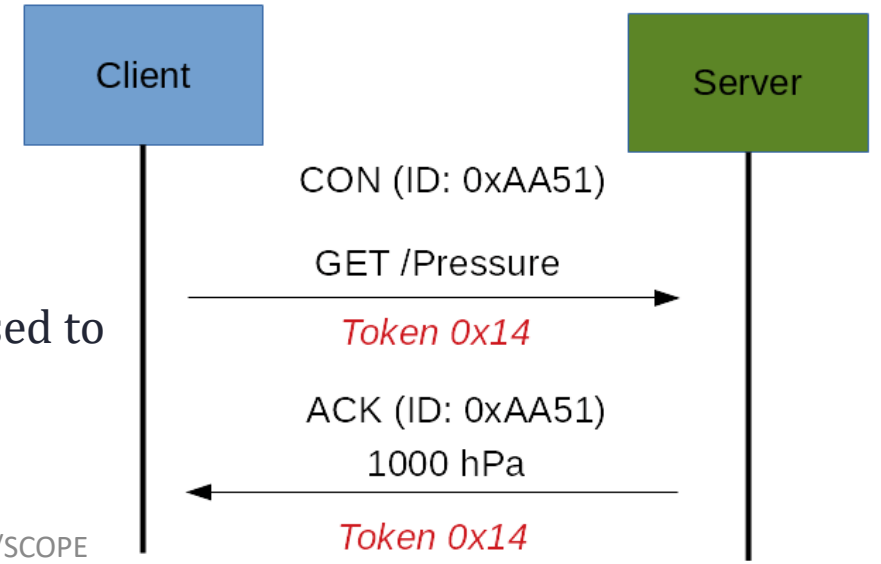
- The other message category is the Non-confirmable (NON) messages
- These are messages that don't require an Acknowledge by the server.
- They are unreliable messages or in other words messages that do not contain critical information that must be delivered to the server.



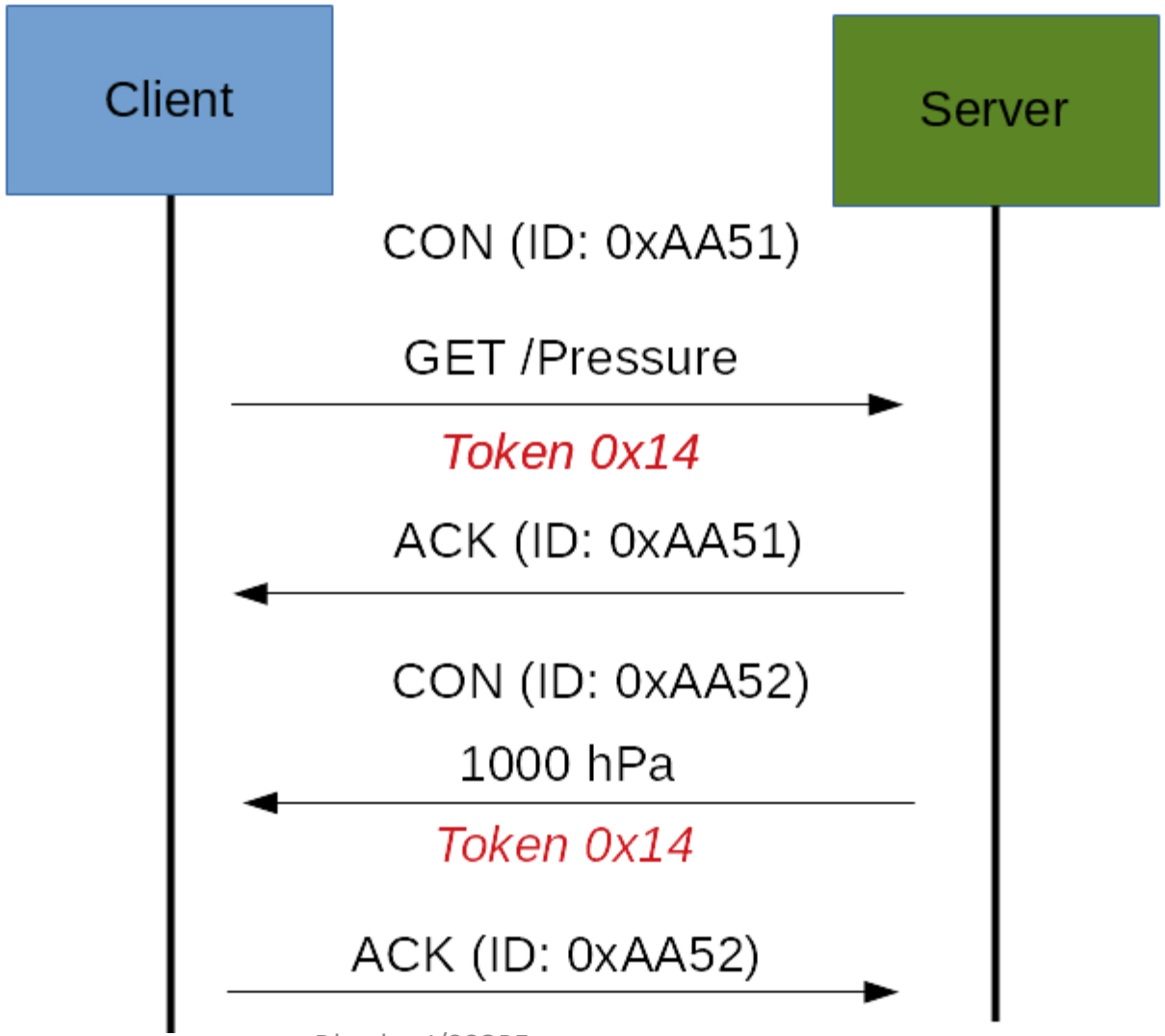
CoAp Request/Response Model

- CoAP Request/Response is the second layer in the CoAP abstraction layer.
- The request is sent using a Confirmable (CON) or Non-Confirmable (NON) message.
- Case 1 - If the server can answer immediately to the client request, then if the request is carried using a Confirmable message (CON), the server sends back to the client an Acknowledge message containing the response or the error code

The Token is different from the Message-ID and it is used to match the request and the response.

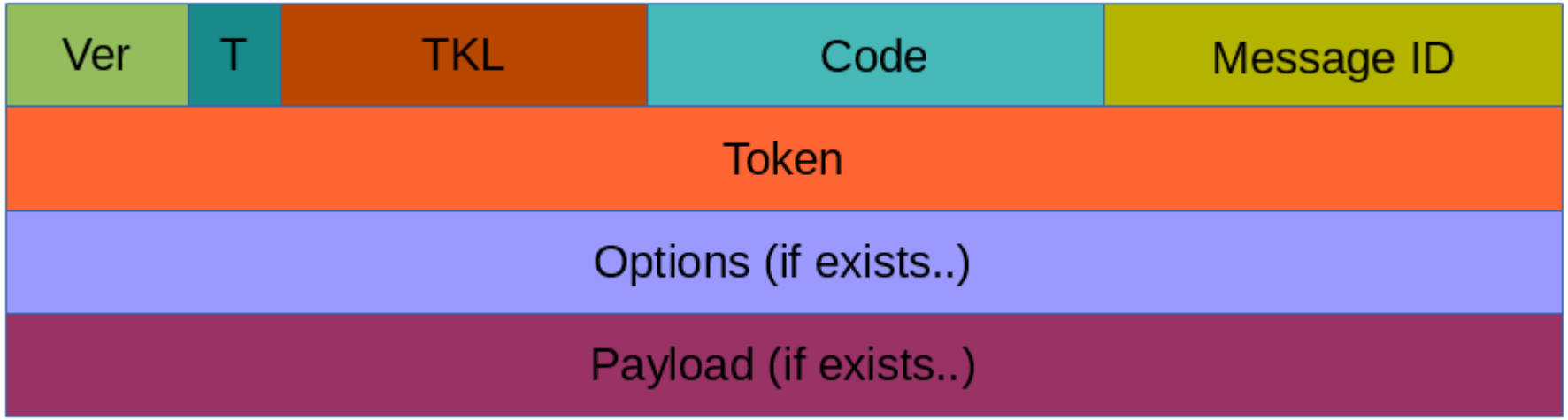


Case 2 - server can't answer to the request coming from the client immediately,



CoAp Message Format

- Constrained environments - it uses compact messages



- **Ver**: It is a 2 bit unsigned integer indicating the version
- **T**: it is a 2 bit unsigned integer indicating the message type: 0 confirmable, 1 non-confirmable
- **TKL**: Token Length is the token 4 bit length
- **Code**: It is the code response (8 bit length) - Request Method (1-10) or Response Code (40-255)
- **Message ID**: It is the message ID expressed with 16 bit (identifier for matching responses)

CON	00(0)	ACK	10(2)
NON	01(1)	RST	11(3)

CoAP Security Aspects

- As HTTP uses TLS over TCP, CoAP uses *Datagram TLS over UDP.*
- DTLS supports RSA, AES, and so on
- **Alternate protocols**
  - MQTT uses a publisher-subscriber while CoAP uses a request-response paradigm.
  - MQTT uses a central broker to dispatch messages coming from the publisher to the clients.
  - CoAP is essentially a one-to-one protocol very similar to the HTTP protocol

6LoWPAN

6LoWPAN

- 6LoWPAN system is used for a variety of applications including wireless sensor networks.
- Sends data as packets and using IPv6 - providing the basis for the name - IPv6 over Low power Wireless Personal Area Networks.
- Provides a means of carrying packet data in the form of IPv6 over IEEE 802.15.4 and other networks.
- Open standard defined by the Internet Engineering Task Force

- The direct IPv6 support is suitable for a dense 6LoWPAN because of the large IPv6 address space
- 6LoWPAN can make IoT and devices connect to other IP networks
- Also, it allows us to use popular tools and protocols running on top of IP technologies.
- Low-power, IP-driven nodes and large mesh network support make this technology a great option for Internet of Things (IoT) applications

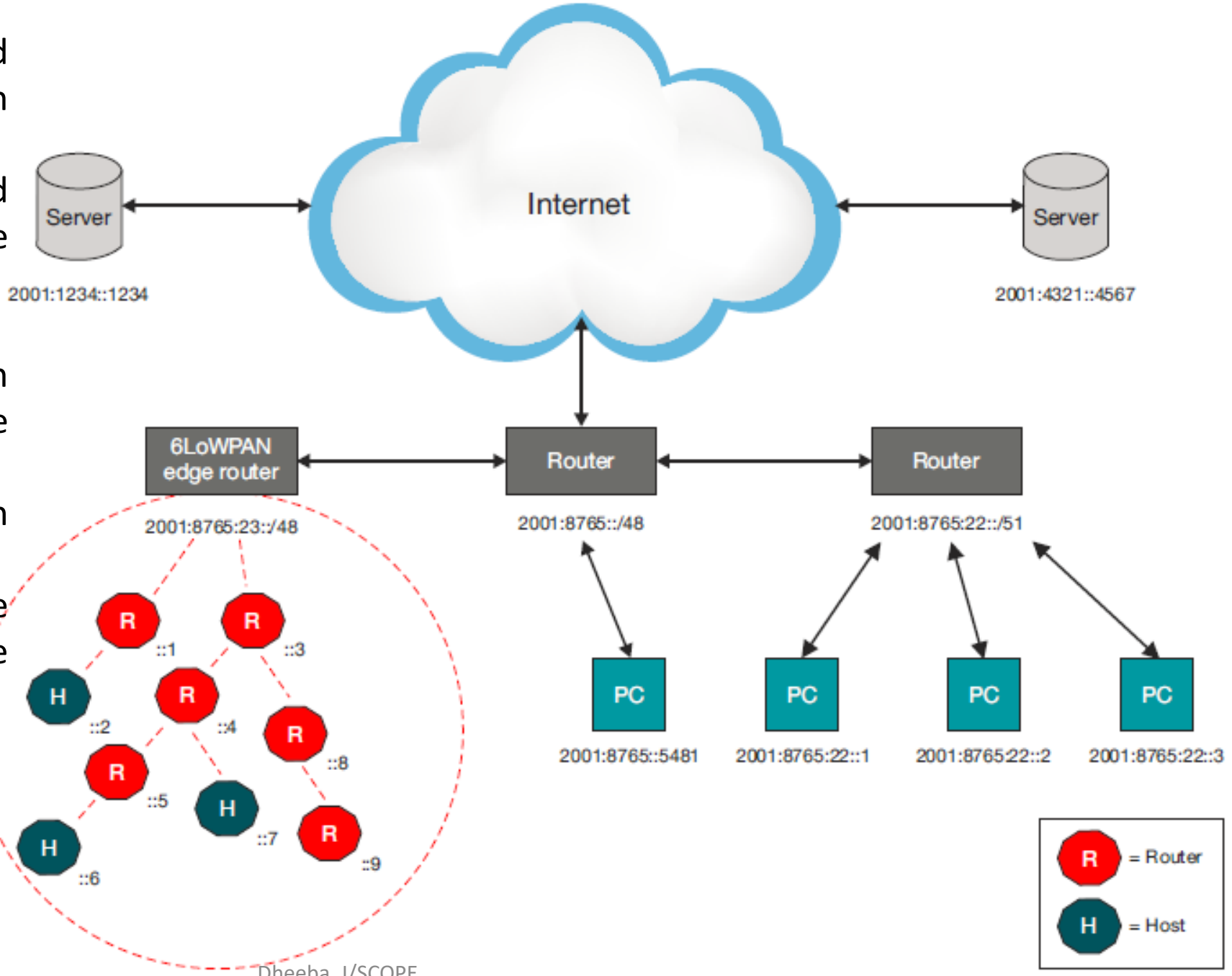
- Issues - mismatch between IP package size and the IEEE 802.15.4 package size. The other is the efficient routing schemes for mesh networking which is not directly supported by IEEE 802.15.4
- So, the solution is to create a sublayer

The uplink to the Internet is handled by the Access Point (AP) acting as an IPv6 router

The 6LoWPAN network is connected to the IPv6 network using an edge router

Edge router handles three actions

1) the data exchange between 6LoWPAN devices and the Internet (or other IPv6 network)
2) Local data exchange between devices inside the 6LoWPAN
3) the generation and maintenance of the radio subnet (the 6LoWPAN network).

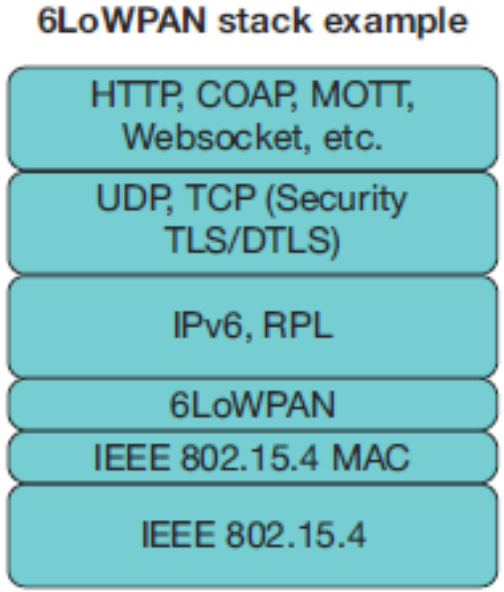


- 6LoWPAN networks will typically operate on the edge, acting as stub networks.
- This means data going into the network is destined for one of the devices inside the 6LoWPAN.
- One 6LoWPAN network may be connected to other IP networks through one or more edge routers that forward IP datagrams between different media.
- Connectivity to other IP networks may be provided through any arbitrary link, such as Ethernet, Wi-Fi or 3G/4G. Because 6LoWPAN only specifies operation of IPv6 over the IEEE 802.15.4 standard

- Two other device types are included inside a typical 6LoWPAN network: routers and hosts.
- Routers can, as the name implies, route data destined to another node in the 6LoWPAN network.
- Hosts are also known as end devices and are not able to route data to other devices in the network.
- Host can also be a sleepy device, waking up periodically to check its parent (a router) for data, enabling very low power consumption.

System stack overview

- a complex application layer gateway was needed to make devices such as ZigBee, Bluetooth and proprietary systems connect to the Internet.
- 6LoWPAN solves this dilemma by introducing an adaptation layer between the IP stack's link and network layers to enable transmission of IPv6 datagrams over IEEE 802.15.4 radio links.



- The physical layer converts data bits into signals that are transmitted and received over the air.
- The data link layer provides a reliable link between two directly connected nodes by detecting and correcting errors that may occur in the physical layer during transmission and receiving.
- The data link layer includes the media access layer (MAC) which provides access to the media, using features like carrier sense multiple access – collision avoidance (CSMA-CA) where the radio listens that no one else is transmitting before actually sending data over the air.
- This layer also handles data framing.

- The 6LoWPAN adaptation layer, providing adaptation from IPv6 to IEEE 802.15.4, also resides in the link layer.
- The network layer addresses and routes data through the network, if needed over several hops.
- IP (or Internet Protocol) is the networking protocol used to provide all devices with an IP address to transport packets from one device to another.

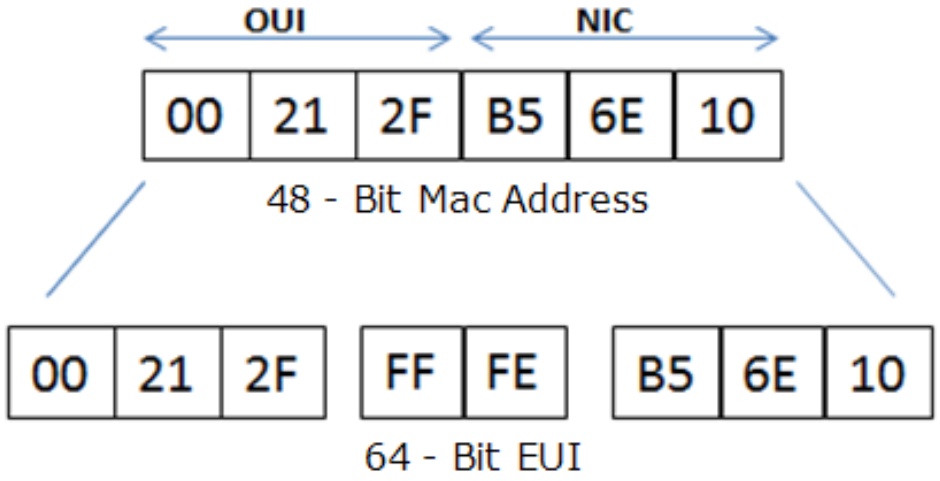
- The transport layer generates communication sessions between applications running on end devices.
- The transport layer allows multiple applications on each device to have their own communications channel.
- TCP is the dominant transport protocol on the Internet.
- However, TCP is a connection-based protocol (including packet ordering) with large overhead and therefore not always suitable for devices demanding ultra-low power consumption.
- For those types of systems, UDP, a lower overhead, connectionless protocol, can be a better option

- Finally, the application layer is responsible for data formatting. It also makes sure that data is transported in application-optimal schemes.
- A broadly used application layer on the Internet is HTTP running over TCP.
- HTTP uses XML, which is a text-based language with a large overhead.
- Therefore, it is not optimal to use HTTP in many 6LoWPAN systems.
- For this reason, the industry and community have developed alternative application layer protocols, such as the constrained application protocol (COAP), a message protocol running over UDP with a bit-optimized REST mechanism very similar to HTTP.
- Message queue telemetry transport (MQTT), an open-source protocol that was invented by IBM.
- MQTT is a publish/subscribe type of protocol running over TCP.
- Data is not transported directly between end points. Instead a broker (i.e., server) is used to relay messages

Internet Protocol version 6 (IPv6) over IEEE 802.15.4

- IPV4 addressing limits to 4,294,967,296 unique addresses and got exhausted in 2011.
- This limitation of IPv4 stimulated the development of IPv6 in the 1990s, which has been in commercial deployment since 2006.
- IPv6 covers an address space of 2^{128} unique addresses.
- To recognize the increase in bandwidth, IPv6 increases the minimum maximum transmission unit (MTU) from 576 to 1280 bytes.
- Both Ethernet and Wi-Fi operate in the context of ample power and highly capable devices.
- IEEE 802.15.4 was designed to serve - long-lived applications that require large numbers of low-cost, ultra-lowpower devices.
- The throughput under this standard is limited to 250 kbps, and the frame length is limited to 127 bytes to ensure low packet and bit error rates in a lossy RF environment.

- Additionally, IEEE 802.15.4 uses two addresses: a 16-bit short address and an EUI-64 extended address (Extended Unique Identifier).
- The IPv6 EUI-64 format address is obtained through the 48-bit MAC address. The MAC address is first separated into two 24-bits, with one being OUI (Organizationally Unique Identifier) and the other being NIC specific. The 16-bit 0xFFFE is then inserted between these two 24-bits for the 64-bit EUI address.



- 6LoWPAN operates most commonly over multiple hops forming a low-power mesh network, a fundamental difference from Ethernet- or Wi-Fi-based networks.
- Finally, devices used to implement 6LoWPAN are typically constrained in terms of resources, having about 16 kB RAM and 128 kB ROM.

Routing

- Routing is the ability to send a data packet from one device to another device, sometimes over multiple hops.
- two categories of routing are defined: mesh-under or route-over.
  - mesh-under
    - Mesh-under networks are best suited for smaller and local networks.
    - Mesh-under uses the layer-two (link layer) addresses (IEEE 802.15.4 MAC or short address) to forward data.
    - The only IP router in such a system is the edge router.
  - route-over
    - Route-over uses layer three (network layer) addresses (IP addresses).
    - The most widely used routing protocol for route-over 6LoWPAN networks today is RPL
    - **Uses RPL** (**Routing Protocol** for Low-Power and Lossy Networks) is a **routing protocol** for wireless networks with low power consumption and generally susceptible to packet loss.

RPL

- Provides a mechanism whereby multipoint-to-point traffic from devices inside the 6LoWPAN network towards a central control point (e.g., a server on the Internet) as well as point-to-multipoint traffic from the central control point to the devices inside the 6LoPWAN are supported.
- RPL supports two different routing modes; storing mode and non-storing mode.
- In storing mode, all devices in the 6LoWPAN network configured as routers maintain a routing table and a neighbor table.
- The routing table is used to look up routes to devices, and the neighbor table is used to keep track of a node's direct neighbors.

- In the non storing mode the only device with a routing table is the edge router, hence source routing is used
- The packet includes the complete route (or hops) it needs to take to reach the destination.
- For example, when sending data from one device to another device inside the same 6LoWPAN network, data is first sent from the source device to the edge router the edge router in turn makes a lookup in its routing table and adds the complete route to the destination in the packet;
- Storing mode imposes higher requirements on the devices acting as routers (i.e., they need to have resources enough to store the routing and neighbor tables), while using non storing mode the overhead increases with the number of hops a packet needs to traverse to reach the destination.

Auto configuration and neighbor discovery

- Similar to Neighbor discovery protocol
- In IPv6 it allows a device to automatically generate its IPv6 address without any outside interaction with a DHCP server or such.
- Involves four message types:
  - Router solicitation (RS)
  - Router advertisement (RA)
  - Neighbor solicitation (NS)
  - Neighbor advertisement (NA)

- IPv6 neighbor discovery (ND) lets a device discover neighbors, maintain reachability information, configure default routes, and propagate configuration parameters.
- The RS message includes, among other things, the IPv6 prefix of the network.
- All routers in the network periodically send out these messages.
- If a host wants to participate in a 6LoWPAN network, it assigns itself a link-local unicast address (FE80::IID), then sends this address in an NS message to all other participants in the subnet to check if the address is being used by someone else.
- If it does not hear an NA message within a defined timeframe, it assumes that the address is unique.
- This procedure is called duplicate address detection, DAD.

- Now, to get the network prefix, the host sends out an RS message to the router to get the correct prefix.
- Using these four messages, a host is able to assign itself a worldwide unique IPv6 address.
- Each host generates a link-local IPv6 address using its IEEE 802.15.4 EUI-64 address, 16-bit short address or both.

RPL

- Low Power and Lossy Networks (LLNs) are composed by nodes with constrained energy, memory, and processing capacity.
- Wireless Sensor Networks (WSNs) are a kind of LLN in which nodes collect data from sensors and send it to the base stations or sinks.
- in smart object networks consisting of battery-powered nodes, the act of communication consumes energy and nodes that communicate more frequently drain their energy faster.
- LLNs are known to be lossy - loss of connectivity
- Routing in LLNs should be able to self manage - For example, it is not possible for a system administrator to assign an address manually or be able to enter passwords for accessing the network (IPV6 addressing)

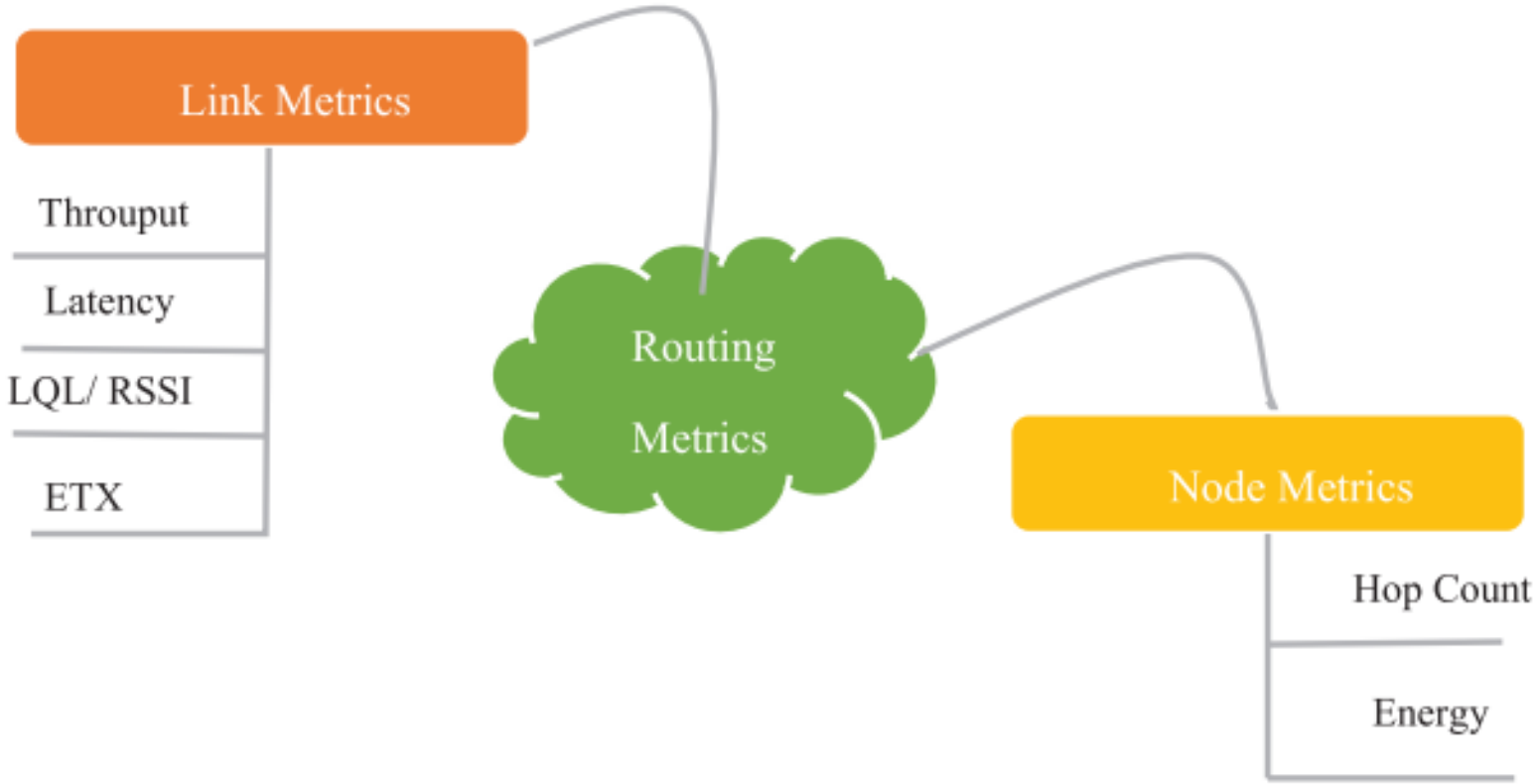
DODAG Building Process

- RPL is a Distance Vector IPv6 routing protocol for LLNs that specifies how to build a Destination Oriented Directed Acyclic Graph (DODAG) using an objective function and a set of metrics/constraints.
- The objective function operates on a combination of metrics and constraints to compute the 'best' path. (for example, the number of parents, back-up parents, use of load-balancing)
- RPL constructs one or more base routing topologies, in the form of DAGs, over gradients defined by optimizing cost metrics along paths rooted at designated nodes.
- DAGs may be grounded, in which case the DAG Root (e.g. an LBR) is offering a default route to an external routed infrastructure such as the Internet.
- The graph building process starts at the root or LBR (LowPAN Border Router), which is configured by the system administrator. (A typical goal for a node participating in DAG Construction may be to find and join a grounded DAG.)

- ICMPv6 control messages
  - DIS (DODAG Information Solicitation)
  - DIO (DODAG Information Object)
  - DAO (DODAG Destination Advertisement Object).

- First, it uses the DODAG Information Object (DIO) to preserve the current rank of the node and calculate the distance between node and root used for selecting the preferred parent.
- Second, it transmits the Destination Advertisement Object (DAO) in upward traffic towards the selected parents.
- Third, it sends the DODAG Information Solicitation (DIS) to solicit DIO messages from a joinable node.
- And finally, the DAO-ACK message which represents an acknowledgement of the reception of DAO message is sent by DAO receiver

- In the context of a particular LLN application one or more nodes will be capable of, e.g. serving as an LBR or acting as a data collection point, and thus be provisioned to act as the most preferred DAG roots.
- These nodes will begin the process of constructing a DAG by occasionally emitting Router Advertisements.
- The root starts advertising the information about the graph using the DIO message.
- DIO - DAGID, a DAGPreference, and an Objective Code Point (OCP)
  - identifier unique to the DAG
  - providing a mechanism by which the DAG may look attractive for other nodes to join
  - provides information as to which metrics and optimization goals are being employed across the DAG
- Links are annotated with ETX (Expected Transmission Count - will help the RPL nodes to use more reliable paths to reach the root)
- Objective Code Point (the least cost path may be determined in part by minimizing energy along a path, or latency, or avoiding the use of battery powered nodes)
  - Metric: ETX
  - Objective: Minimize ETX



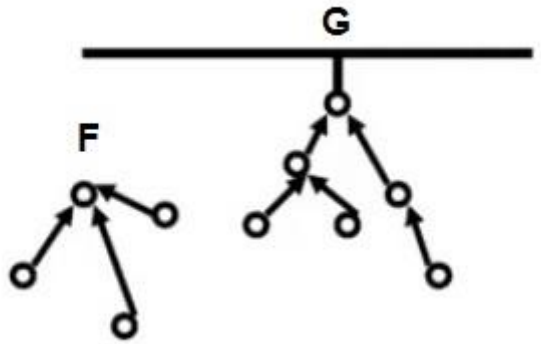
Received Signal Strength Indicator (RSSI)
Link Quality Indicator (LQI) (Range 0 to 7)
Expected Transmission Count (ETX)

Terminology

- **Directed Acyclic Graph :**
- It is a Graph that contains no cycle (Figure 1), we see such kind of graphs in Spanning trees.
- **Root** : it is the destination of the nodes in DAG, it has no outgoing edge.
- **Up** : It is any edge that is directed towards the Root (Figure 2).
- **Down** : It is any edge which is directed away from root.
- **Destination Oriented DAG (DODAG)** : This a special kind of DAG where each node wants to reach a single destination

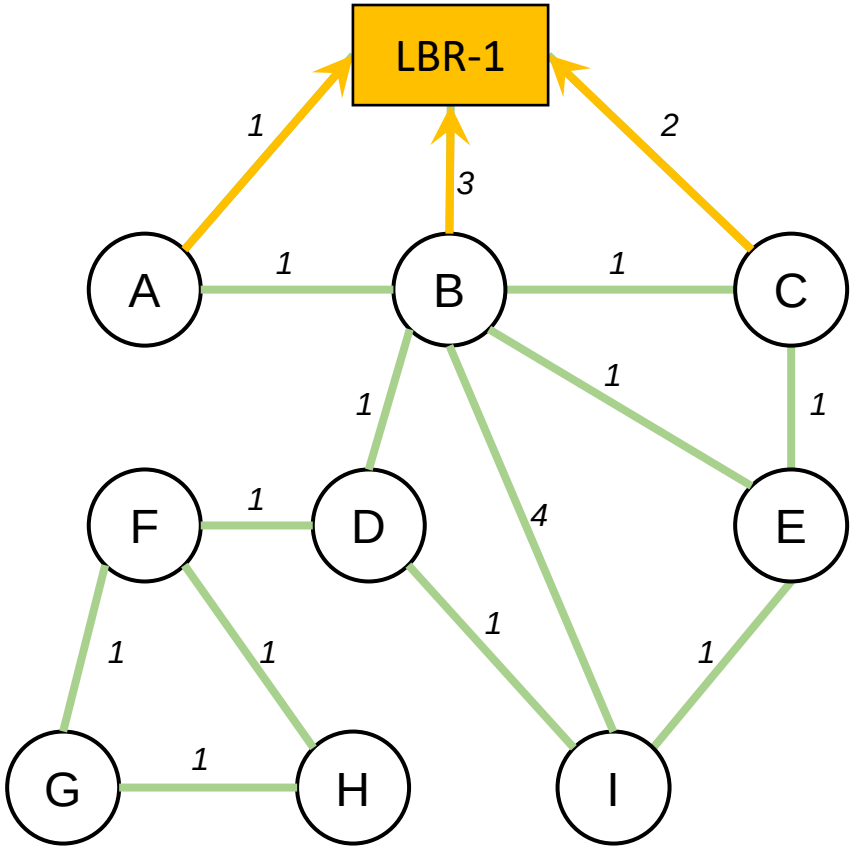
- **Objective Function** : It helps us to decide whether we are near to the root or away from it. Objective Function is decided by a programmer or designer . It is something which we want to minimize. It can be energy, it can be Latency. And once we decide what we want to minimize, we give it a Number.
- **Rank** : it is the distance from Root.
- **RPL instance**: When we have one or More DODAGs, then each DODAG is an instance. Figure 3 shows two RPL instances.
- **DODAG ID** : Each DODAG has an IPv6 ID (128 bit). This ID is given to its root only. And as long as the root doesn’t change ID also doesn’t change.
- **DODAG Version**: Each new shape Of a DODAG means a new version.
- **GOAL**: It is where a DODAG wants to reach, it can be a Wired network. Goal is different that Objective function. In objective function our aim is to minimize. However Goal is where we want to go.

- **Grounded** : When a DODAG reaches its goal it is known as Grounded. G in Figure shows Grounded DODAG.
- **Floating**: When a DODAG isn’t connected, or is yet to reach the Goal, it is called Floating. F in Figure Shows Floating DODAG



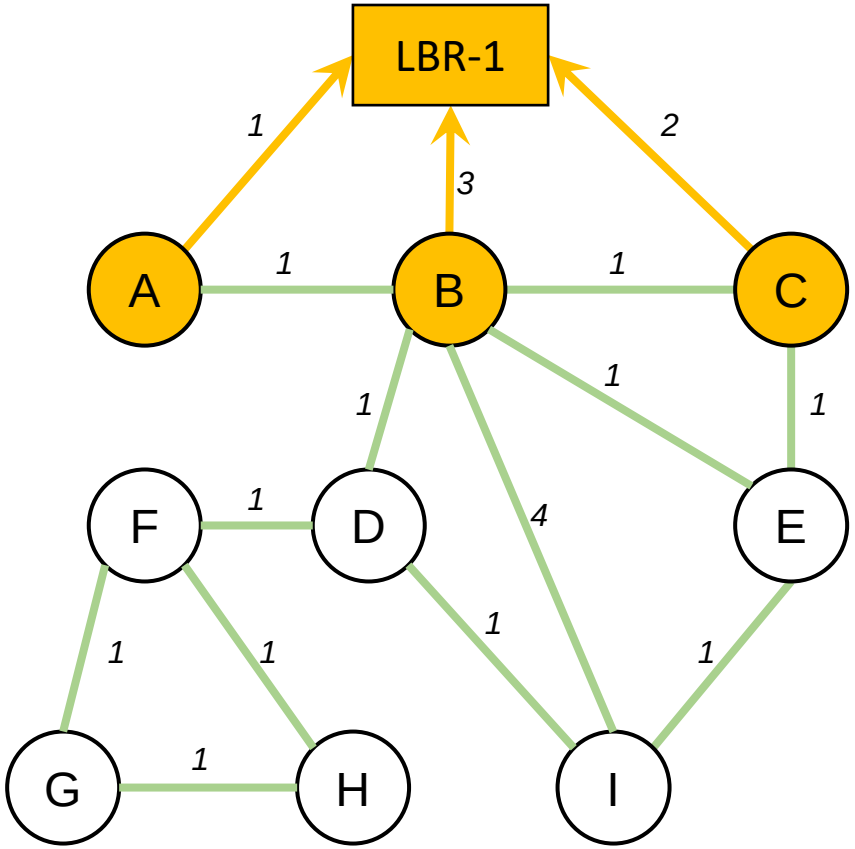
- **Parent**: Parent is where the Arrow is pointing towards. And a Child is where the arrow comes from. Parents can have multiple children, Similarly a child can have Multiple parents.
- **Sub-DODAG** : It is any subtree of a given DODAG.
- **Storing** : Storing nodes keep the whole routing table. They know how to go from one node to another.
- **Non-Storing** : They are simple, they don’t store an entire Routing Table, they only know about their Parents.

DAG Construction

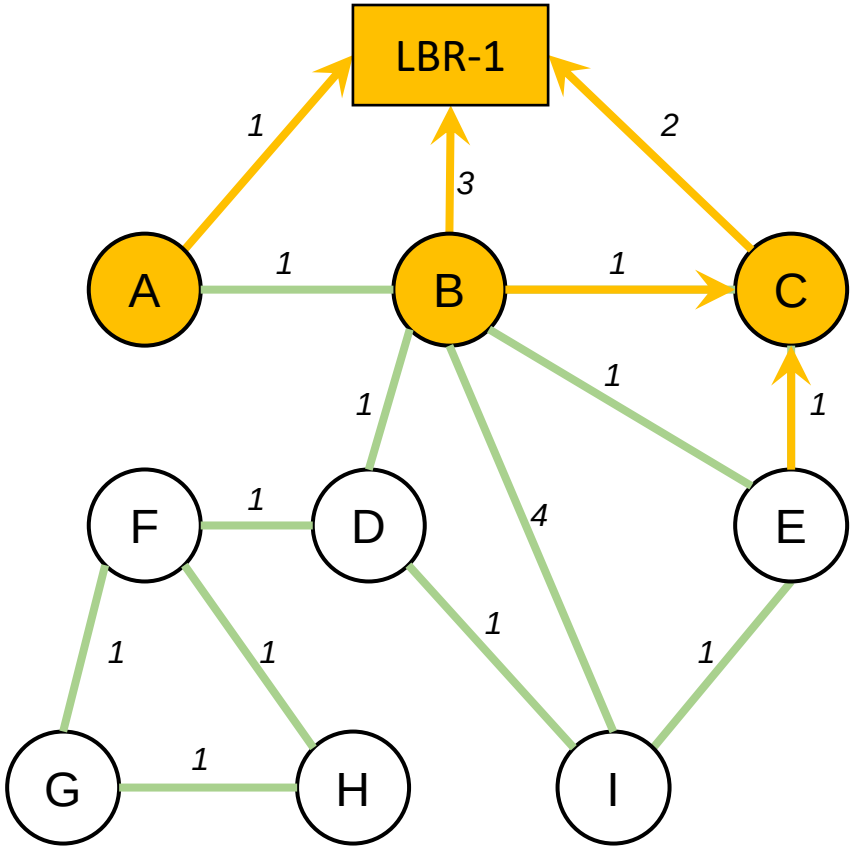


- LBR-1 multicasts Router advertisement, RA-DIO
- Nodes A, B, C receive and process RA-DIO
- Nodes A, B, C consider link metrics to LBR-1 and the optimization objective
- The optimization objective can be satisfied by joining the DAG rooted at LBR-1
- Nodes A, B, C add LBR-1 as a DAG parent and join the DAG
- When a node adds the first DAG parent to the set of DAG parents for a particular DAGID, the node is said to have joined, or attached to, the DAG designated by DAGID
- Nodes A, B, C have installed default routes (::/0) with LBR-1 as successor

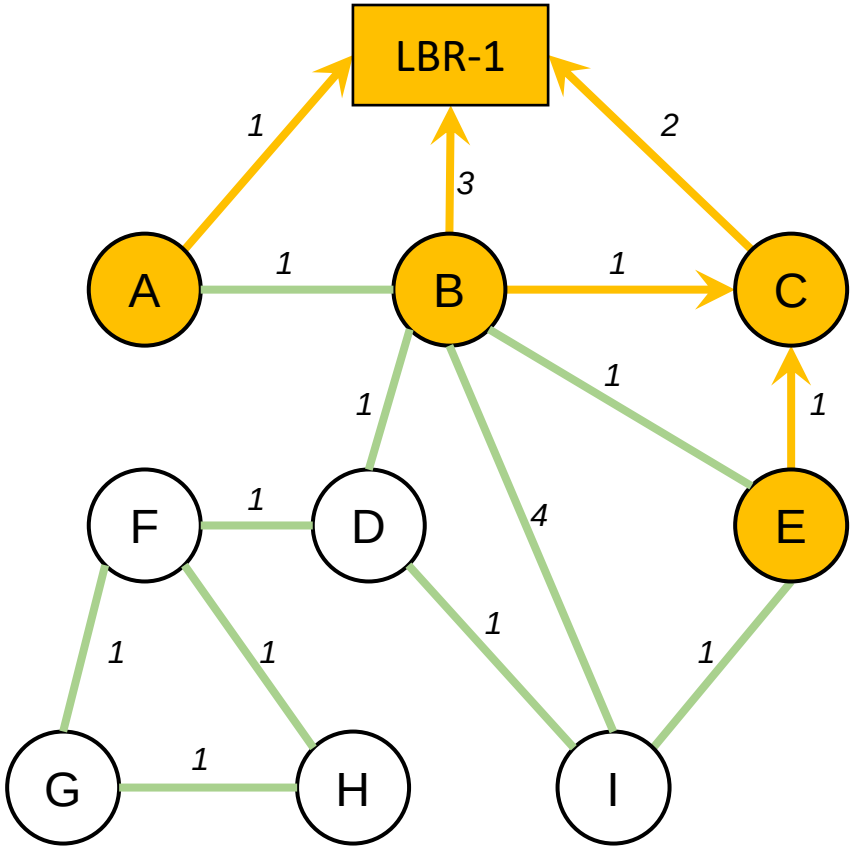
DAG Construction



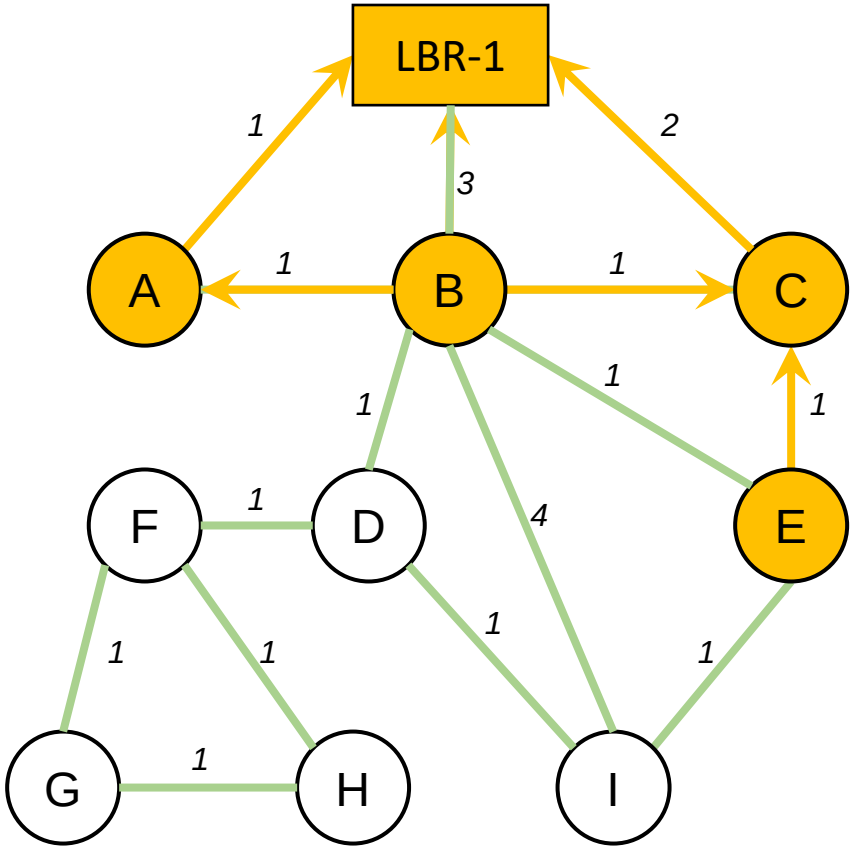
DAG Construction



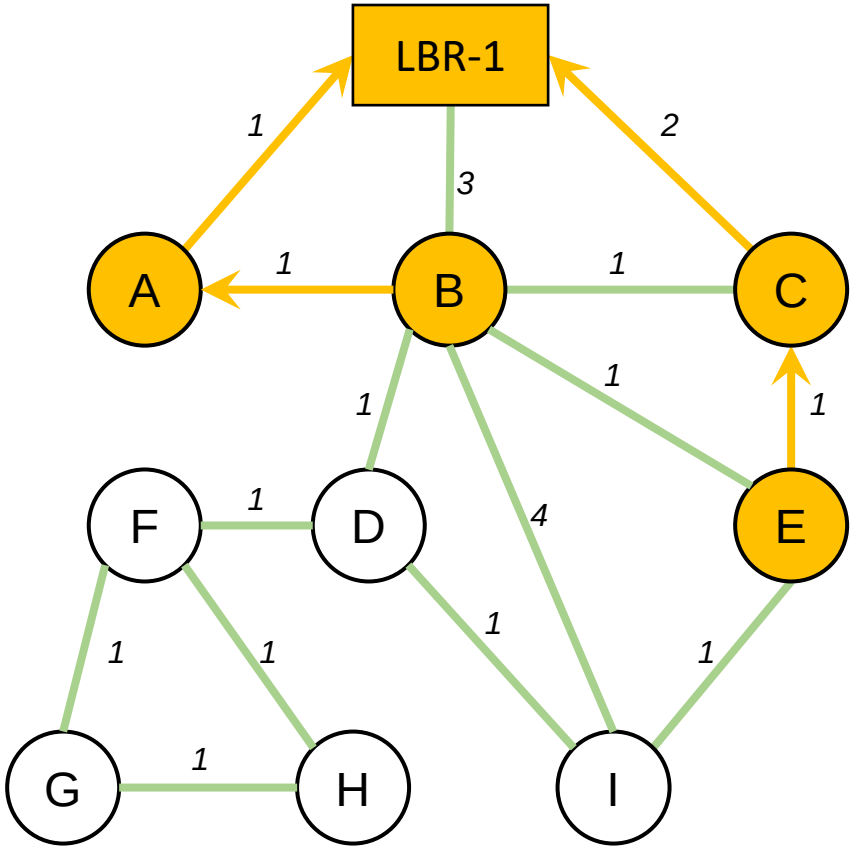
DAG Construction



DAG Construction

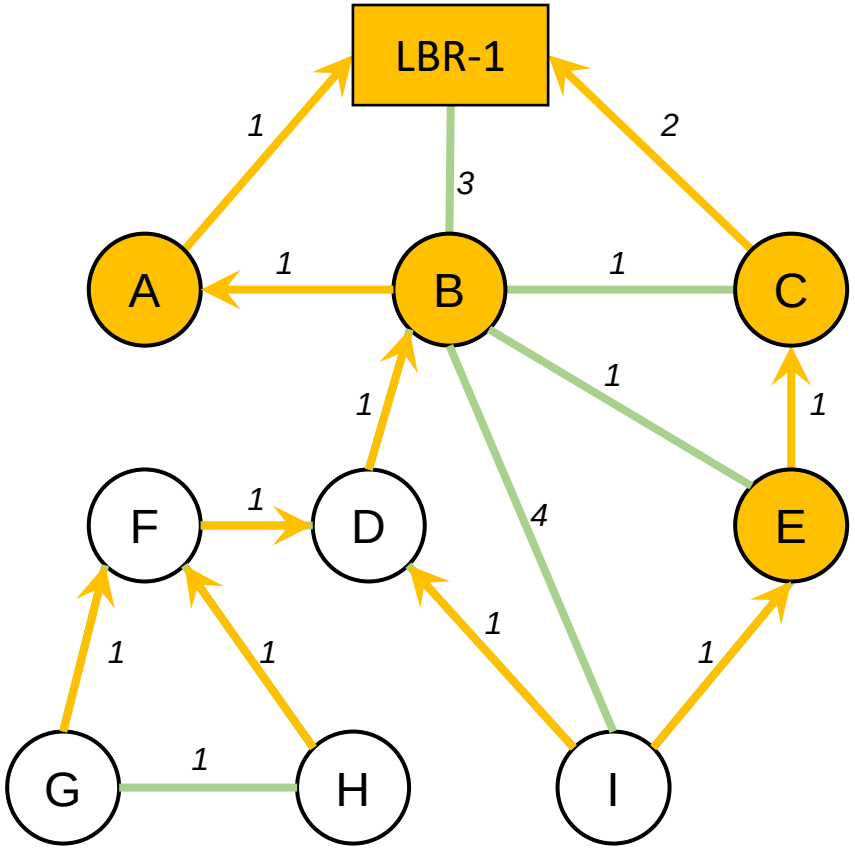


DAG Construction



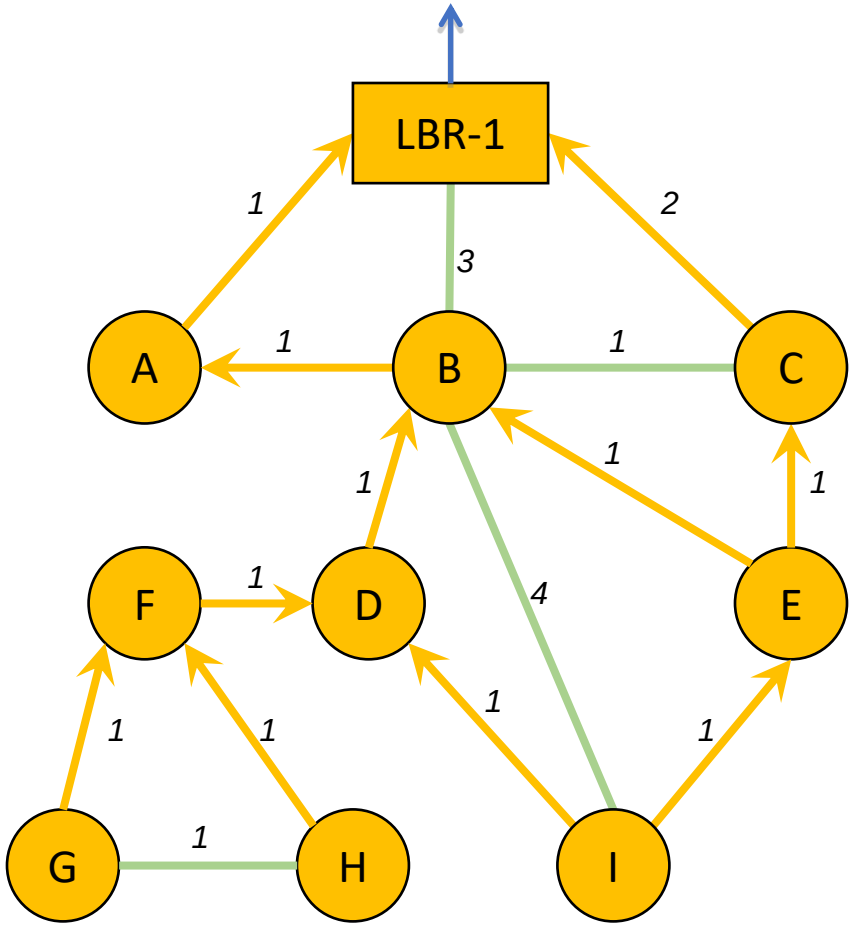
- Node A is at Depth 1, ::/0 via LBR-1 with ETX 2
- Node B is at Depth 2, ::/0 via A with ETX 2
- Node C is at Depth 2, ::/0 via LBR-1 with ETX 2
- Node E is at Depth 3, ::/0 via C with ETX 3

DAG Construction



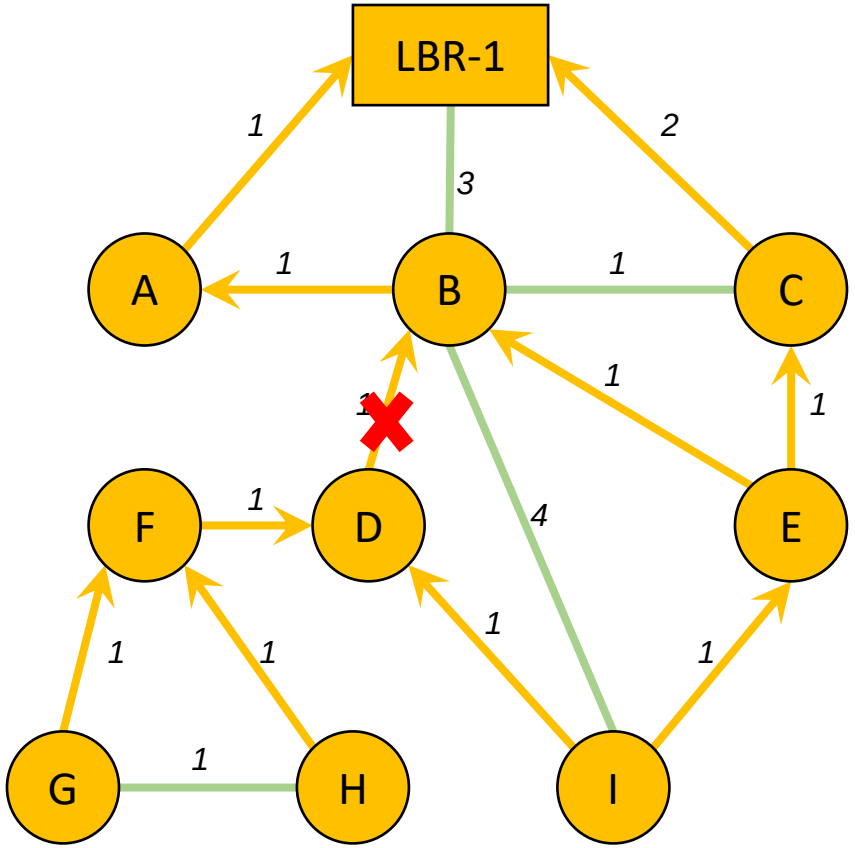
- DAG Construction continues…
- And is continuously maintained

MP2P Traffic



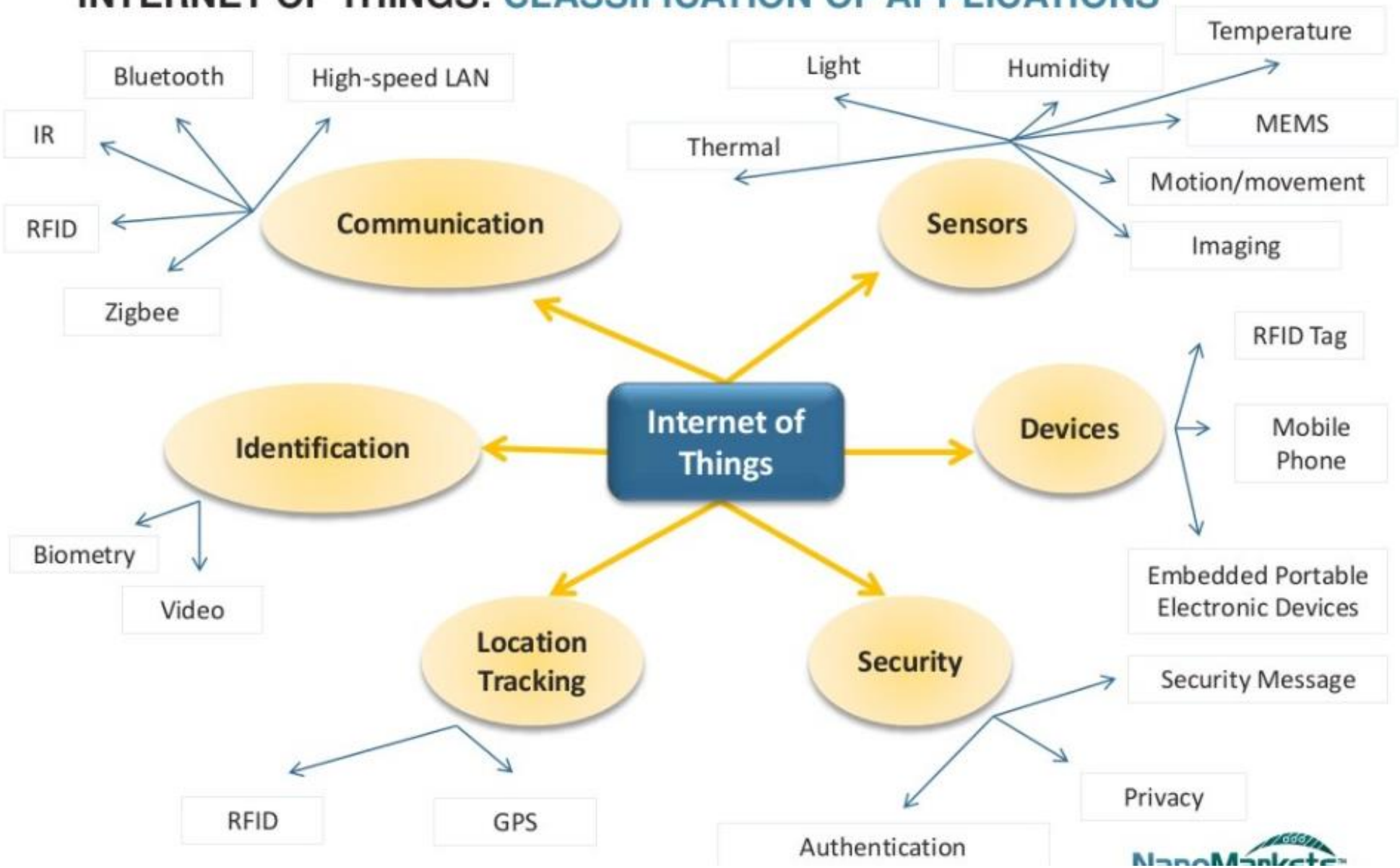
- MP2P traffic flows inwards along DAG, toward DAG Root
- DAG Root may also extend connectivity to other prefixes beyond the DAG root, as specified in the DIO
- Nodes may join multiple DAGs as necessary to satisfy application constraints

DAG Maintenance
Loop Avoidance



- Consider the case where the link B—D goes bad
- Node D will remove B from its DAG parent set
- Node D no longer has any DAG parents in the grounded DAG, so it will become the root of its own floating DAG

INTERNET OF THINGS: CLASSIFICATION OF APPLICATIONS



Power sources

- Electro chemical power sources – rechargeable and non chargeable batteries and microfuel cells. Non rechargeable batteries helps in powering the central data centre and not any portable devices.
- Biological Power sources – uses biological energy (trees, plants, human body, microorganisms)
- Energy Harvesting - This is the most important power enabler for IoT devices. It includes several technologies to facilitate ambient energy conversion and storage such as piezoelectric, thermoelectric, pyroelectric, geo-magnetic, electrostatic, direct photovoltaics, and microwave conversion approaches. IoT wireless sensor nodes will have to recover energy from a variety of energy sources if they are going to be fully autonomous. So additionally, they will require micro-batteries to serve as backup energy sources, recharged as soon as the nodes have harvested enough energy.

- Five most important drivers for IoT power sources in the industry are:
  - Wireless, smart self-charging capability
  - Environmentally friendly and cost-effective materials
  - Flexible shape and small size
  - Enhancement in energy and power density
  - Longer lifetime, preferably comparable to product lifetime

- Thank You