

Internet of Things (IoT)

Definitions and Walkthrough

Syllabus

1. IoT Trends, IoT Architecture, IoT Applications
2. IoT Standards and Protocols
3. Wireless LAN: IEEE 802.11
4. Wireless PAN: IEEE 802.15.1 & 802.15.4, Zigbee
5. Bluetooth, BTLE, LPWAN (LoRa, NBIoT), 6LowPAN
6. REST, CoAP, MQTT
7. Basics of Cryptography, Overview of IoT and Embedded security
8. Overview of 5G technologies

IoT Trends, IoT Architecture, IoT Applications

Internet of Things (IoT)



- Old term, probably its first appearance in 1999 by Kevin Ashton
- IoT term applied to RFID, supply chain, and the Internet
- Then, in 2009: “Conventional diagrams of the Internet include servers and routers and so on, but they leave out the most numerous and important routers of all: people. The problem is, **people have limited time, attention and accuracy** [...] If we had **computers that knew everything** there was to know **about things** [...] we would be able to [...] greatly **reduce waste, loss and cost**. We would know when things needed replacing, repairing or recalling, and whether they were fresh or past their best

Internet of Things - Scenarios

- Since 1999 the concept evolved far beyond RFID
- **Everything can now be connected to the Internet**
- The term IoT now refers to different scenarios:
 - Wireless Sensor Networks (WSN)
 - Near Field Communications (NFC)
 - Biotechnology and Body Area Networks (BAN)
 - Machine-to-Machine communications (M2M)
 - Personal Area Networks (PAN)
 - ...

IoT versus machine to machine

Machine2Machine:

- It is a general concept involving an autonomous device communicating directly to another autonomous device.
- It may very well be the case that an M2M device uses no internet services or topologies for communication.
- This leaves out typical internet appliances used regularly for cloud services and storage.
- An M2M system may communicate over non-IP based channels as well, such as a serial port or custom protocol.

Internet of Things:

- IoT systems may incorporate some M2M nodes (such as a Bluetooth mesh using non-IP communication), but aggregates data at an edge router or gateway.
- An edge appliance like a gateway or router serves as the entry point onto the internet. Regardless of where the internet *on-ramp* exists, the fact that it has a method of tying into the internet fabric is what defines IoT.

IoT - How Big?

- Possibly every single device and object will be connected to the Internet
- About 50-100 billions devices in 2020 (data from SAP/Intel and Ericsson)
- IBM Smarter Planet vision:
 - instrumented
 - interconnected
 - intelligent
- Several real world examples: industrial control systems, health monitoring, smart metering, home automation, ...



Internet of Things - Use Cases

Smart
Wearables



Smart
Home



Smart
City



Smart
Agriculture



Connected
Car



Health
Care



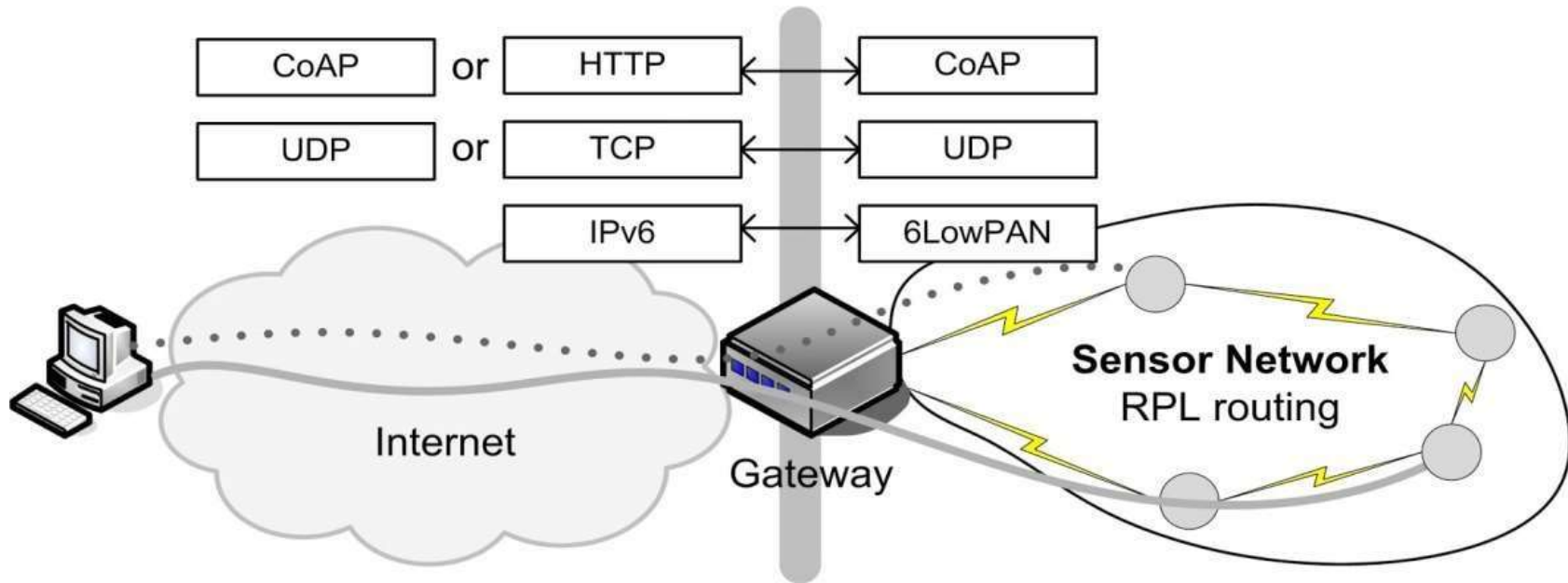
Industry
Automation



Smart
Energy



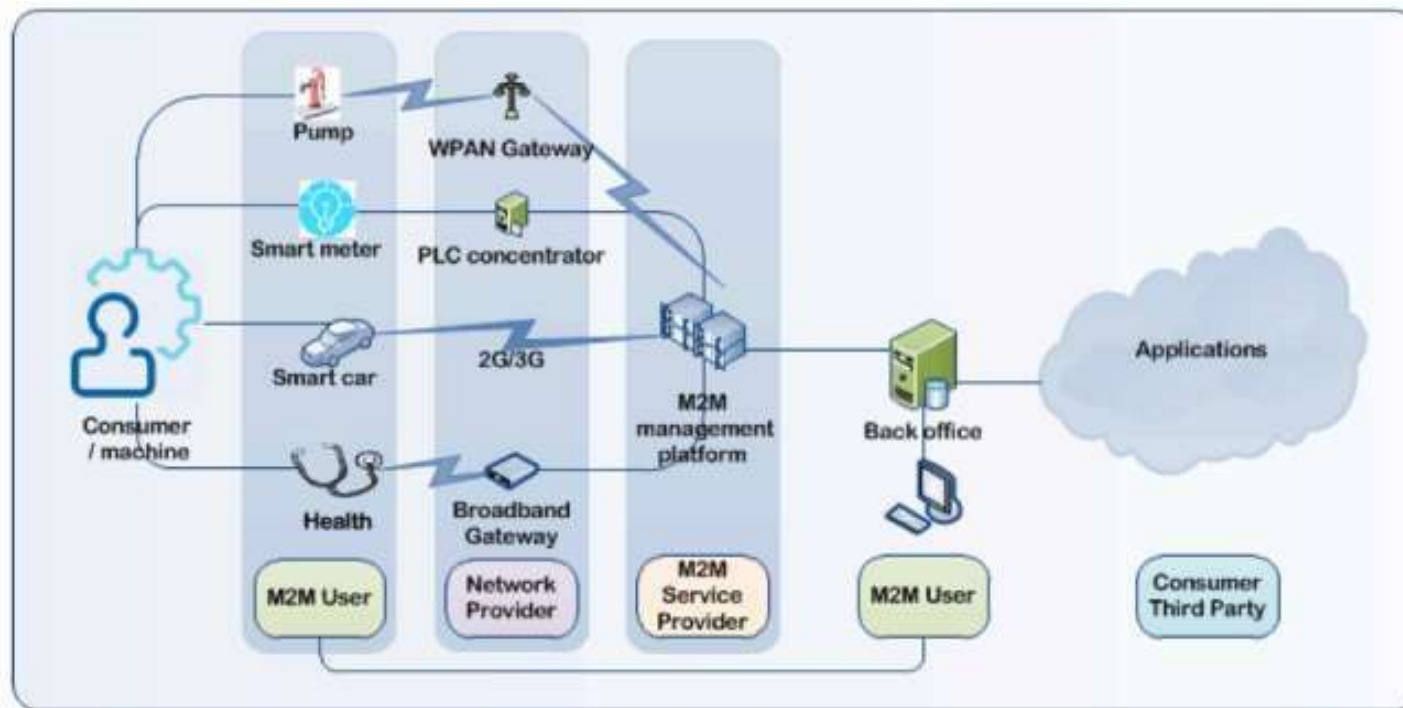
IoT - the General Idea



- The general idea behind the (commonly accepted) vision of IoT consists in the **extension of Internet protocols to Wireless Sensors Networks (WSNs)**, composed of sensors as well as actuators

IoT for Manufacturing - Machine to Machine

- The term “Machine to Machine” (**M2M**) describes devices **connected to each other**, by using a variety of fixed/wireless networks and through the Internet to the wider world. They are **active** communication devices



- Note the **wide variety of communication** infrastructures and services and **massive number of nodes**

IoT - Main Tasks

- **Gather information from things** and send commands to things
 - monitoring: state information
 - control: command enforcement
- **Send information back and forth** remote locations (private/public cloud)
- **Store and aggregate** information
- **Analyze** information to improve system knowledge
- **Take decisions**, in a human-assisted or autonomous manner

Outline

1. Introduction to IoT

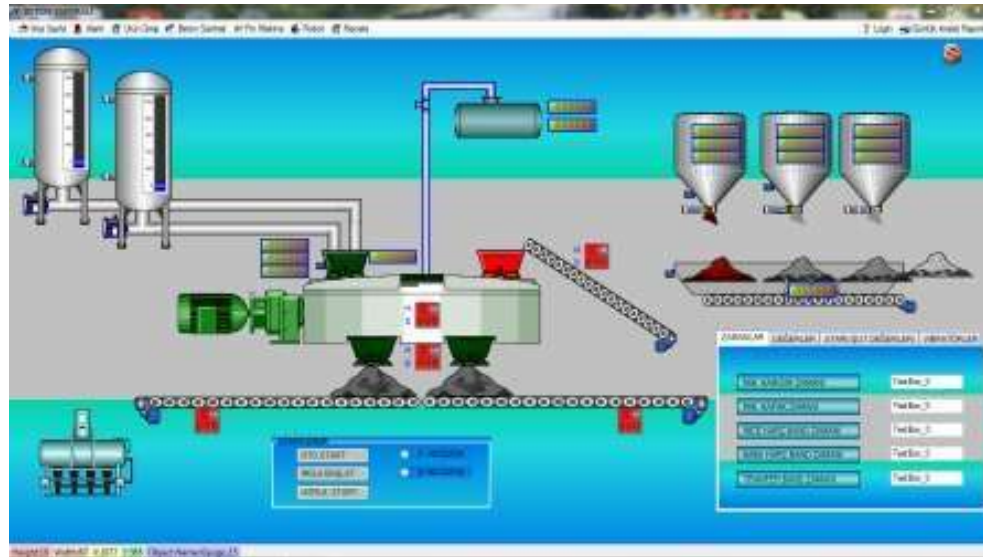
- **definition, enabling technologies and concepts to better understand the general framework of IoT solutions**
- layering architecture, cloud computing vs. fog computing

2. Most relevant components of IoT solutions

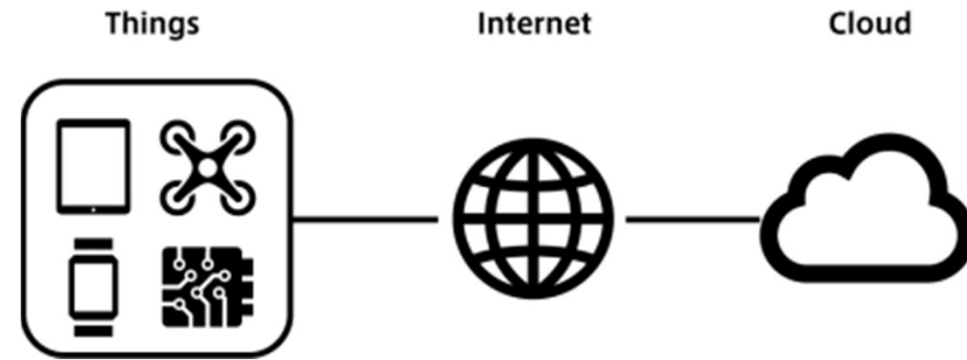
- devices, wireless communication protocols, data exchange protocols, IoT platforms, and data analysis

SCADA - Supervisory Control And Data Acquisition

- Before IoT, **remote monitoring and control** already available for **years**
- Central control system with sensors/actuators, controllers, communication equipment, and software
- Issues with SCADA : **Expensive, lack of standard, no interoperability**



IoT - Main Goals, in a nutshell...




- IoT can be seen as a novel business approach
 - based on a set of (already available) technology tools
 - exploited in novel (industrial) scenarios
- The Internet (and its standards) exploited to transfer data about things in an **efficient**, **interoperable**, and **secure** manner
- Things can be
 - **physical**: Cyber Physical System (CPS) solutions to create a bridge between the physical and digital worlds
 - **digital**: information are already in binary format, but typically not in a standard format
- Gathered data analyzed to acquire a more **in-depth knowledge of physical/digital systems**, typically composed of **geographically distributed** and **heterogeneous** things

IoT Definition – Small Environment Scenario

- An IoT
 - is a network that
 - connects uniquely identifiable “Things”
 - to the Internet
- The Things
 - have sensing/actuation and
 - potential programmability capabilities
- Through the exploitation of unique identification and sensing
 - information about the Thing can be collected
 - and the state of the Thing can be changed
 - from anywhere, anytime, by anything

IoT Enabling Technologies

- Reduced **hardware** cost and size
 - from special-purpose to Commercial Off-The-Shelf (COTS)
 - Pervasive and cheap **wireless communication**
 - from cables to large-bandwidth and/or wide-coverage wireless communication
- 
- actual game changers, IMHO
- Consolidated and emerging **Web-based communication**
 - from close protocols to open standards, also applied in constrained devices
 - **Standards**, to achieve interoperability
 - e.g., communication standards and data representation
 - General purpose **horizontal solutions**
 - from SCADA to IoT platforms
 - Automatic tools to **infer knowledge**
 - wide application of AI (Artificial Intelligence) techniques

Outline

1. Introduction to IoT

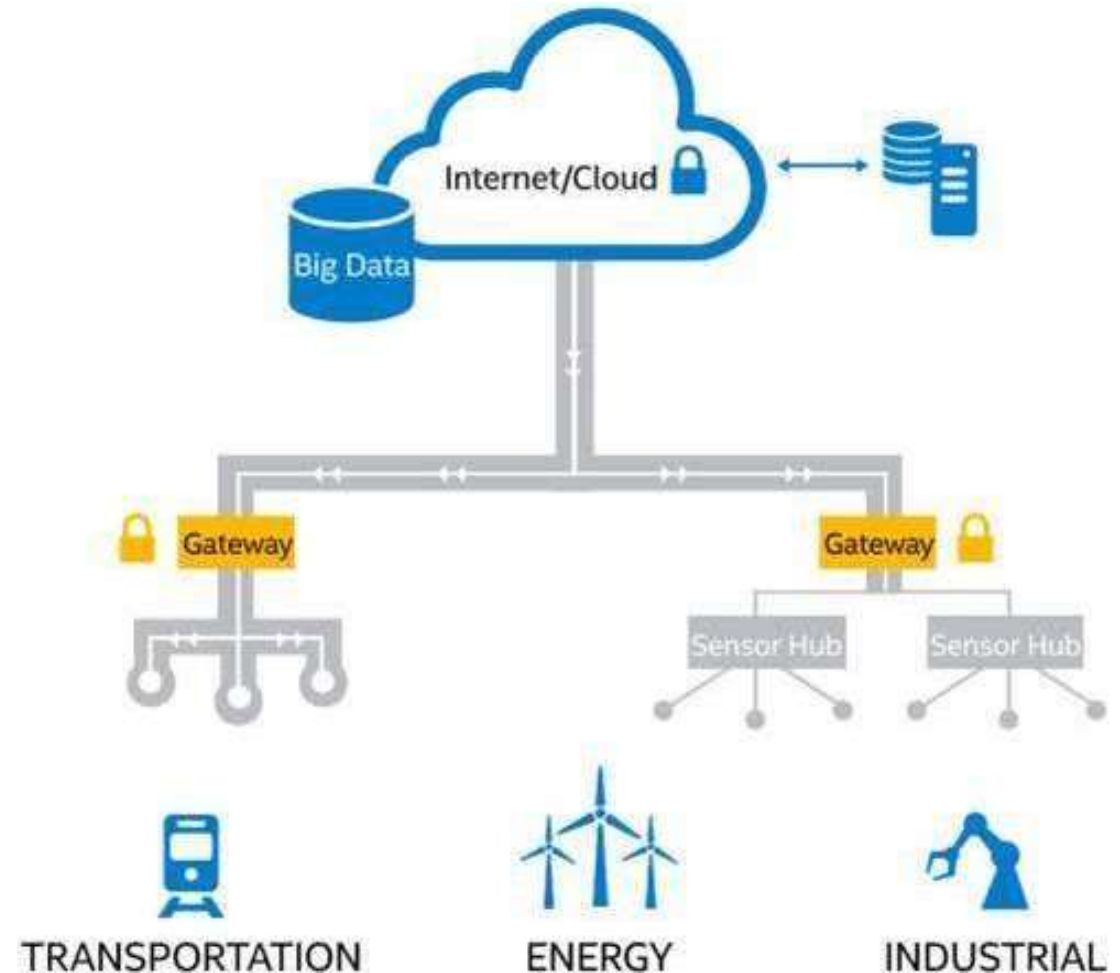
- definition, enabling technologies and concepts to better understand the general framework of IoT solutions
- **layering architecture, cloud computing vs. fog computing**

2. Most relevant components of IoT solutions

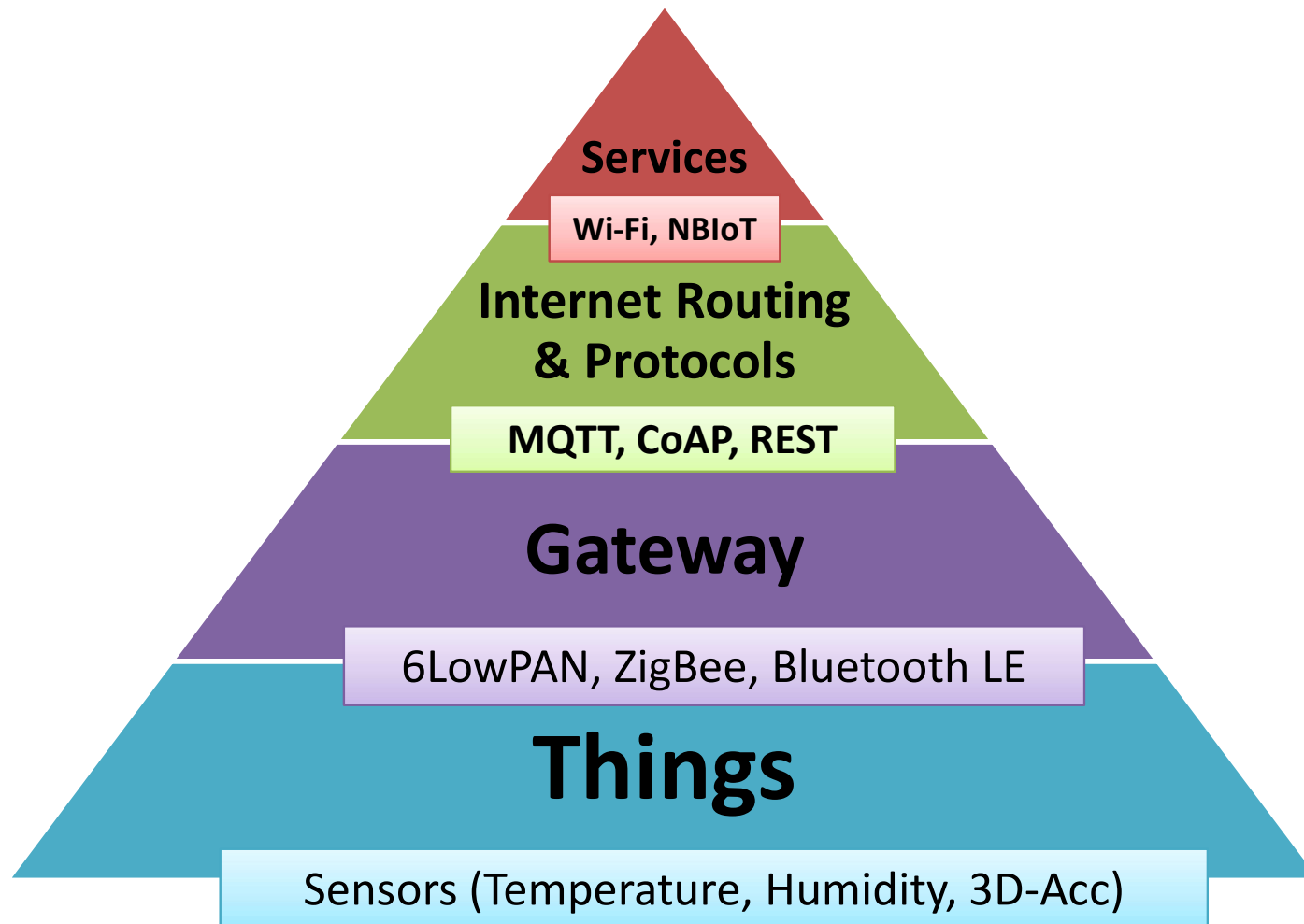
- devices, wireless communication protocols, data exchange protocols

Typical Cloud-based IoT Architecture

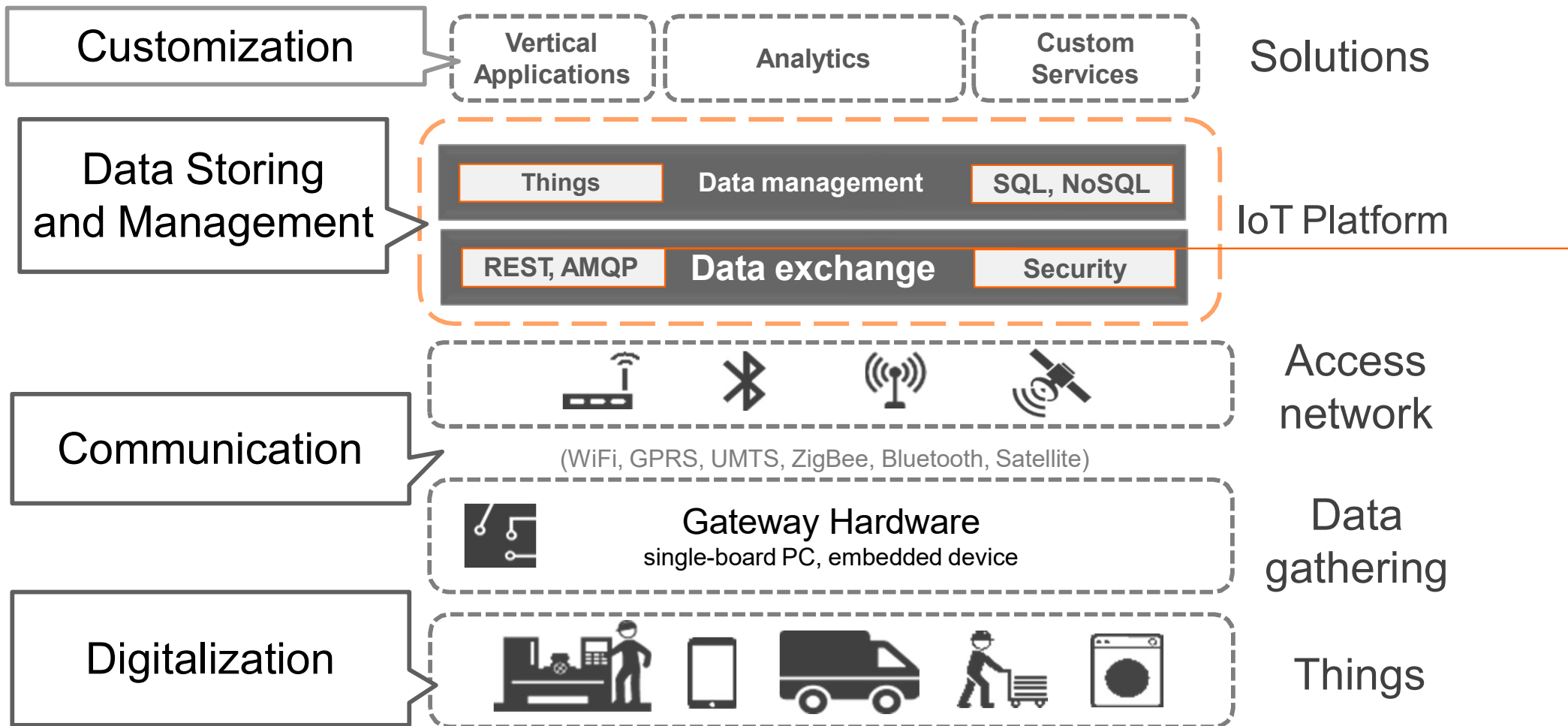
- Several heterogeneous **things**, e.g., sensors and actuators
- Multiple **gateways** geographically close to sensors/actuators
 - directly interact with things
 - dispatch data to/from the Internet
- Server-side remote **applications** stored in the Cloud and managing data



IoT Architecture



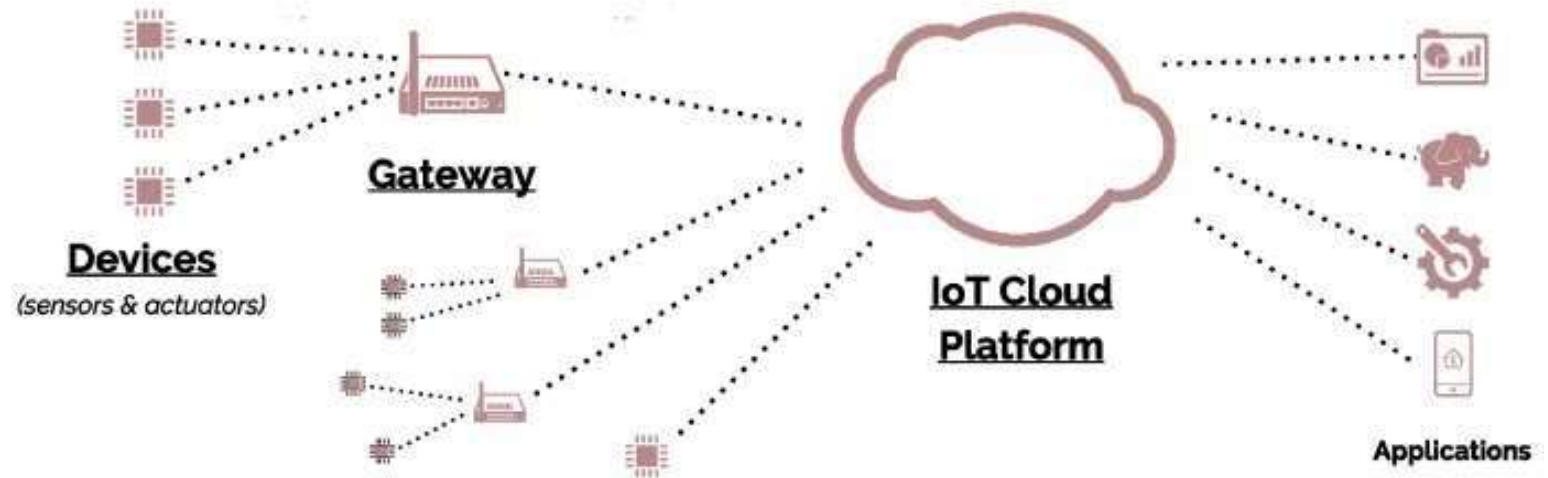
IoT: One Solution, Many Layers



Layering to Simplify Complexity

- **Things:** any physical or digital objects that should be monitored or controlled
 - physical objects must be digitalized
 - virtual objects must be standardized
- **Gateway:** close to one or multiple things to interact with them and send data and command back and forth the Internet
- **Communication protocol:** wired/wireless technology to actually send bytes
- **Data exchange protocol:** software protocol to standardize how information are transported (and eventually also represented)
- **IoT Platform:** data storing and management, application of (simple) aggregation/processing functions on data
- **Analytics:** complex analysis on data to infer new knowledge

Gateway

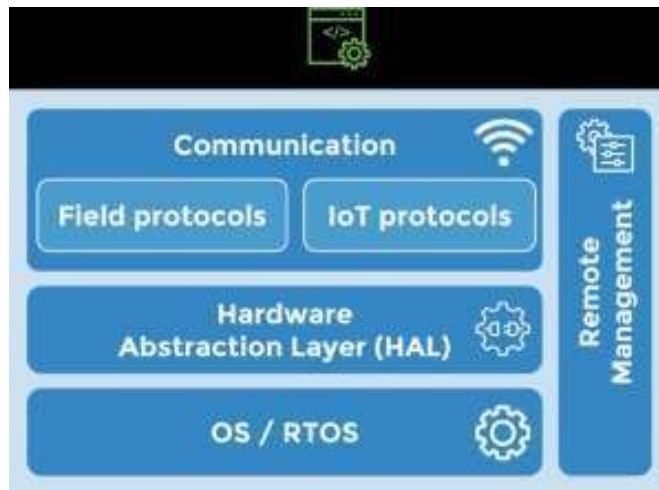


- **Protocol translation** between peripheral trunks of the IoT, eventually provided with lower parts of the communication stacks
- Gateways can also provide: pre-processing, **security**, scalability, service discovery, **geo-localization**, **billing**, etc.
- Pre-processing:
 - data **buffering**: temporarily store data to wait for connectivity or to increase efficiency
 - data **efficiency**: temperature read every 1s, but only per-minute average sent
 - data **aggregation**: water level from different silos, but only the sum is sent
 - data **filtering**: send temperature values only if greater than 25°C

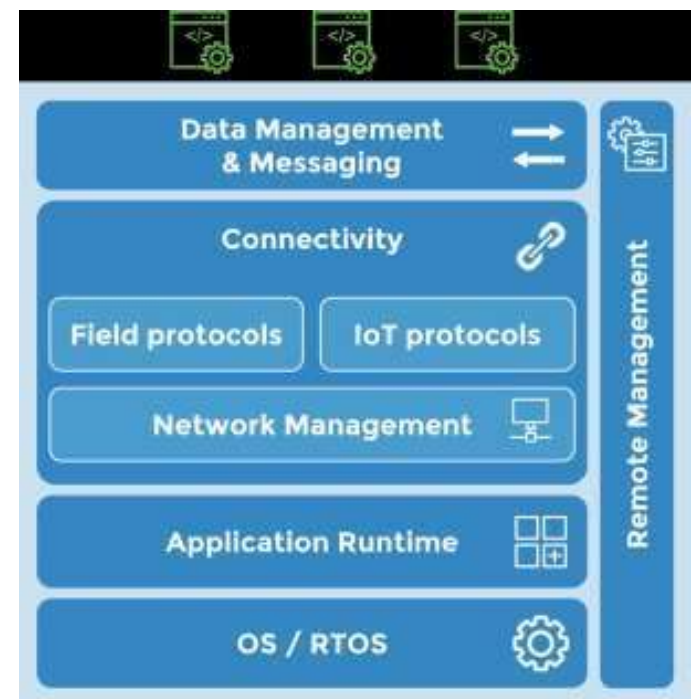
With/Without Gateway

- If there is no gateway, things have to send/receive data on their own
- In case of constrained devices, reduced set of capabilities, e.g.,
 - no security since cryptography is CPU-intensive
 - no data buffering, filtering aggregation
 - no programmability
 - ...

Stack for constrained devices



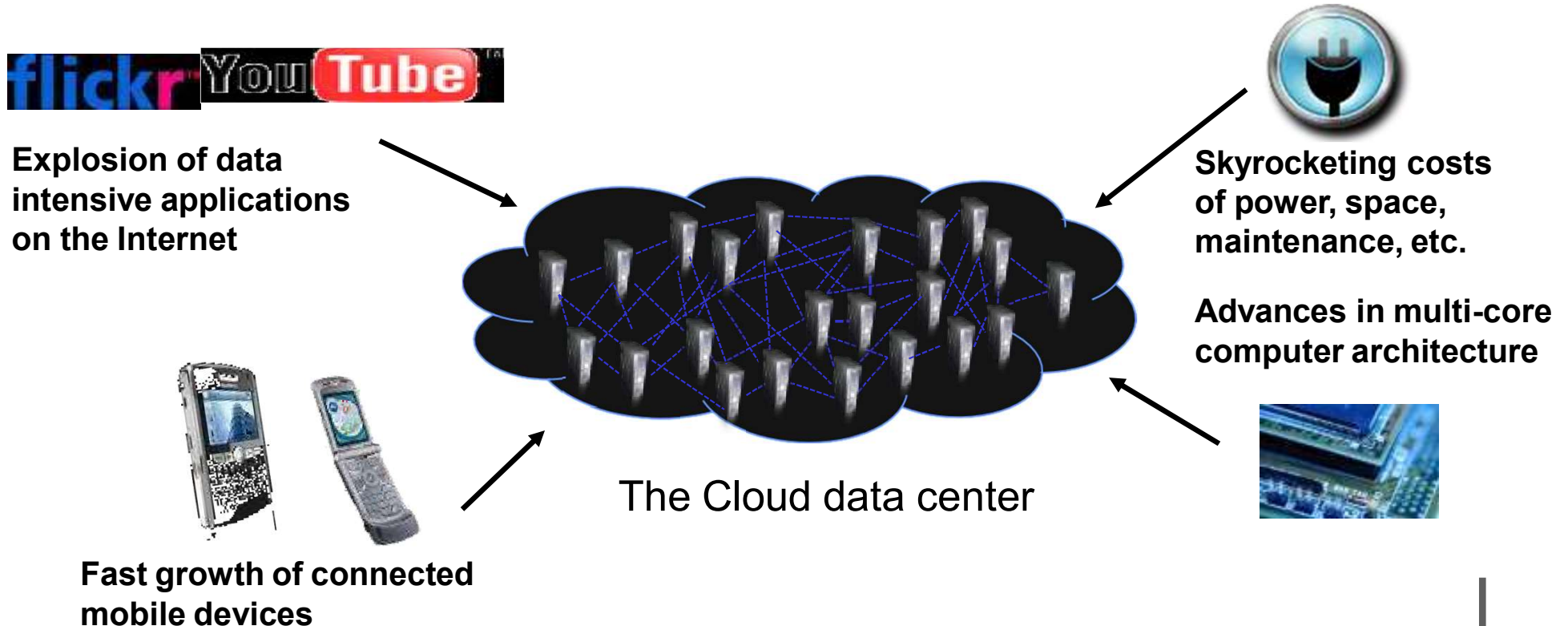
Stack for gateways



Cloud computing: problem space

*“It starts with the premise that the **data services and architecture** should be on **servers**. We call it **cloud computing** – they should be in a ‘cloud’ somewhere. And that if you have the right kind of **browser** or the right kind of access, it doesn’t matter whether you have a PC or a Mac or a mobile phone or a BlackBerry or what have you – or new devices still to be developed – you can get access to the cloud...”*

Dr. Eric Schmidt, Google CEO, August 2006

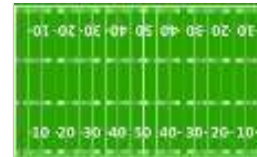


Clouds are Cheaper... and Winning...

- Range in size from “edge” facilities to **megascale**
- **Scale economies**
- Approximate **costs** for a **small size center** (1K servers) and a **larger**, 50K server center



Technology	Cost in small-sized Data Center	Cost in Large Data Center	Cloud Advantage
Network	\$95 per Mbps/month	\$13 per Mbps/month	7.1
Storage	\$2.20 per GB/month	\$0.40 per GB/month	5.7
Administration	~140 servers/Administrator	>1000 Servers/Administrator	7.1



Each data center is
11.5 times
the size of a football field

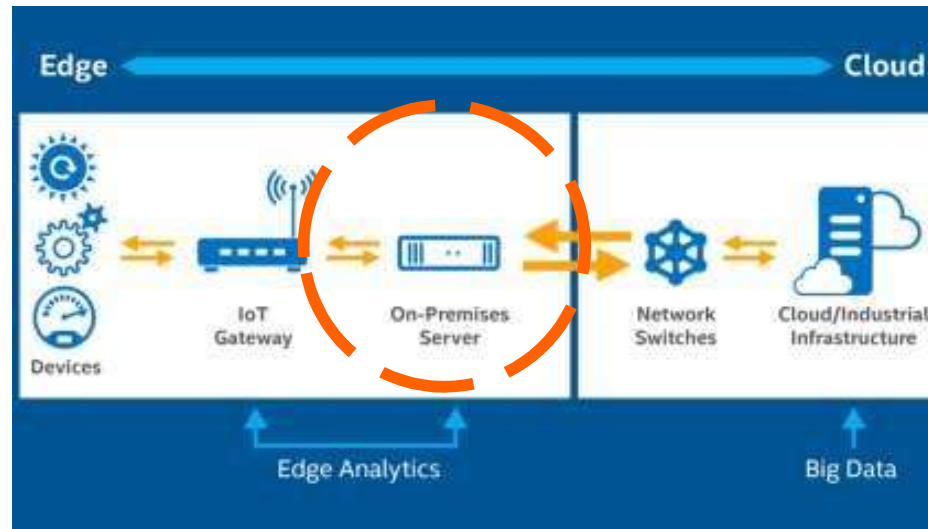
Cloud Computing: a brief introduction

- Primary concepts
 - IT **on demand** pricing
 - best benefits in a **reliable** context
 - pool of **virtualized** computer resources
 - rapid live **providing** while demanding
 - systems on **scaling** architecture
- What is a Cloud
 - one Cloud is capable of providing **IT resources “as a service”**
 - one Cloud is an IT service delivered to users that have:
 - **reduced incremental management costs** when additional IT resources are added
 - services oriented management architecture
 - massive scalability



Beyond the cloud:

From Cloud Computing to Fog/Edge Computing



- First evolution wave: **IoT Cloud Computing** architecture
 - most of the computation on the Cloud
 - **only gateways are deployed close to things**
 - gateways perform **few and simple tasks**
- Second evolution wave: **IoT Fog/Edge** Computing architecture
 - additional **relatively powerful devices**
 - **close to things**, but between gateways and the Cloud
 - **complex analytical tasks** on the client-side, before sending data to the Cloud

Fog/Edge Computing for IoT

- Cloud models are not designed for the volume, variety, and velocity of data that the IoT generates
- Fog/Edge Computing allows to
 - minimize **latency**
 - conserve network **bandwidth**
 - address **security** concerns in transit and at rest
 - **move data** to the best place for processing
- When to consider Fog/Edge Computing
 - data is collected at the **extreme edge**: vehicles, ships, factory floors, roadways, railways, etc.
 - **thousands or millions of things** across a large geographic area are generating data
 - it is necessary to analyze and **act on data promptly**, in less than a second

Fog/Edge Computing for IoT use case: Rails



- **Improve passenger safety**
 - analyze and correlate data from cameras on the trains and at stations
 - monitor sensors on wheels and brakes to determine when parts need service before failure causes an accident
- **Prevent cybersecurity attacks**
 - take automated actions such as suspending operations or transferring control to a failover system
- **Alert drivers** to treacherous conditions ahead
 - Fog nodes gather sensor data on tracks and trains to detect unsafe conditions

Fog/Edge Computing for IoT use case: Manufacturing



- **Increase agility**
 - quickly change production lines and introduce new products
- **Reduce downtime**
 - predictive maintenance to avoid costly equipment downtime
 - Fog/Edge nodes collect machine data and report early signs of problems
- Continually **confirm that safety systems are intact**
 - analyze machine data in real-time
 - promptly shut down compromised equipment automatically, without waiting for a human to respond to an alert

IoT Standards and Protocols

Outline

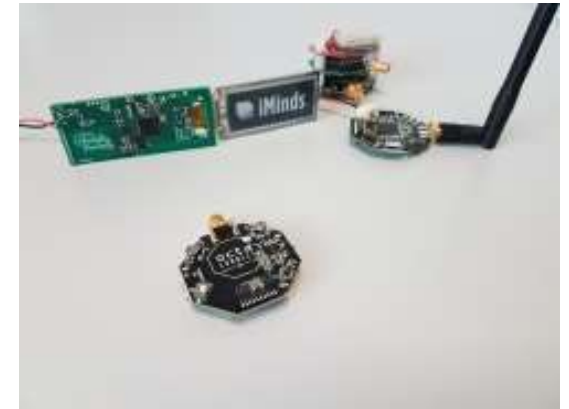
1. Introduction to IoT

- definition, enabling technologies and concepts to better understand the general framework of IoT solutions
- layering architecture, cloud computing vs. fog/edge computing

2. Most relevant components of IoT solutions

- **devices**, wireless communication protocols, data exchange protocols

Constrained Devices



- “A node where some of the characteristics that are otherwise pretty much taken for granted for Internet nodes **at the time of writing** are not attainable, [...] due to **cost, size, and energy constraints**”
- Significant constraints on:
 - maximum code complexity (ROM/Flash)
 - size of state and buffers (RAM)
 - available computational power
 - connectivity

Constrained Networks



- “A network where some of the characteristics pretty much taken for granted with link layers in common use in the Internet **at the time of writing** are not attainable”
- Significant constraints on:
 - low achievable **throughput**
 - high **packet loss**
 - highly **asymmetric links**
 - severe penalties for using **larger packets**
 - limits on **reachability** over time

Classes of Constrained Nodes

Name	Data size (RAM)	Code size (Flash)
Class 0	<< 10 KiB	<< 100 KiB
Class 1	~ 10 KiB	~ 100 KiB
Class 2	~ 50 KiB	~ 250 KiB

Values in 2014

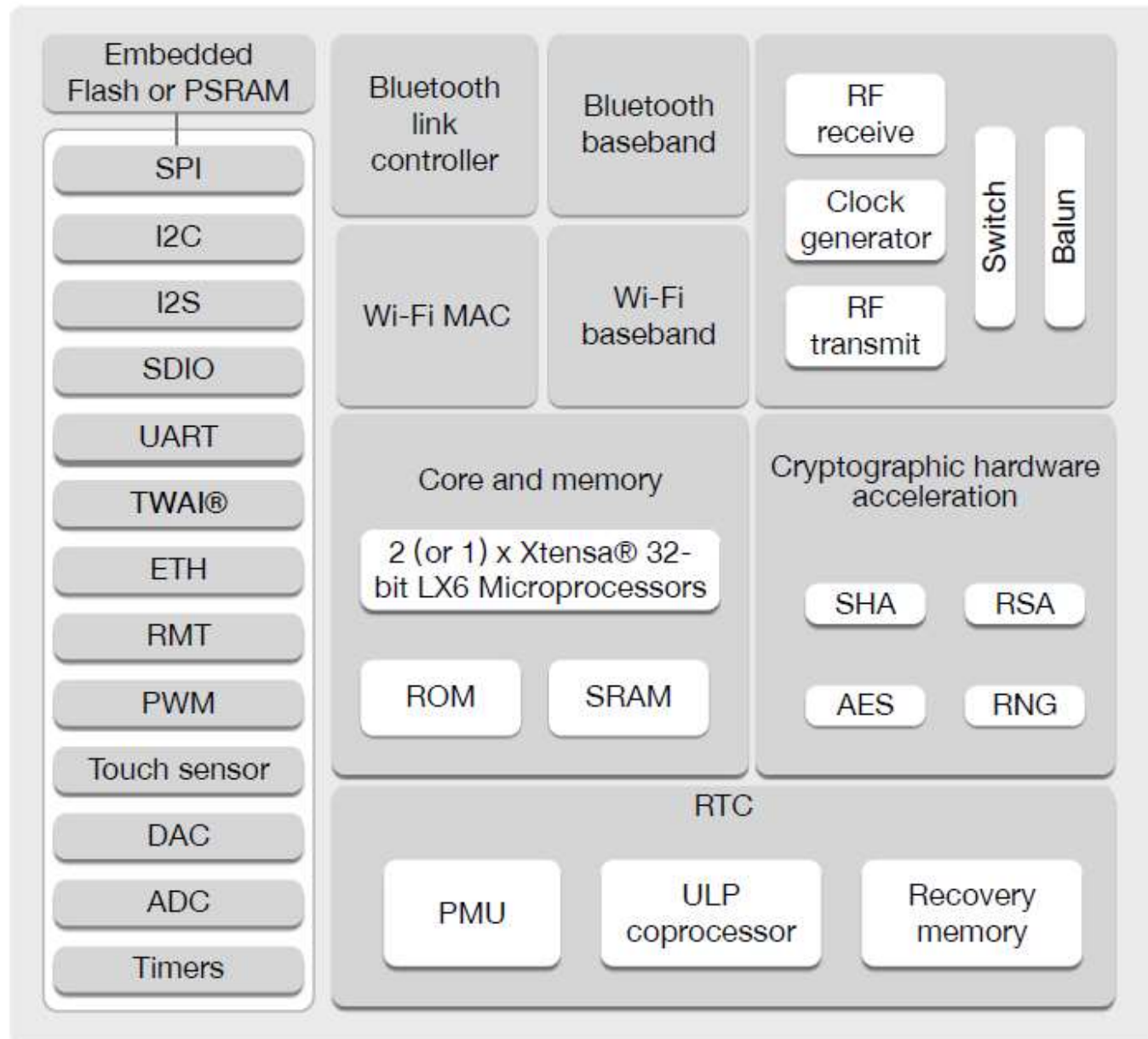
- C0 Devices
 - no direct secure Internet connection
 - use larger devices as gateways/proxies
 - preconfigured and rarely reconfigured
- C1 Devices
 - can use environment specific protocols, e.g., CoAP
 - no access to standard Internet protocols, e.g., HTTP, TLS
 - can be integrated into an IP network
- C2 Devices
 - can use most of protocols

IoT Device Example: ESP32

- Ultra Low Power Solution
- Wi-Fi Key Features
 - 802.11 b/g/n
 - 802.11 n (2.4 GHz), up to 150 Mbps
- Bluetooth Key Features
 - Compliant with Bluetooth v4.2 BR/EDR and Bluetooth LE specifications
 - Class-1, class-2 and class-3 transmitter without external power amplifier
 - Bluetooth Piconet and Scatternet
 - Multi-connections in Classic Bluetooth and Bluetooth LE
 - Simultaneous advertising and scanning
- CPU and Memory
 - Xtensa® single-/dual-core 32-bit LX6 microprocessor(s)
 - 4MB of Flash



ESP32 Block Diagram



Beyond Class 2: Single Board Computers

- In the last 5/10 years
 - tremendous improvement in CPU/memory capabilities
 - dramatically reduced costs
- Modern Single-Board Computers (SBCs) are very cheap (~100\$) and powerful
 - can host complete operating systems
 - extensions via daughterboards
 - mostly designed to be mains-powered



Outline

1. Introduction to IoT

- definition, enabling technologies and concepts to better understand the general framework of IoT solutions
- layering architecture, cloud computing vs. fog computing

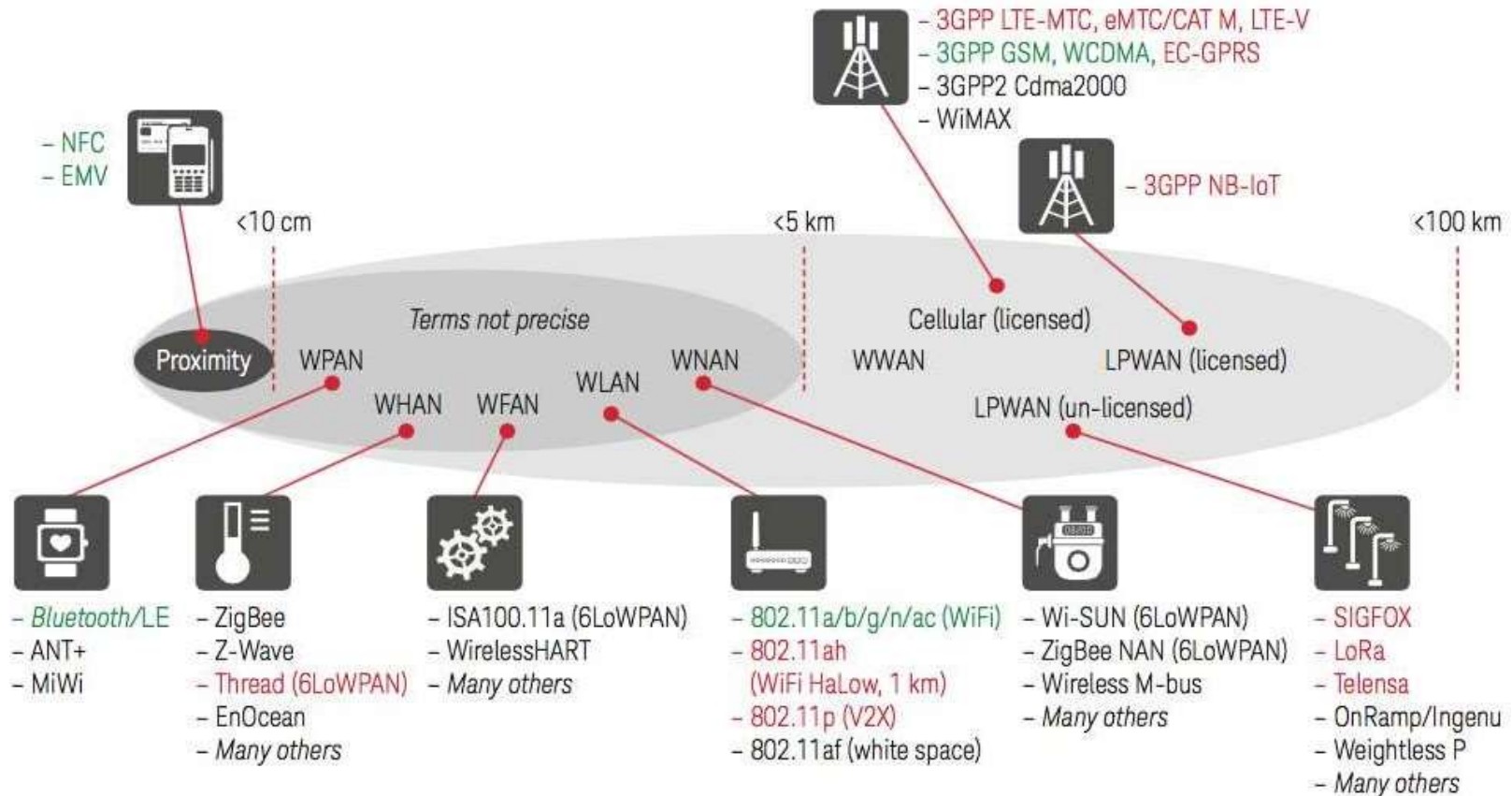
2. Most relevant components of IoT solutions

- devices, **wireless communication protocols**, data exchange protocols

Wireless Communication Protocols for the IoT

- The capability of connecting to things in a **seamless, ubiquitous,** and **cheap** manner have pushed the spread of IoT solutions
- IoT wireless communication protocols primarily differs in relation to
 - **coverage range:** from few cm to several km
 - **power consumption:** from few mW to several W
 - **bandwidth:** from few bytes per day to hundreds of MB/s
 - **security:** from plain data to strong encryption
 - **cost:** greatly varying, both for equipment and data transmission

Several Wireless Communication Protocols

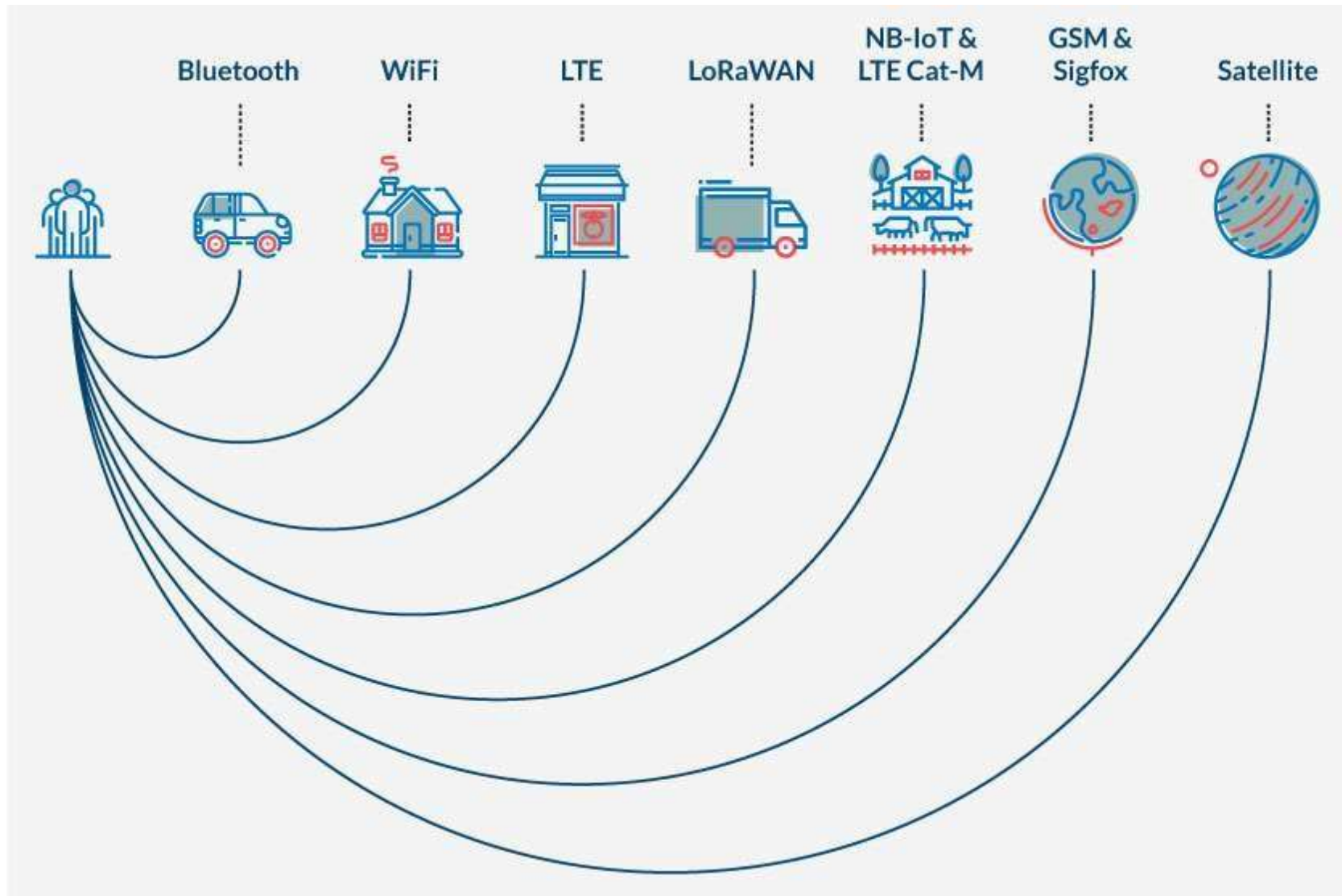


■ : > Billion units/year now
 ■ : Emerging

WPAN: Wireless Personal Area Network
 WHAN: Wireless Home Area Network
 WFAN: Wireless Field (or Factory) Area Network
 WLAN: Wireless Local Area Network

WNAN: Wireless Neighborhood Area Network
 WWAN: Wireless Wide Area Network
 LPWAN: Low Power Wide Area Network

Wireless Protocols per Coverage Range



Bluetooth



- Bluetooth and BLE are radio protocols for **Personal Area Networks (PAN)**
- Mostly these are on a person's body or in close proximity to them
- Typical range: very short, 20m (or less)
- Max output power: very limited, 0.003 W
- Bandwidth: limited, 0.7–2.1 Mbit/s
- Security: pairing task to exchange encryption keys
- Cost: cheap equipment, no transmission costs
- Good for: devices that stay **in close proximity of each other**, like between a smartphone and a headset, heart rate monitor, bicycle speedometer

Wireless LAN: IEEE 802.11

WiFi - IEEE 802.11



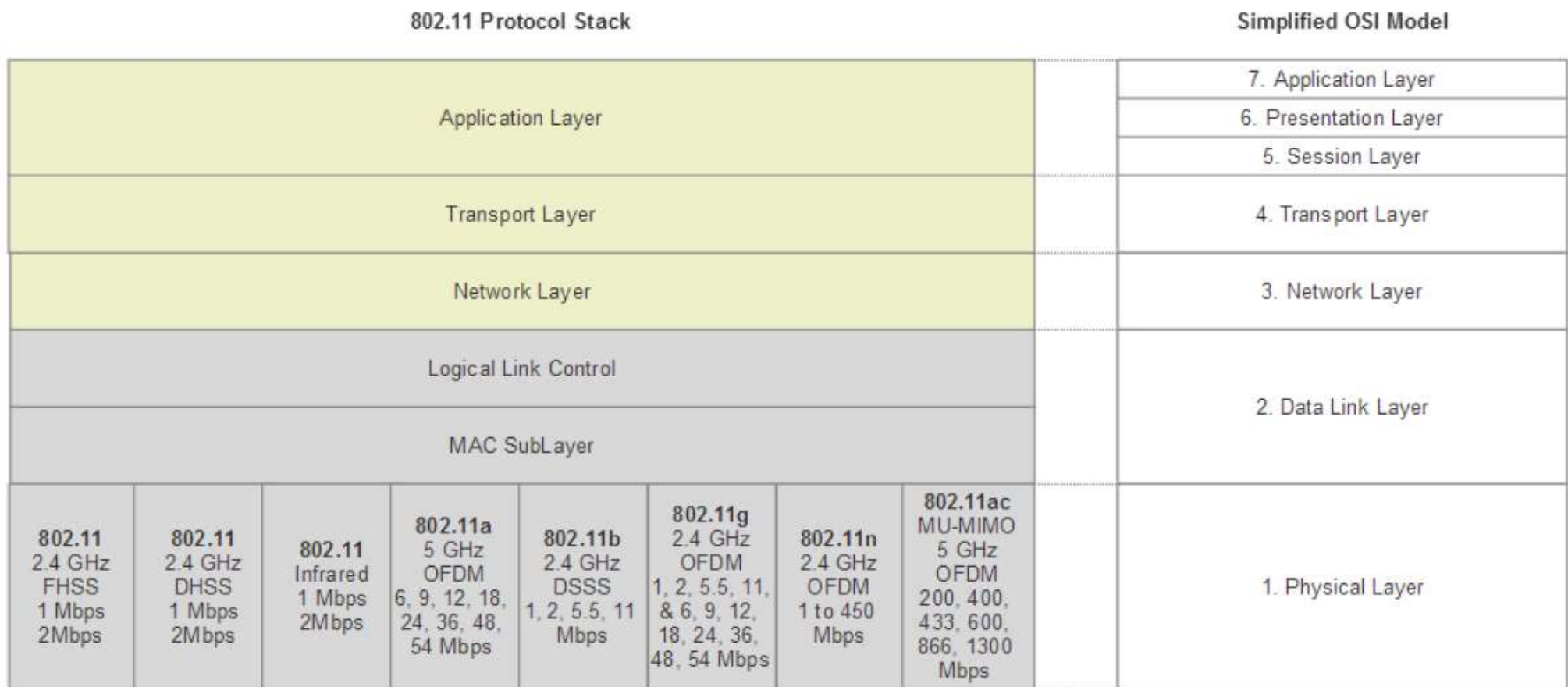
- WiFi is meant for **broadband network** connections in a confined area
- Normally less than 100 square meter per access point
- Typical range: short, 50m
- Max output power: medium/high, 0.1 W
- Bandwidth: large, up to hundreds of MB/s
- Security: suffered recent exploits, work in progress
- Cost: cheap equipment, no transmission costs
- Good for: security cameras, power meters or anything that is installed in a **fixed location, has power, and needs bandwidth**

IEEE 802.11 suite of Protocol and Comparison

IEEE 802.11 Protocol	Use Case	Release Date	Frequency (GHz)	Bandwidth (MHz)	Streaming Data Rate per Channel min-max (Mbps)
802.11	First 802.11 design	Jun-97	2.4	22	1 to 2
a	Release simultaneously with 802.11b Less prone to interference than 802.11b	Sep-99	5	20	6 to 54
			3.7		
b	Release simultaneously with 802.11a Significant speed increase over 802.11a at improved range	Sep-99	2.4	22	1 to 11
g	Speed increase over 802.11b	Jun-03	2.4	20	6 to 54
n	Multiple antenna technology for improved speed, and range.	Oct-09	2.4 / 5	20	7.2 to 72.2
				40	15 to 150
ac	Better performance and coverage over 802.11n. Wider channel and improved modulation. Allows multiple users using MU-MIMO. Introduced beamforming.	Dec-13	5	20	7.2 to 96.3
				40	15 to 200
				80	32.5 to 433.3
				160	65 to 866.7
ah	"WiFi HaLow" Designed for IoT and sensor networks. Very low power and wider range.	Dec-16	2.4 / 5	1 to 16	347
p	"Wireless Access in Vehicular Environments" "Intelligent Transport Systems" Dedicated Short Range Communication Transport uses cases: toll collection, safety and collision emergencies, vehicular networking.	Jun-09	5.9	10	27
af	"white WiFi" or "Super WiFi" Deploy unused spectrum in TV bands to provide last mile connectivity in India, Kenya, Singapore, US and UK	Nov-13	0.470 to 0.710	6 to 8	568
ad	WiGig Alliance 60 GHz Wireless for HD video and projectors Audio and video transport and cable replacement	Dec-12	60	2160	4260
ax	"High Efficiency Wireless (HEW)" Next gen 802.11 4x increase in capacity over 802.11ac Average increase of 4x speed per user over 802.11ac Backwards compatible to 802.11a/b/g/n/ac Dense deployment scenarios	2019	2.4 / 5	20	450 to 10000
				40	
				80	
				160	

802.11 Architecture

From a stack perspective, the 802.11 protocols reside in the link layer (one and two) of the OSI model, as shown in the following figure:



802.11 Topologies

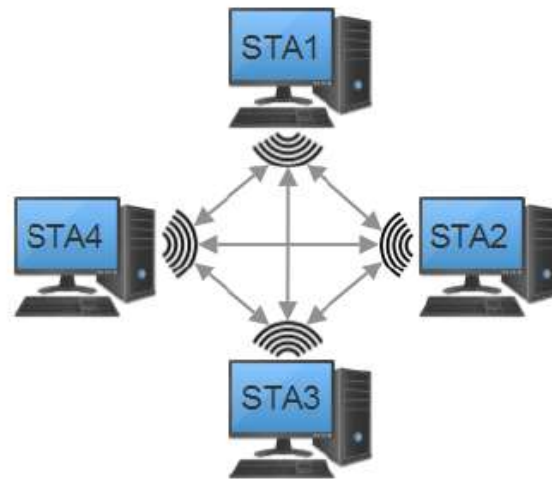
802.11 systems support three basic topologies:

- **Infrastructure:** In this form, a **Station (STA)** refers to an 802.11 endpoint device (like a Smartphone) that communicates with a central **access point (AP)**. An AP can be a gateway to other networks (WAN), a router, or a true access point in a larger network. This is also known as **Infrastructure Basic Set Service (BSS)**. This topology is a star topology.
- **Ad hoc:** 802.11 nodes can form what is called an **Independent Basic Set Service (IBSS)** where each station communicates and manages the interface to other stations. No access point or a star topology is used in this configuration. This is a peer-to-peer type of topology.
- **Distribution system (DS):** The DS combines two or more independent BSS networks through access point interconnects.

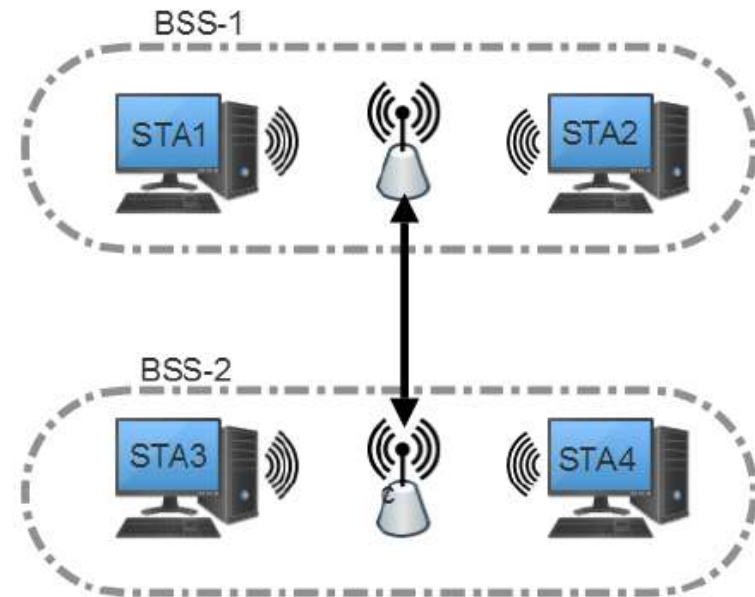
802.11 Topologies Diagram



Basic Service Set



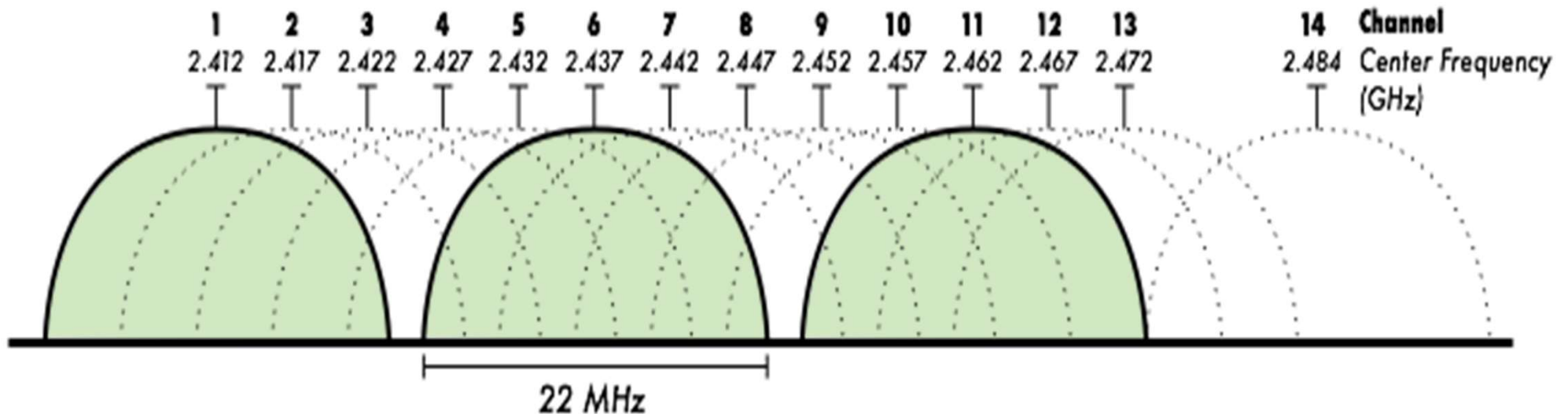
Independent Basic Service Set



Distribution System

IEEE 802.11 spectrum allocation

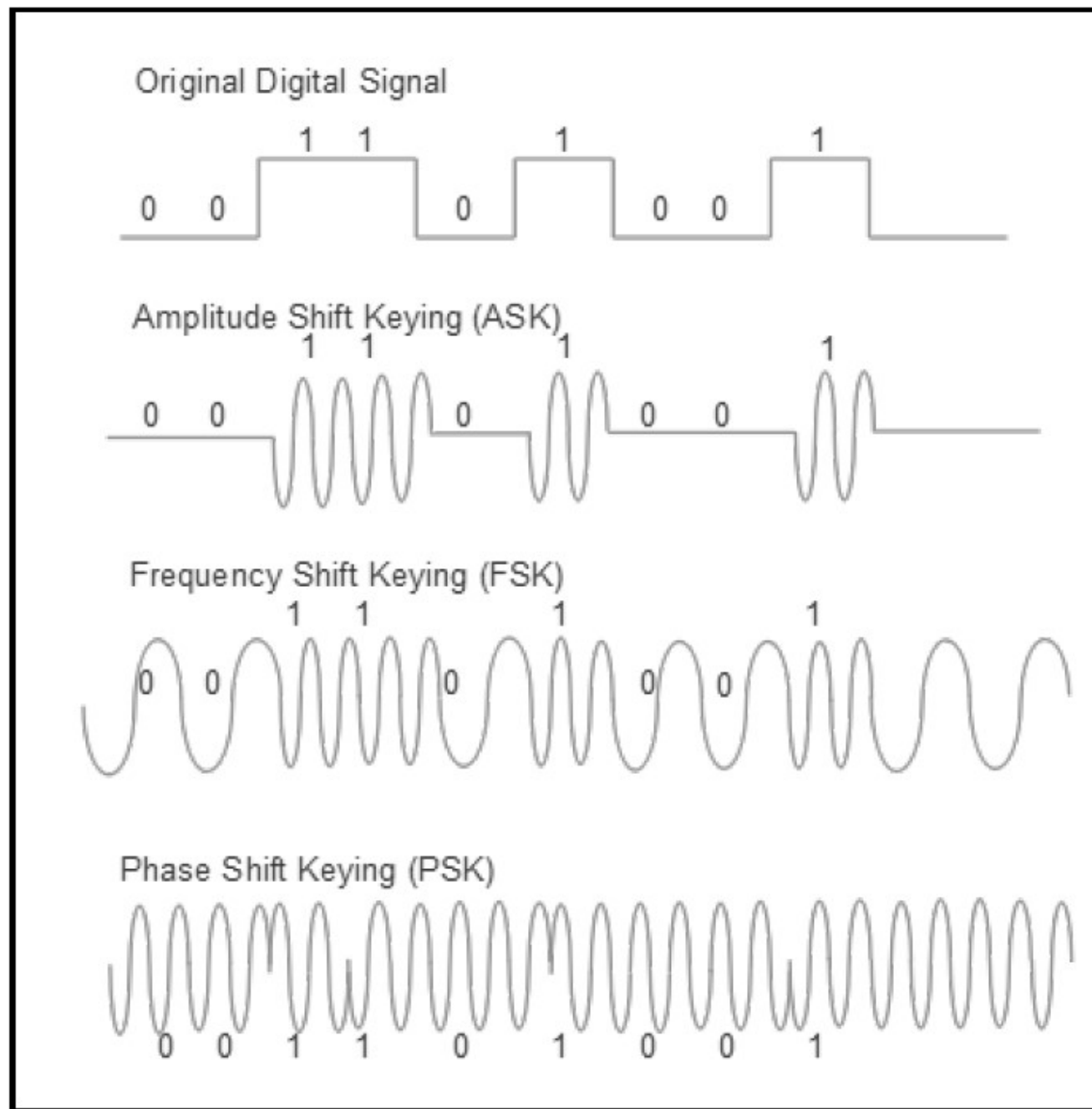
- The first 802.11 protocol used a spectrum in the 2 GHz and 5 GHz ISM region and evenly spaced channels roughly 20 MHz apart from each other.
- The channel bandwidth was 20MHz, but later amendments from IEEE allowed 5 MHz and 10 MHz to operate as well.
- Three of the channels are non-overlapping (1,6,11)



IEEE 802.11 modulation and encoding techniques

- **Amplitude Shift Keying (ASK):** This is a form of amplitude modulation. Binary 0 is represented by one form of modulation amplitude and 1 a different amplitude.
- **Frequency Shift Keying (FSK):** This modulation technique modulates a carrier frequency to represent 0 or 1. The simplest form shown in the following figure is **Binary Frequency Shift Keying (BFSK)**, which is the form used in 802.11 and other protocols.
- Bluetooth and Z-Wave, those protocols use a form of FSK called **Gaussian Frequency Shift Keying (GFSK)** that filters the data through a Gaussian filter, which smooths the digital pulse (-1 or +1) and shapes it to limit spectral width.
- **Phase Shift Keying (PSK):** Modulates the phase of a reference signal (carrier signal). Used primarily in 802.11b, Bluetooth, and RFID tags. PSK uses a finite number of symbols represented as different phase changes.

IEEE 802.11 modulation



802.11 standards interference mitigation techniques

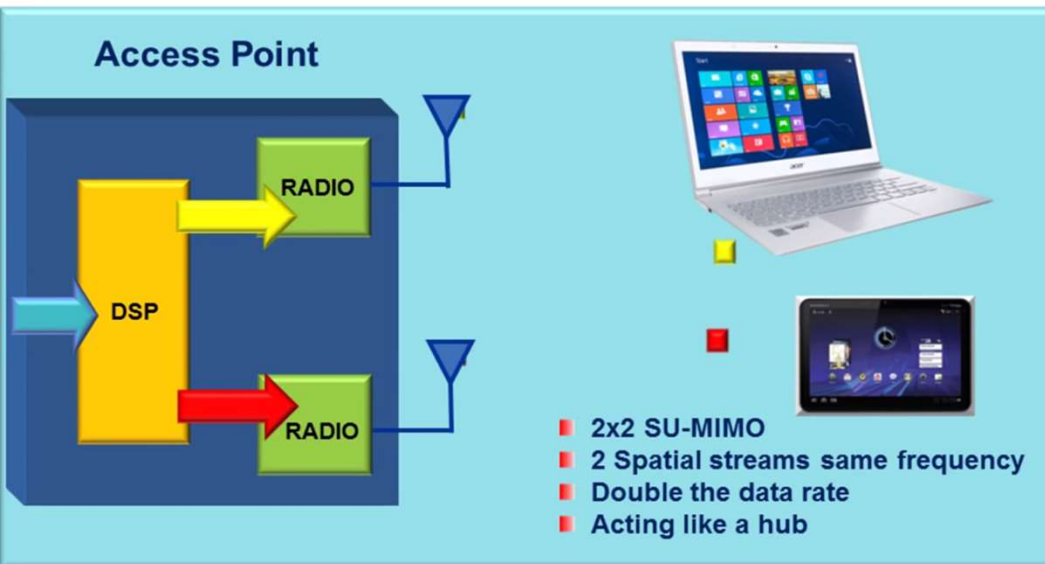
- **Frequency Hopping Spread Spectrum (FHSS):** Spreads signal over 79 nonoverlapping channels that are 1 MHz wide in the 2.4 GHz ISM band. Uses a pseudo-random number generator to start the hopping process.
- **Direct sequence spread spectrum:** First used in 802.11b protocols and has 22 MHz-wide channels. Each bit is represented by multiple bits in the signal transmitted. The data being transmitted is multiplied by a noise generator. This will effectively spread the signal over the entire spectrum evenly using a pseudorandom number sequence (called the *Pseudo-Noise* PN code).
- **OFDM:** Used in IEEE 802.11a and the newer protocols. This technique divides a single 20 MHz channel into 52 sub-channels (48 for data and four for synchronization and monitoring) to encode data using QAM and PSM.

IEEE 802.11 MIMO

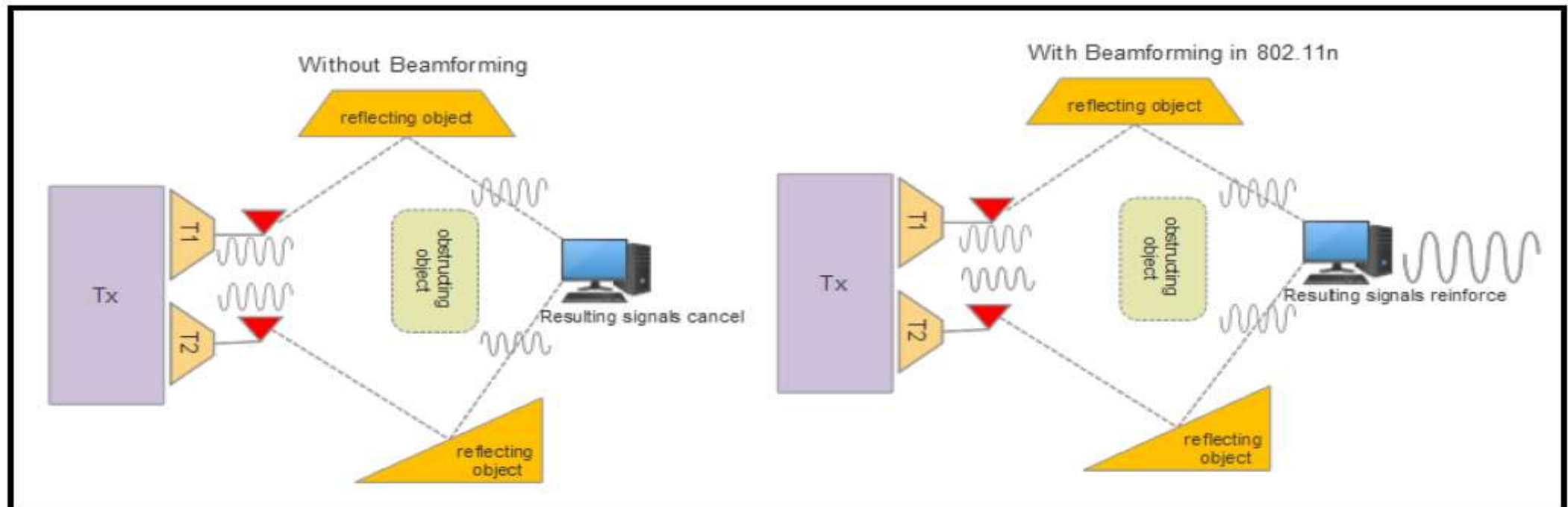
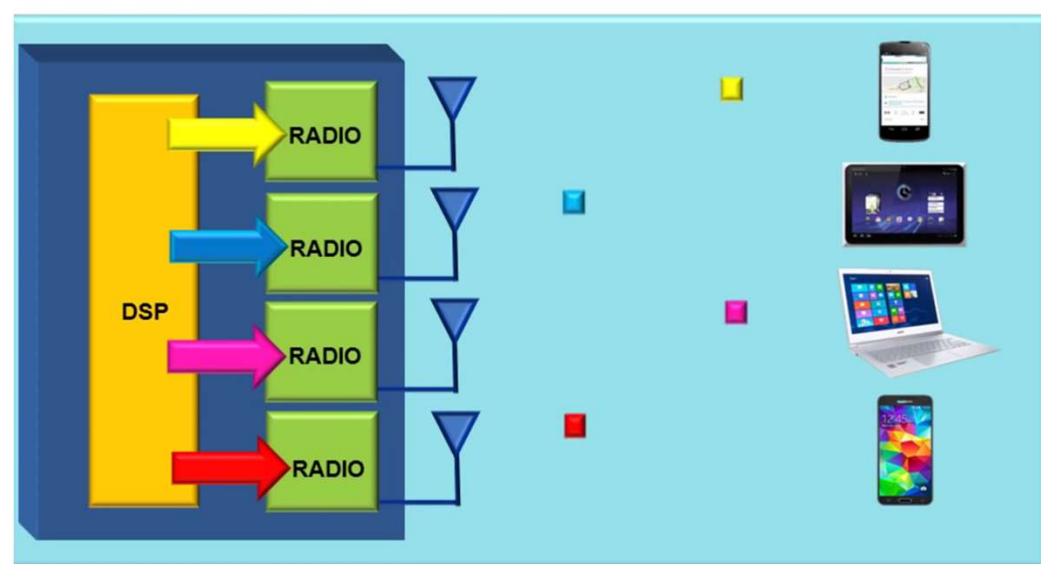
- MIMO is the acronym that refers to multiple input multiple output.
- MIMO exploits a RF phenomenon called multipath. Multipath transmission implies that signals will reflect off walls, doors, windows, and other obstructions. A receiver will see many signals each arriving at different times via different paths. Multipath tends to distort signals and cause interference, which eventually degrades signal quality (this effect is called multipath fading).
- With the addition of multiple antennas, a MIMO system can linearly increase the capacity of a given channel by simply adding more antennas. There are two forms of MIMO:
 - **Spatial diversity:** This refers to transmit-and-receive diversity. A single stream of data is transmitted on multiple antennas simultaneously using space-time coding. These provide improvements in the signal to noise ratio.
 - **Spatial multiplexing:** Used to provide additional data capacity by utilizing the multiple paths to carry additional traffic; that is, increasing the data throughput capability.

SU-MIMO vs MU-MIMO

Single User-Multiple In Multiple Out (SU-MIMO)



Multi User-Multiple In Multiple Out (MU-MIMO)



IEEE 802.11 packet structure

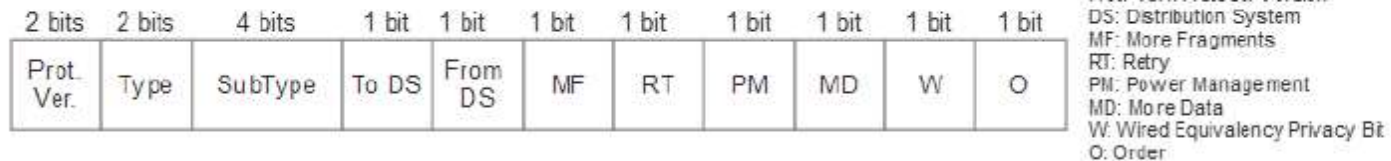
802.11 PHY Frame



802.11 MAC Frame



802.11 MAC Frame FC Header Details



Address fields: 802.11 can manage four MAC addresses in the following order:

- Address 1:** Receiver
- Address 2:** Transmitter
- Address 3/4:** Used for filtering

IEEE 802.11 operation

- An STA is considered a device equipped with a wireless network interface controller. An STA will always be listening for active communication in a specific channel. The first phase of connecting to Wi-Fi is the scanning phase.
- After a channel is selected, the device performing the scan will receive beacons and probe requests from nearby STAs. An access point may transmit a beacon, and if the STA receives the transmission, it may progress to join the network.

The beacon packet contains information needed by the STA:

- **SSID:** Service Set ID. 1 to 32-character network name (this field can optionally be hidden by setting the SSID length to zero. Even if it is hidden the other portions of the beacon frame are transmitted as usual.
- **BSSID:** Basic Service Set ID. Unique 48-bit following layer-2 MAC address conventions. Formed by the combination of the 24-bit Organization Unique Identifier and the manufacturer's assigned 24-bit identifier for the radio chipset.

IEEE 802.11 security

Types of authentication used on Wi-Fi WLANs and various strengths and weaknesses:

WEP: Wired equivalent privacy. This mode sends a key in plain text from the client. The key is then encrypted and sent back to the client. WEP uses different size keys but they are typically 128 bit or 256 bit. WEP uses a shared key, which means that the same key is available to all clients. It can be easily compromised by simply listening and sniffing for all the authentication frames coming back to clients joining a network to determine the key used for everyone.

WPA: Wi-Fi protected access (or WPA-Enterprise) was developed as the IEEE 802.11i security standard to replace WEP. One significant difference is WPA uses a **Temporal Key Integrity Protocol (TKIP)**, which performs per-packet key mixing and rekeying. This means that each packet will use a different key to encrypt itself, unlike in the case of WEP. Data can now be encrypted.

WPA-PSK: WPA pre-shared key or WPA-Personal. This mode exists where there is no 802.11 authentication infrastructure. Here, one uses a passphrase as a pre shared key. Each STA can have their own pre-shared key associated with its MAC address.

Wireless PAN: IEEE 802.15.1 & 802.15.4,
Zigbee

802.15 standards

- The 802.15 group was initially formed to focus on wearable devices (coining the phrase personal area network).
- Their work has expanded significantly and now focuses on higher data rate protocols, meter to kilometer ranges, and specialty communications.
- Over one million devices are shipped each day using some form of 802.15.x protocol.
- **802.15:** Wireless personal area network definitions
- **802.15.1:** Original foundation of the Bluetooth PAN
- **802.15.4:** Low data rate, simple, simple design, multi-year battery life specifications (Zigbee)

IEEE 802.15.4 architecture - Frequency

The IEEE 802.15.4 protocol operates in the unlicensed spectrum in three different radio frequency bands: 868 MHz, 915 MHz, and 2400 MHz.

868 MHz Band

Central Frequency	Channel
868 MHz	0

915 MHz Band

Central Frequency	Channel
906 MHz	1
908 MHz	2
910 MHz	3
912 MHz	4
914 MHz	5
916 MHz	6
918 MHz	7
920 MHz	8
922 MHz	9
924 MHz	10

2.4 GHz Band

Central Frequency	Channel
2405 MHz	11
2410 MHz	12
2415 MHz	13
2420 MHz	14
2425 MHz	15
2430 MHz	16
2435 MHz	17
2440 MHz	18
2445 MHz	19
2450 MHz	20
2455 MHz	21
2460 MHz	22
2465 MHz	23
2470 MHz	24
2475 MHz	25
2480 MHz	26

IEEE 802.15.4 architecture – Principle & Protocol Stack

To manage a shared frequency space, 802.15.4 and most other wireless protocols use some form of **Carrier Sense Multiple Access Collision Avoidance (CSMA/CA)**.

Since it is impossible to listen to a channel while transmitting on the same channel, collision detection schemes don't work; therefore, we use collision avoidance.

IEEE 802.15.4 Protocol Stack

Simplified OSI Model

Other Standard or Proprietary Layers		7. Application Layer
		6. Presentation Layer
		5. Session Layer
		4. Transport Layer
		3. Network Layer
IEEE 802.15.4 MAC Layer		2. Data Link Layer
IEEE 802.15.4 PHY (2.4 GHz Radio) (868/915 MHz Radio)		1. Physical Layer

Communications in IEEE 802.15.4

There are two types of communication in IEEE 802.15.4:

1. **Beacon** communication.
 2. **Beaconless** communication.
- For a ***beacon-based network***, the MAC layer can generate beacons that allow a device to enter a PAN as well as provide timing events for a device to enter a channel to communicate.
 - The beacon is also used for battery-based devices that are normally sleeping.
 - The device wakes on a periodic timer and listens for a beacon from its neighbors.
 - IEEE 802.15.4 allows for ***beacon-less networking***. This is a much simpler scheme where no beacon frame is transmitted by the PAN coordinator. It implies, however, that all nodes are in a receiving mode all the time. This provides full-time contention access using unslotted CSMA/CA.
 - This mode will consume much more power than beacon-based communication.

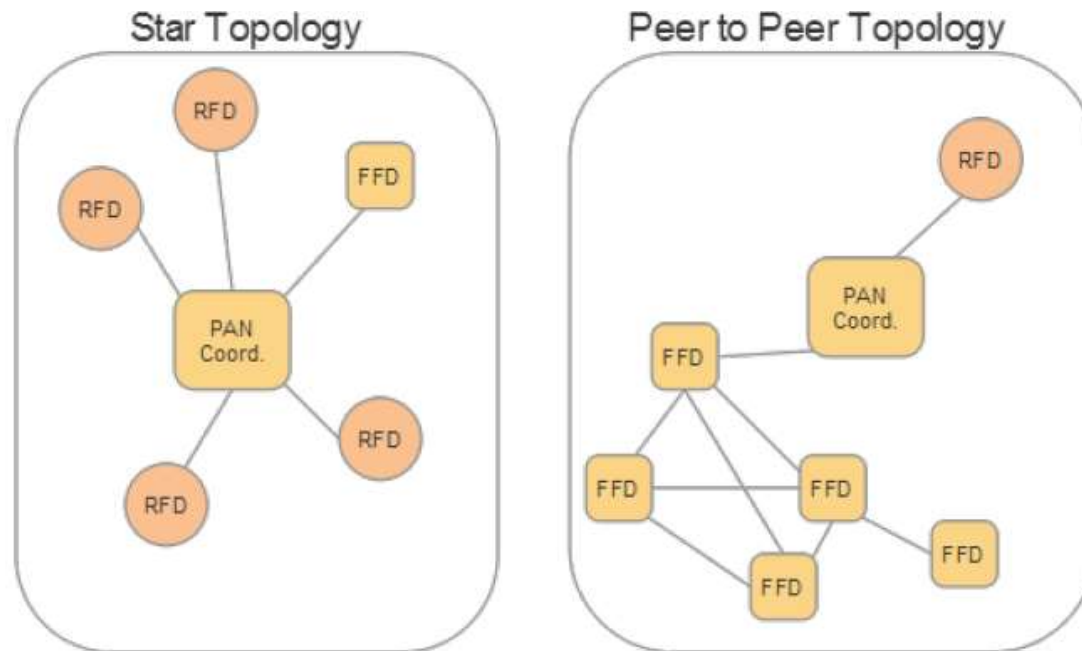
IEEE 802.15.4 topology

There are two fundamental device types in IEEE 802.15.4:

- **Full function device (FFD):** Supports any network topology, can be a network (PAN) coordinator and can communicate to any device PAN coordinator
- **Reduced function device (RFD):** Limited to only a star topology, cannot perform as a network coordinator, can only communicate with a network coordinator

The ***star topology*** is the simplest but requires all messages between peer nodes to travel through the PAN coordinator for routing.

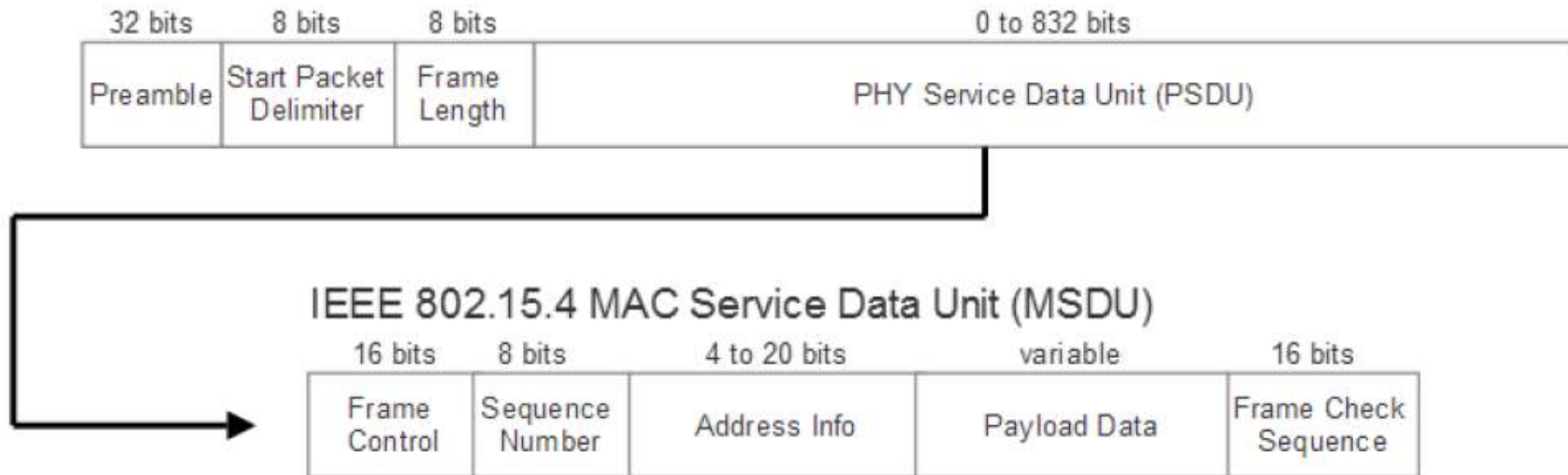
A ***peer-to-peer topology*** is a typical mesh and can communicate directly with neighbor nodes.



IEEE 802.15.4 address modes and packet structure

- The standard dictates that all addresses are based on unique **64-bit values** (IEEE address or MAC address).
- However, **to conserve bandwidth and reduce the energy of transmitting** such large addresses, 802.15.4 allows a device joining a network to "trade-in" their unique 64-bit address for a short **16-bit local address**, allowing for more efficient transmission and lower energy.

IEEE 802.15.4 PHY Packet



IEEE 802.15.4 start-up sequence

IEEE 802.15.4 maintains a process for startup, network configuration, and joining of existing

networks. The process is as follows:

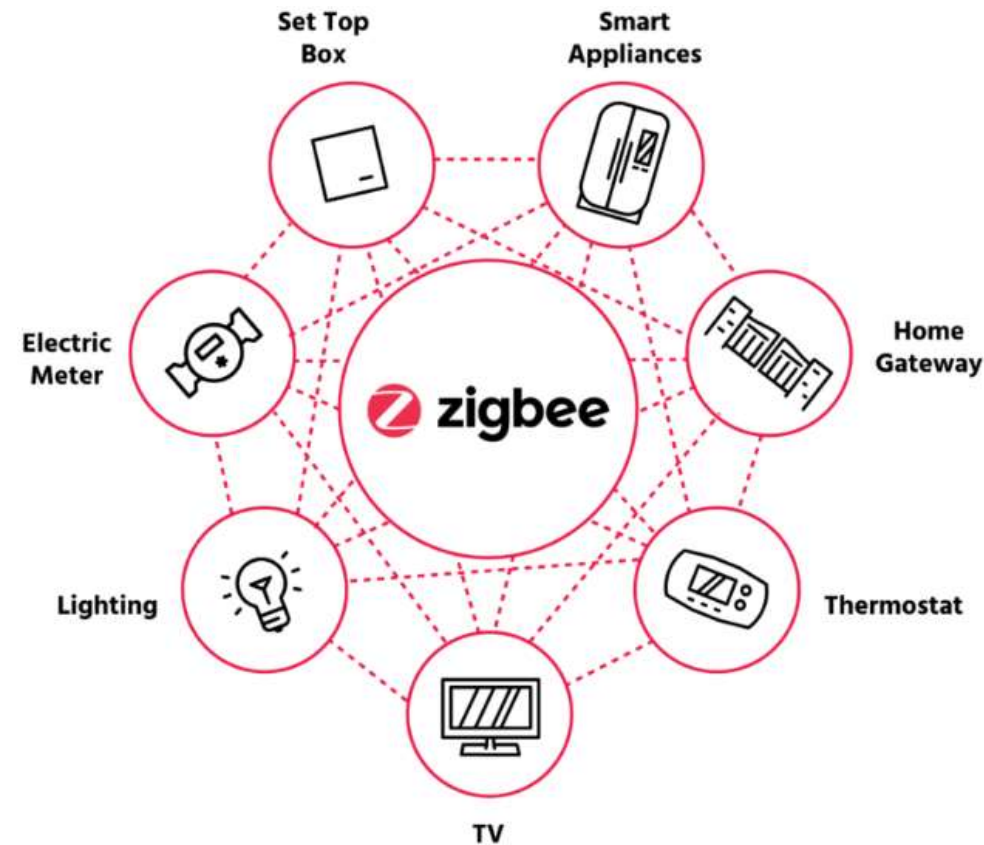
1. Device **initializes** its **stack** (PHY and MAC layers).
2. PAN **coordinator** is **created**. Each network has only one PAN coordinator.
3. The PAN coordinator will **listen** to **other networks** it has access to and **derives** a **PAN ID** that is unique to the PAN it will administer.
4. The PAN coordinator will **choose** a **specific radio frequency** to use for the network.
5. The network will be started by configuring the PAN coordinator and then **starting** the device in **coordinator mode**. At this point, the PAN coordinator can **accept requests**.
6. Nodes can join the network by finding the PAN coordinator using an active channel scan where it **broadcasts** a **beacon request** across all its frequency channels. In a beacon-based network, the PAN coordinator will routinely send out a beacon and the device can perform a passive channel scan and listen for the beacon. The device will then send an **association request**.
7. The PAN coordinator will determine if the **device should** or can join the network. If accepted, the PAN coordinator will **assign a 16-bit short address** to the device.

IEEE 802.15.4 security

- The IEEE 802.15.4 standard includes security provisions in the form of **encryption** and **authentication**. The architect has flexibility in the security of the network based on cost, performance, security, and power.
- AES-based encryption which uses a block cipher with a counter mode can be used.

Zigbee

- Zigbee is a WPAN protocol based on the IEEE 802.15.4 foundation targeted for commercial and residential IoT networking that is constrained by cost, power, and space.
- Zigbee got its name from the concept of a bee flying. As a bee flies back and forth between flowers gathering pollen, it resembles a packet flowing through a mesh network - device to device.



Zigbee Overview

- Zigbee is based on 802.15.4 but layers on network services similar to TCP/IP. It can form networks, discover devices, provide security, and manage the network.
- It does not provide data transport services or an application execution environment.
- It is essentially a mesh network, its self-healing and ad hoc in form.

There are three principal components in a Zigbee network.

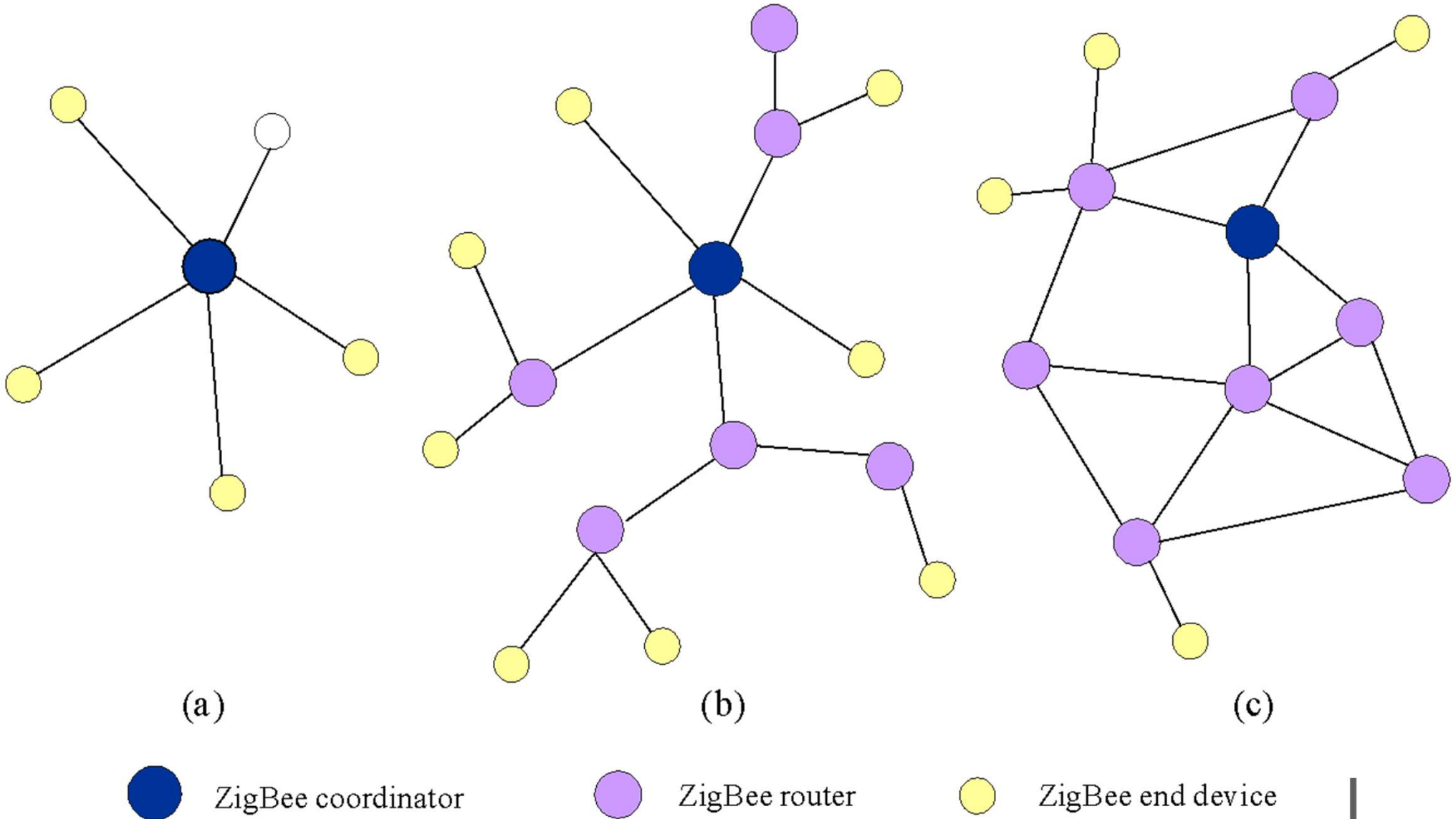
Zigbee controller (ZC): Highly capable device on a Zigbee network that is used to form and initiate network functions. Each Zigbee network will have a single ZC that fulfills the role of an 802.15.4 2003 PAN coordinator (FFD).

Zigbee router (ZR): This component is optional but handles some of a load of mesh network hopping and routing coordination. It too can fulfill the role of an FFD and has an association with the ZC.

Zigbee end device (ZED): This is usually a simple endpoint device such as a light switch or thermostat. It contains enough functionality to communicate with the coordinator. It has no routing logic; therefore, any messages arriving at a ZED that are not targeted to that end device are simply relayed.

Zigbee Topologies

Three kinds of networks are supported: **star**, **tree**, and mesh networks



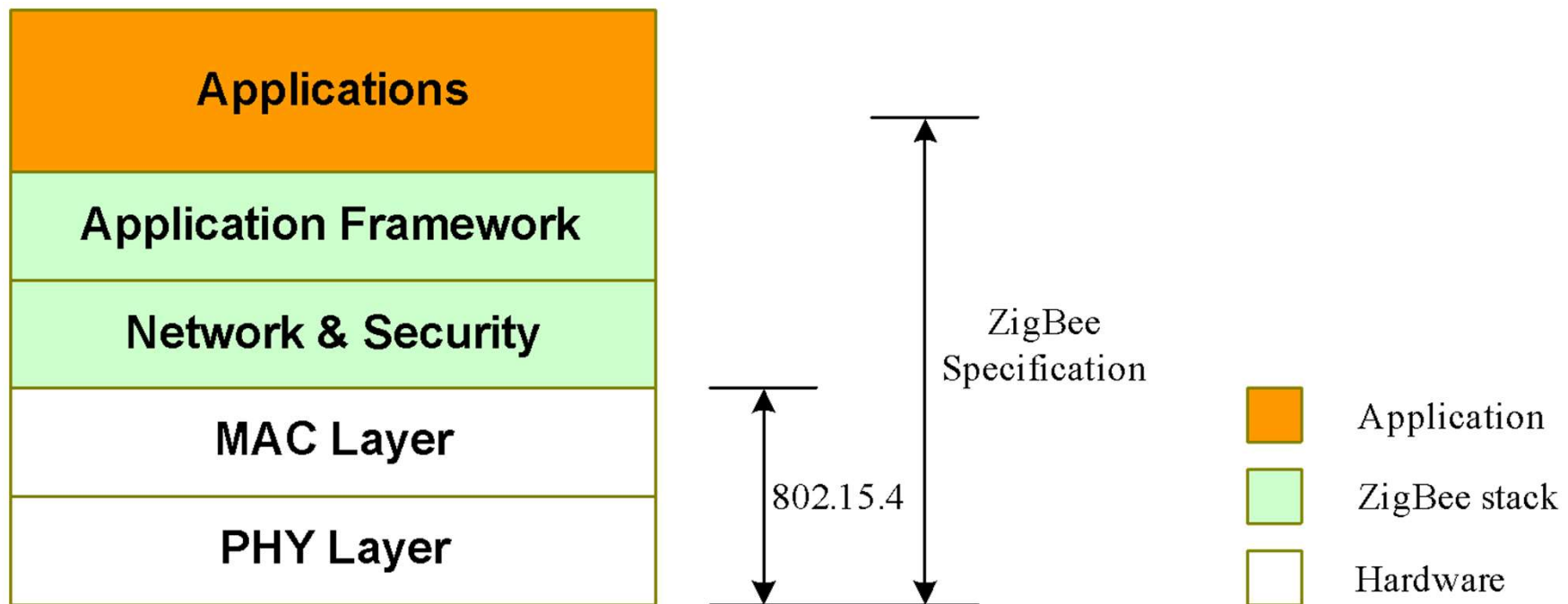
Zigbee Data Traffic

Zigbee targets three different types of data traffic.

- **Periodic data** is delivered or transmitted at a rate defined by the applications (for example, sensors periodically transmitting).
- **Intermittent data** occurs when an application or external stimulus occurs at a random rate. A good example of intermittent data suitable for Zigbee is a light switch.
- **Repetitive low latency data.** Zigbee allocates time slots for transmission and can have very low latency, which is suitable for a computer mouse or keyboard.

Zigbee PHY and MAC

- Zigbee operates primarily in the 2.4 GHz ISM band.
- It also operates at 868 MHz and 915 MHz because of the lower frequency, it has better propensity to penetrate walls and obstacles over traditional 2.4 GHz signals.
- Zigbee does not use all the IEEE802.15.4 PHY and MAC specifications.
- Zigbee does make use of the CSMA/CA collision avoidance scheme.
- It also uses the MAC level mechanism to prevent nodes from talking over each other.



Zigbee addressing

- The Zigbee protocol, as shown, resides on top of the 802.15.4 PHY and MAC layers and reuses its packet structures.
- The network diverges at the network and application layers.

Zigbee uses two unique addresses per node:

Long address (64 bit): Assigned by the manufacturer of the device and is immutable. Uniquely identifies the Zigbee device from all other Zigbee devices. This is the same as the 802.15.4 64-bit address. The top 24 bits refer to the organizational unique identifier (OUI) and the bottom 40 bits are managed by the OEM.

Short address (16 bit): This too is the same as the PAN ID of the 802.15.4 specification and is also optional.

Zigbee Routing Protocol

Zigbee can route packets in multiple manners:

- **Broadcasting:** Transmit packet to all other nodes in the fabric.
- **Mesh routing (table routing):** If a routing table for the destination exists, the route will follow the table rules accordingly. Very efficient. Zigbee will allow a mesh and table to route up to 30 hops away.
- **Tree routing:** Unicast messaging from one node to another. Tree routing is purely optional and can be disallowed from the entire network. It provides better memory efficiency than mesh routing since a large routing table doesn't exist. Tree routing does not have the same connection redundancy as a mesh, however. Zigbee supports tree routing hops up to 10 nodes away.
- **Source routing:** Used primarily when a data concentrator is present. This is how Z-Wave provides mesh routing.

Zigbee association

- **Zigbee end devices (ZED)** do not participate in routing. End devices communicate with the parent, who is also a router.
- When a **Zigbee coordinator (ZC)** allows for a new device to join a network, it enters a process known as an *association*. If a device loses contact with its parent, the device can at any time rejoin through the process known as *orphaning*.
- To formally join a Zigbee network, a *beacon request* is broadcast by a device to ask for subsequent beacons from devices on the mesh that are authorized to allow new nodes to join. At first, only the PAN coordinator is authorized to provide such a request; after the network has grown, other devices may participate.