WLANs, WPANs, and LP-WANs

DAT610 – Wireless Communications

Naeem Khademi

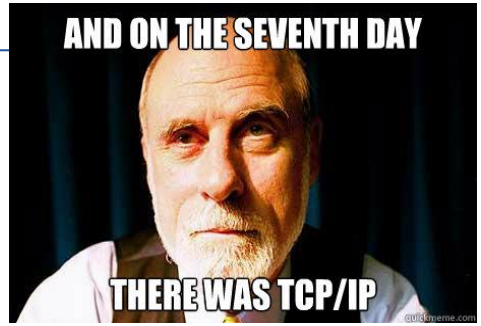
Associate Professor, IDE/UiS

naeem.khademi@uis.no

TCP/IP vs OSI Model

Open Systems Interconnection (OSI) by **ISO & ITU**
Developed/adopted
Late 70's, early 80's

Vint Cerf and **Robert Kahn** (1974); standards maintained by the IETF



Presentation layer: Translation of data between a networking service and an application; including character encoding, data compression and encryption/decryption

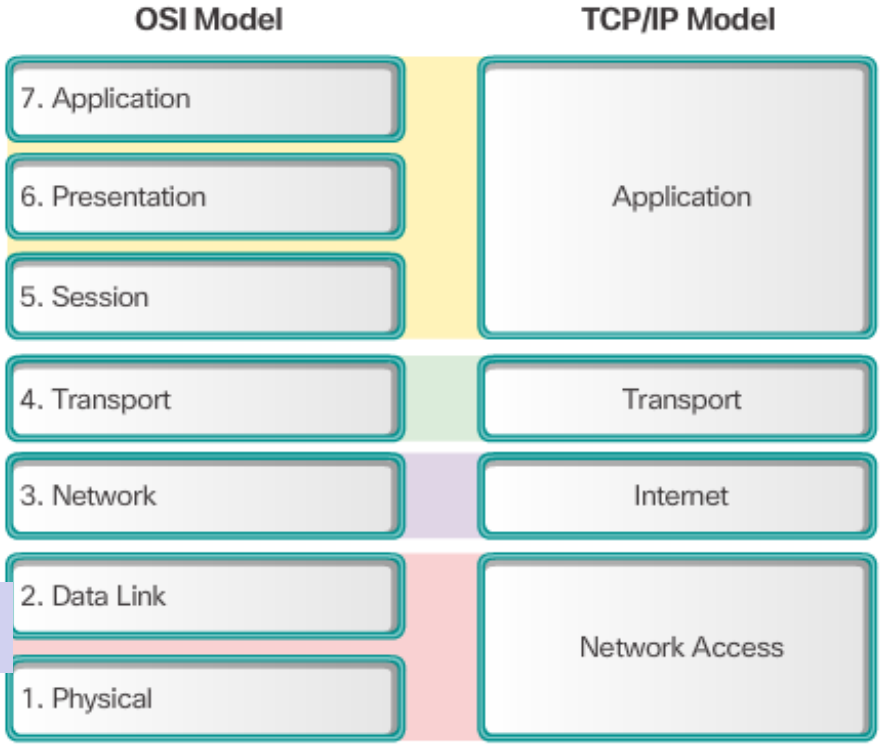
Session layer: Managing communication sessions, i.e., continuous exchange of information in the form of multiple back-and-forth transmissions between two nodes

Transport layer: **Reliable end-to-end communication** for services/applications, with flow control, multiplexing and connection-oriented communication

Network layer: Multi node/network data transfer, with **network addressing**, **routing** and **traffic control**

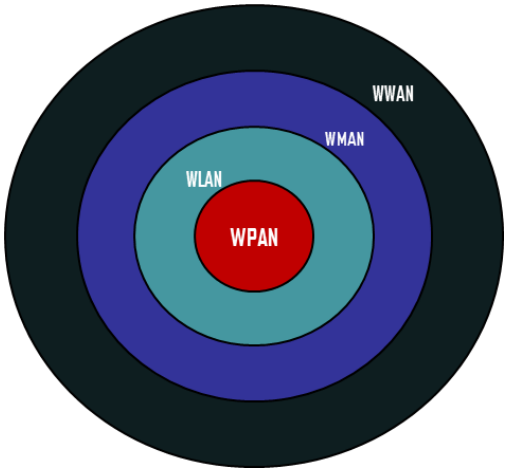
Datalink layer: **Reliable transmission** of data frames between two nodes **connected by a physical layer**

Physical layer: **Raw bit streams** over physical transmission medium

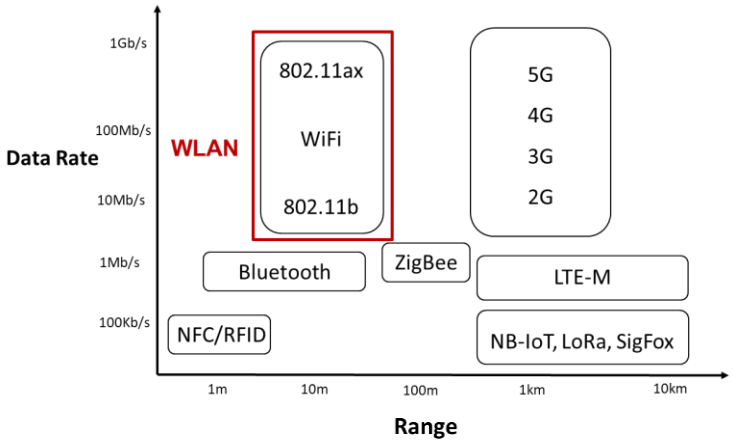


Why Wireless?

- **Wireless: voice and data through electromagnetic waves in open space**
  - **No wires:** Cheaper installation and less annoying to deal with cables!
  - **Connectivity:** anywhere, anytime, with mobility (possible to move around)
  - **Global coverage** where wire is unfeasible – e.g., in remote/rural areas, outer space, battlefield, offshore
  - **Flexible:** connect to multiple devices simultaniously



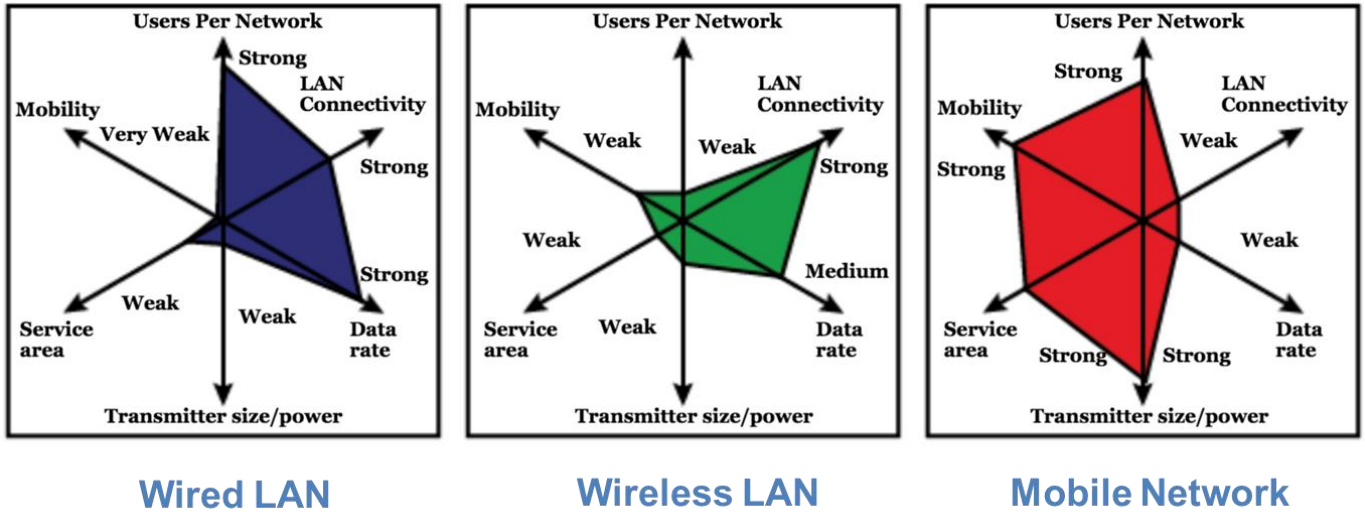
- **Wireless Personal-Area Network (WPAN):** low power and short-range (6-9 meters). Based on IEEE 802.15 std and 2.4 GHz freq. (e.g., Bluetooth and Zigbee)
- **Wireless LAN (WLAN):** medium sized nets up to about 90m. Based on IEEE 802.11 std and 2.4 or 5.0 GHz freq.
- **Wireless MAN (WMAN):** large geographic area such as city or district. Uses specific licensed frequencies.
- **Wireless WAN (WWAN):** extensive geographic area for national or global communication. Uses specific licensed frequencies.



Universitetet i Stavanger

WLAN

Wireless LANs

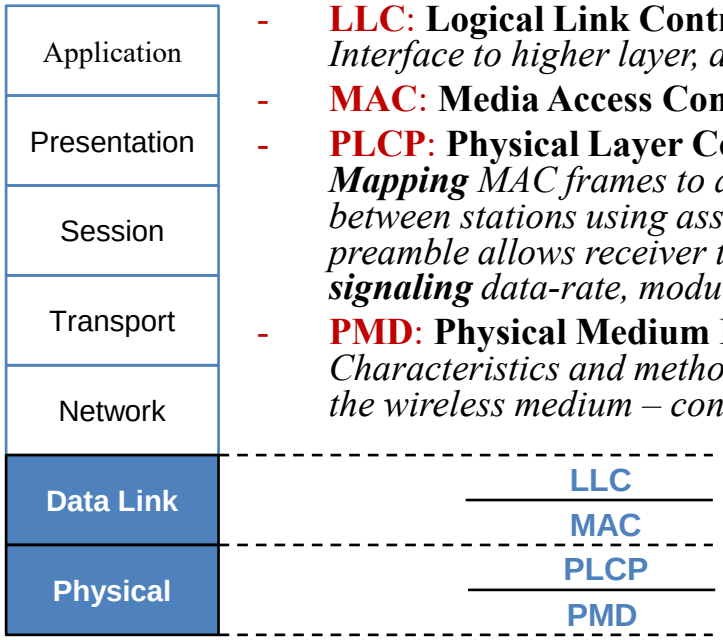


Wired LAN | Wireless LAN | Mobile Network

WLAN service requirements:

- Throughput: efficient use of wireless medium
- Number of nodes: hundreds of nodes
- Connection to backbone LAN
- Service Area: coverage area with diameter of 100 to 300 m
- Battery power consumption: long battery life
- Transmission robustness and security: no eavesdropping
- Collocated network operation: interference
- License-free operation
- Handoff/roaming
- Dynamic configuration

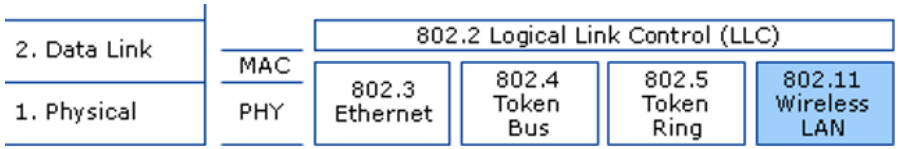
IEEE 802 Architecture



OSI Model

- **LLC: Logical Link Control**
  Interface to higher layer, address recognition, error control
- **MAC: Media Access Control**
- **PLCP: Physical Layer Convergence Procedure**
  ***Mapping** MAC frames to a format suitable for transferring information between stations using associated PMD system; **synchronization:** preamble allows receiver to sync and interpret the incoming signal; **signaling** data-rate, modulation and length in PLCP header.*
- **PMD: Physical Medium Dependent**
  Characteristics and method of transmitting and receiving data through the wireless medium – converting digital bits into suitable signals

Scope of IEEE 802 standards



IEEE 802.11: a set of specifications for implementing WLAN developed by working group 11 of the IEEE LAN/MAN Standards Committee (IEEE 802)

Wi-Fi: alliance which certifies that IEEE 802.11 products from different vendors will successfully interoperate.

Universitetet i Stavanger

IEEE 802.11 Standards (#1)

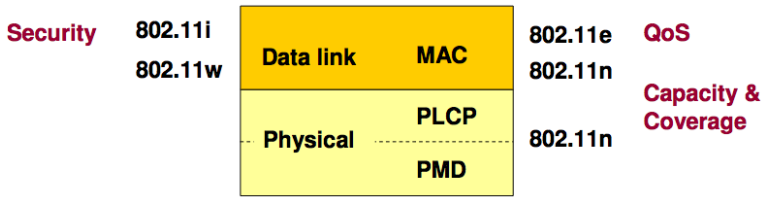
IEEE Std	Radio Frequency	Year	Description
802.11	2.4 GHz	1997	Data rates up to **2 Mb/s**
802.11a	5 GHz	1999	Data rates up to **54 Mb/s** Not interoperable with 802.11b or 802.11g
802.11b	2.4 GHz	1999 2001 (corr1)	Data rates up to **11 Mb/s** Longer range than 802.11a and better able to penetrate building structures
802.11g	2.4 GHz	2003	Data rates up to **54 Mb/s** Backward compatible with 802.11b
802.11n	2.4 and 5 GHz	2009	Data rates **150 – 600 Mb/s** Require multiple antennas with **MIMO technology**
802.11ac	5 GHz	2014	Data rates **up to 6.93 Gb/s** Supports up to **eight antennas (i.e., spatial streams)**
802.11ax	2.4 and 5 GHz	2021	High-Efficiency Wireless (HEW); **aka Wi-Fi 6 (2019)** **6 GHz band** (Wi-Fi 6E extension), up to **9.6 Gb/s**
802.11be	2.4 and 5 and 6 GHz	2025	Up to **16 spatial streams** Up to **46 Gb/s** **Multi-Link Operation (MLO)**, bonding multiple links – i.e., a single super channel

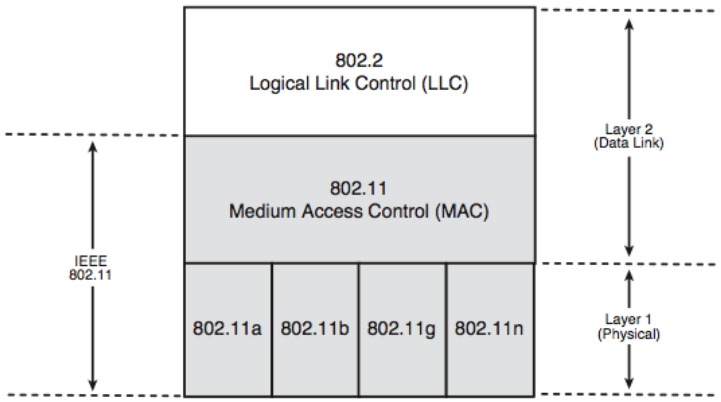
Universitetet i Stavanger

IEEE 802.11 Standards (#2)

IEEE Std	Year	Description
802.11c	2004	**Bridge operation procedures;** included in the IEEE 802.1D standard (2001)
802.11d	2001	Specification for Operation in Additional Regulatory Domains
802.11e	2005	Enhancements to 802.11 to support **QoS differentiation** at MAC Layer, inclusion of packet bursting
802.11f	2003-2006	Withdrawn; Recommended Practice for Multi-Vendor Access Point Interoperability via an Inter-Access Point Protocol (IAPP) Across Distribution Systems Supporting IEEE 802.11 Operation.
802.11h	2004	Spectrum and Transmit Power Management Extensions in the 5GHz band in Europe. This has been introduce in order to control transmission power since in Europe the IEEE 802.11 systems can interfere with RADAR
802.11i	07/2004	Define new security mechanisms for user authentication, data ciphering on radio channel. It has been proposed in order to solve the security problems of the first version of standard. The standard is based on IEEE 802.1X authentication architecture, dynamic management of ciphering keys, AES ciphering algorithm
802.11j	2004	802.11 and 802.11a PHY 5 GHz operation in Japan
802.11k	2008	Radio Resource Measurements of WLANs
802.11p	2010	WAVE - Wireless Access for the **Vehicular Environment** (such as ambulances and passenger cars)
802.11r	2008	Fast BSS-Transition
802.11s	2011	**ESS Mesh Networking**
802.11u	2011	Interworking with external networks (e.g., cellular)
802.11v	2011	Wireless network management
802.11w	2009	Protected Management Frames
802.11y	2008	3650-3700 Operation in the U.S.
802.11z	2010	Extensions to Direct Link setup
802.11aa	2012	Robust streaming of Audio Video Transport Streams
802.11ay	2020	Enhanced Throughput in License-Exempt Bands above 45 GHz, while ensuring backward compatibility and coexistence with legacy directional multi-gigabit stations (defined by IEEE 802.11ad-2012 amendment) operating in the same band. Improvements of the PHY/MAC layers aimed at enabling at least one mode of operation capable of supporting a max throughput of at least 20 Gbps, while maintaining or improving the power efficiency per station.

IEEE 802.11 Standards (#3)





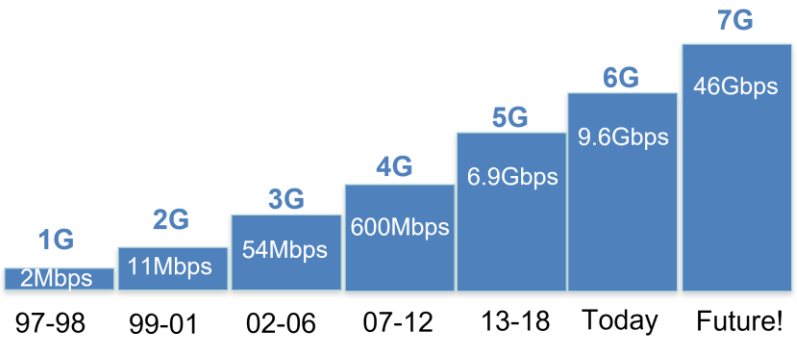
802.11 PHY layer

Version	WiFi 4	WiFi 5	WiFi 6	WiFi 6E	WiFi 7
Year	2007	2013	2019	2020	2024
Protocol	802.11n	802.11ac	802.11ax	802.11ax	802.11be
Bands	2.4 / 5 GHz	5 GHz only	2.4 / 5 GHz	2.4 / 5 / 6* GHz	2.4 / 5 / 6 GHz
Peak Speed	600 Mb/s	6.9 Gb/s	9.6 Gb/s	9.6 Gb/s	46 Gb/s
Channel Widths	20 / 40 MHz	20 / 40 / 80 / 160 MHz	20 / 40 / 80 / 160 MHz	20 / 40 / 80 / 160 MHz	20 / 40 / 80 / 160 / 320 MHz
Security	WPA2	WPA2	WPA3	WPA3	WPA3
Key Features	4 x 4 MIMO	8 x 8 MIMO	8 x 8 MIMO	8 x 8 MIMO	16 x 16 MIMO
	LDPC Error Correction	4 x DL MU-MIMO	8 x DL MU-MIMO	8 x DL MU-MIMO	16 x DL & UL MU-MIMO
	64-QAM	Beam Forming	Beam Forming	Beam Forming	Multi-AP
		256-QAM	OFDMA	OFDMA	Multi-RU Puncturing
			TWT	TWT	Multi-Link
			1024-QAM	1024-QAM	Beam Forming
				*6 GHz added, USA Only	OFDMA
					TWT
					4096-QAM

Evolution to WiFi 7

IEEE 802.11 PHY

- **PHY data rate is determined by:**
  - Channel Width: size of freq. band.
  - Modulation and Coding Scheme **(MCS)**
  - number of Spatial Streams **(SS)**
  - Guard Interval **(GI)**, to prevent inter-symbol interference (ISI)



IEEE Std (Band GHz)	Transmission Scheme	Modulation
802.11a (5)	OFDM	BPSK, QPSK, 16-QAM, 64-QAM
802.11b (2.4)	DSSS	BPSK, QPSK, CCK
802.11g (2.4,5)	DSSS, OFDM	BPSK, QPSK,CCK, 16-QAM, 64-QAM
802.11n (2.4,5)	MIMO-OFDM	BPSK, QPSK, 16-QAM, 64-QAM
802.11ac (5)	MIMO-OFDM	Same as .11n but with **256-QAM**
802.11ax (2.4,5)	OFDMA	Same as .11ac but with **1024-QAM**
802.11be (2.4,5,6)	OFDMA	Same as .11ax but with **4096-QAM**

Technology	20 MHz[a]	40 MHz	80 MHz	160 MHz
802.11b	11 Mbps			
802.11a/g	54 Mbps			
802.11n (1 SS)	72 Mbps	150 Mbps		
802.11ac (1 SS)	87 Mbps	200 Mbps	433 Mbps	867 Mbps
802.11n (2 SS)	144 Mbps	300 Mbps		
802.11ac (2 SS)	173 Mbps	400 Mbps	867 Mbps	1.7 Gbps
802.11n (3 SS)	216 Mbps	450 Mbps		
802.11ac (3 SS)	289 Mbps	600 Mbps	1.3 Gbps	2.3 Gbps[b]
802.11n (4 SS)[c]	289 Mbps	600 Mbps		
802.11ac (4 SS)	347 Mbps	800 Mbps	1.7 Gbps	3.5 Gbps
802.11ac (8 SS)	693 Mbps	1.6 Gbps	3.4 Gbps	6.9 Gbps

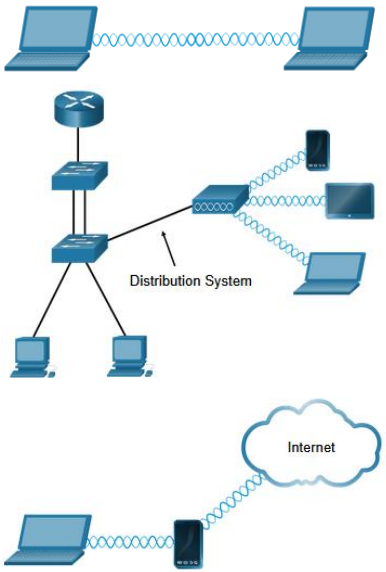
Data rate per channel width.

QAM: Quadrature Amplitude Modulation; encodes data by varying both the amplitude and phase. 16-QAM 4-bit per symbol; 256-QAM 8 bits per symbol. Higher order QAM is more sensitive to noise.

CCK: Complementary Code Keying; encodes 4 or 8 bits per symbol using complex spreading codes (complementary codes)

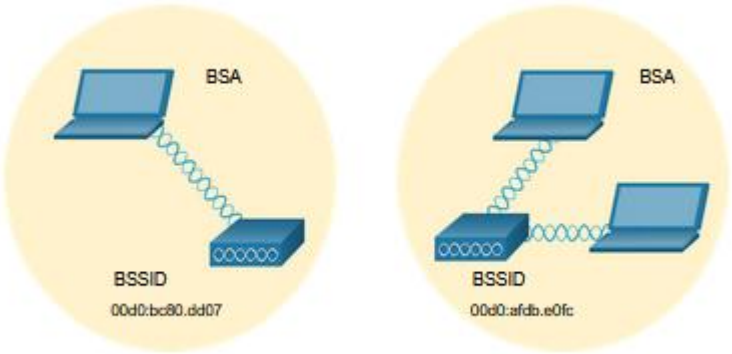
802.11 WLAN Architecture

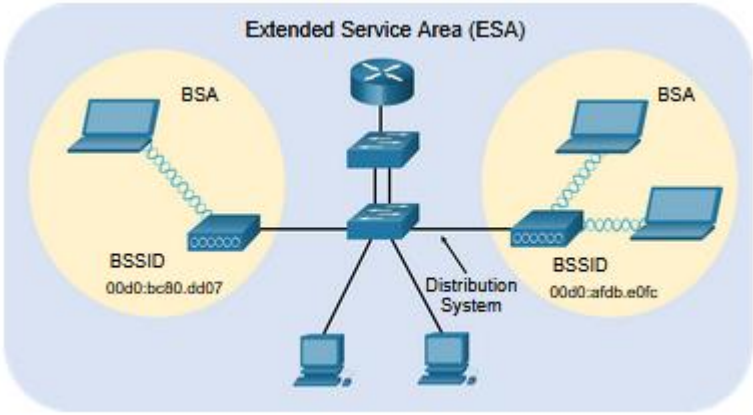
- **802.11 topology modes:** ad-hoc (p2p without AP), infrastructure (connect clients through an AP) and tethering (type of ad-hoc for creating personal hotspot – e.g., via a cellular-enabled tablet/phone)



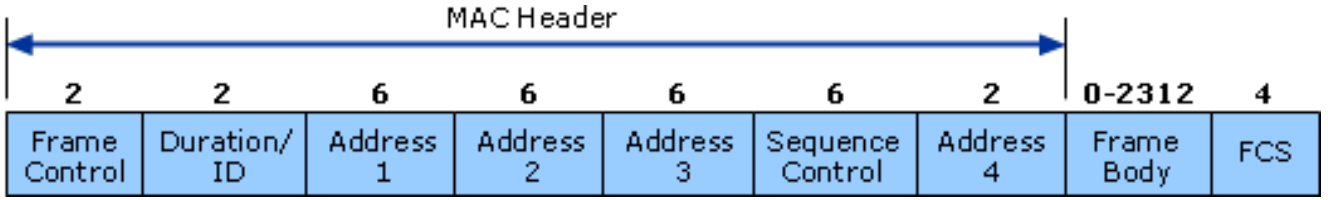
- **Infrastructure mode:** BSS and ESS
  - **Basic Service Set (BSS):** single AP to interconnect all wireless clients within the same BSS.
  - **Extended Service Set (ESS):** a union of two or more BSS interconnected by wired distro systems. Clients in each BSS can communication through ESS and can roam between them.

- **BSSID:** MAC addr of the AP's NIC the client is connected to.
- **ESSID (aka SSID):** network's name e.g. "eduroam"





IEEE 802.11 MAC



- **CSMA/CA with RTS/CTS and DCF**
  - Contention Service
- **Point Coordination Function (PCF)**
  - Contention-free Service

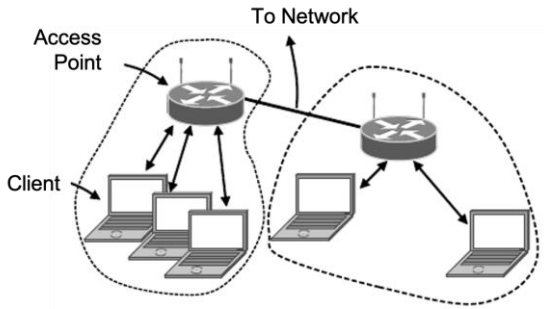
- **Frame control:** frame type (**control** - indicates start/stop/retransmit, **management** - negotiation between AP and STA, or **data**), control information
- **Duration/connection ID:** channel allocation time.
- **Addresses:** source, destination and AP MAC addresses.
- **Sequence control:** numbering and reassembly.
- **Frame Check Sequence (FCS):** 32-bit Cyclic Redundancy Check (CRC).

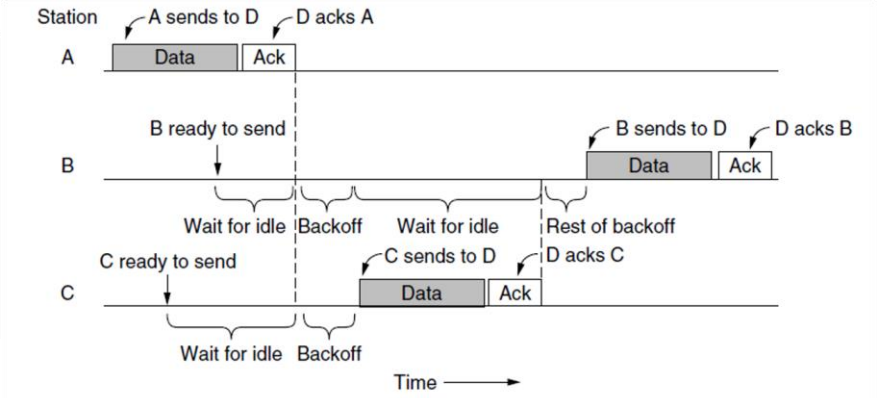
CSMA/CA with RTS/CTS

- WLANs are half-duplex (can send and receive but not at the same time!)
- Client cannot "listen" while sending => impossible to detect a collision (CD).
- WLANs use **Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA)** to determine how and when to send data.

A wireless client does the following:

a) Listens to channel to see if idle – i.e., no other traffic currently on the channel. (Carrier Sense)
b) Sends a **Ready to Send (RTS)** message to AP to request dedicated channel access. (Optional)
c) Receives a **Clear to Send (CTS)** message from AP granting access to channel. (Optional)
d) Waits a random amount of time before restarting the process if no CTS message received/channel busy. (Collision Avoidance)
e) Transmits the data!
f) Acknowledges all transmissions. If a wireless client does not receive an acknowledgment, it assumes a collision occurred and restarts the process





CN5E by Tanenbaum & Wetherall, © Pearson Education-Prentice Hall and D. Wetherall, 2011

Wireless LAN Security (#1)

- Two early security feature: SSID Cloacking and MAC address filtering
  - **SSID Cloacking:** SSID beacon frame disabled on AP. Wi-Fi clients must be manually configured with the SSID.
  - **MAC address filtering:** admin manually permit/deny clients based on their MAC addr.

- 802.11 original authentication methods: Open system (no password, client must use own VPN) and Shared key (WEP, WPA, WPA2, WPA3 to authenticate and encrypt data; password must be pre-shared)

Authentication Method	Description
Wired Equivalent Privacy (WEP)	The original 802.11 spec designed to secure the data using the **Rivest Cipher 4 (RC4)** encryption method with a static key. **WEP is no longer recommended and should never be used.**
Wi-Fi Protected Access (WPA)	A Wi-Fi Alliance standard that uses WEP but secures the data with the much stronger **Temporal Key Integrity Protocol (TKIP)** encryption algorithm. TKIP changes the key for each packet, making it much more difficult to hack.
WPA2	It uses the **Advanced Encryption Standard (AES)** for encryption. **AES is currently considered the strongest encryption protocol.**
WPA3	This is the next generation of Wi-Fi security. All WPA3-enabled devices use the latest security methods, **disallow outdated legacy protocols**, and require the use of Protected Management Frames (PMF).

Wireless LAN Security (#2)

- Home routers typically have two authentication choices: WPA or WPA2. WPA 2 has two authentication methods:
  - **Personal:** for SOHO networks, users authenticate with a **pre-shared key (PSK)**. No server required.
  - **Enterprise:** for enterprise nets. Requires a Remote **Authentication Dial-In User Service (RADIUS)** authentication server. The device must be authenticated by the RADIUS server and then users must **authenticate using 802.1X standard**, which uses the Extensible **Authentication Protocol (EAP)** for authentication.

- WPA/WPA2 have two encryption protocols:
  - **Temporal Key Integrity Protocol (TKIP):** used by WPA. Provides support for legacy WLAN equipment by addressing the original flaws of WEP. It makes use of WEP, but encrypts L2 payload using TKIP, and carries out a **Message Integrity Check (MIC)** in the encrypted packet to ensure the message has not been altered.
  - **Advanced Encryption Standard (AES):** used by WPA2 and uses the **Counter Cipher Mode with Block Chaining Message Authentication Code Protocol (CCMP)** that allows destination hosts to recognize if the encrypted and non-encrypted bits have been altered.

- **Enterprise authentication** requires AAA RADIUS server; required info are RADIUS server IP addresses, UDP port numbers (1812 for RADIUS Authentication, and 1813 for RADIUS Accounting; can also use ports 1645 and 1646) and Shared Key (to authenticate with RADIUS server)

Wireless LAN Security (#3)

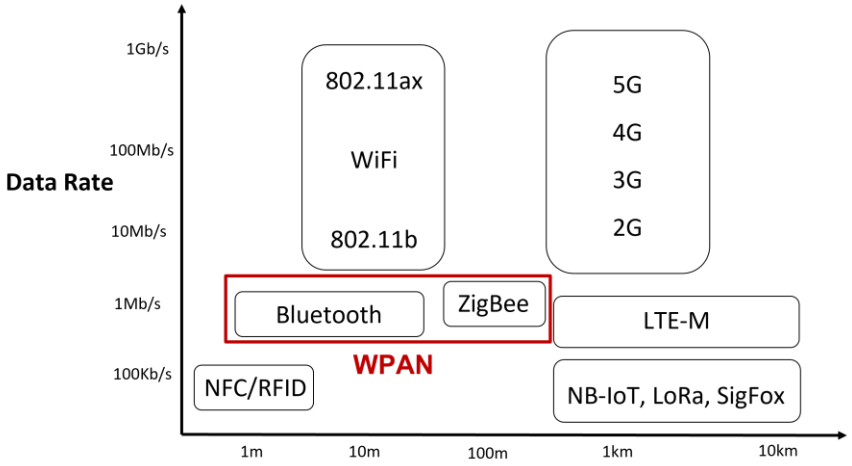
- Because WPA2 is no longer considered secure, WPA3 is recommended when available. WPA3 includes four features:
  - **WPA3 – Personal:** thwarts brute force or dictionary attacks by using **Simultaneous Authentication of Equals (SAE)**.
  - **WPA3 – Enterprise:** uses 802.1X/EAP authentication. However, it requires the use of a **192-bit cryptographic suite** and eliminates the mixing of security protocols for previous 802.11 standards.
  - **Open Networks:** does not use any authentication. However, uses **Opportunistic Wireless Encryption (OWE)** to encrypt all wireless traffic.
  - **IoT Onboarding:** uses **Device Provisioning Protocol (DPP)** to quickly onboard headless (i.e., no GUI) IoT devices. **WPS** in WPA2 vulnerable to a variety of attacks and not recommended.
    - **DPP:** each headless device has a hardcoded public key. The key is typically stamped on the device as a QR code. The net admin can scan the QR and quickly onboard the device. Although not strictly part of the WPA3, DPP will replace WPS over time.

Universitetet i Stavanger

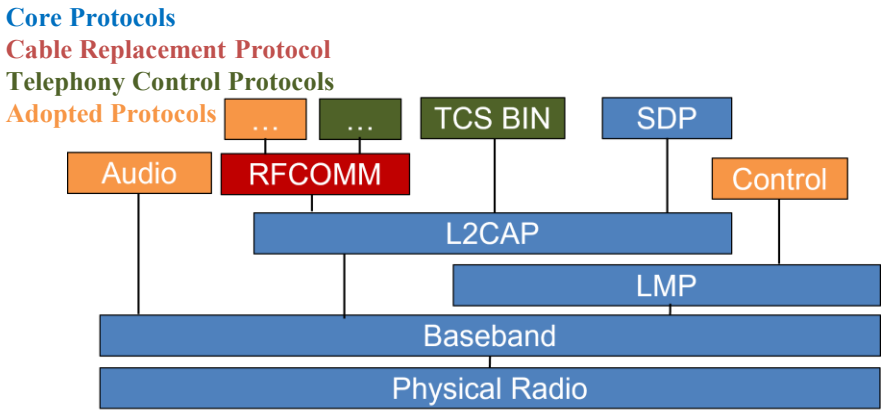
WPAN

Wireless Personal Area Networks (WPAN)

- **WPAN**
  - **IEEE 802.15.1 (Bluetooth)**
  - IEEE 802.15.3 (high-rate WPAN)
  - IEEE 802.15.4
    - ZigBee
    - 6LoWPAN



- **Bluetooth:** managed by the Bluetooth Special Interest Group
- "Always-on, short-range radio hookup"
- Robust, low power, low cost
- Application areas:
  - Data and voice access points
  - Cable replacement
  - Ad-hoc networking
- Standards:
  - Core specifications: *protocol architecture (from radio to link)*
  - Profile specifications: *usage models (subset of core specs)*



LMP: Link Manager Protocol
L2CAP: Logical link Control and Adaptation Protocol
SDP: Service Discovery Protocol
RFCOMM: Radio Frequency Communication
TCS BIN: Telephony Control Specification – Binary

Bluetooth Profiles

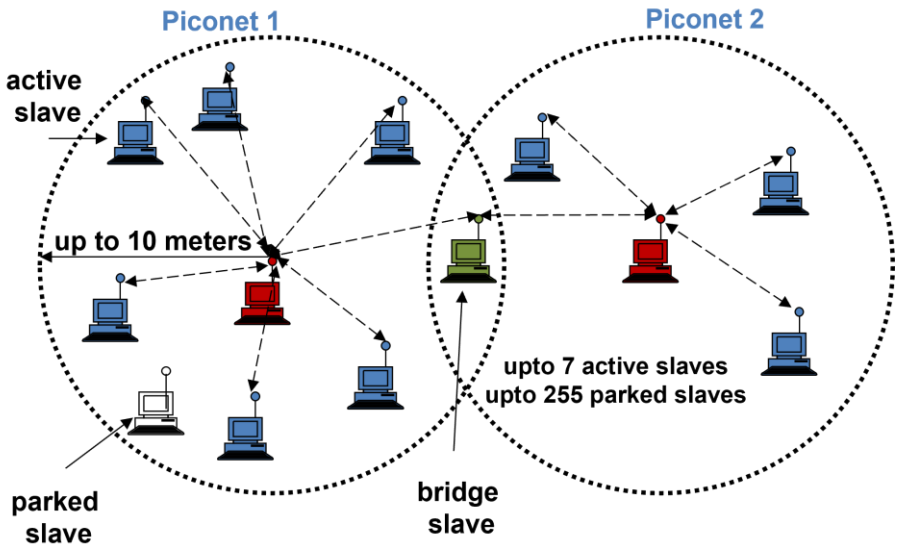
- **Profile**: set of protocols that implement a particular Bluetooth-based function/application (usage model) on top of Bluetooth protocol stack. “rulebook” telling a device:
  1. Which protocols to use
  2. How to format and exchange data
  3. How to manage the connection

Bluetooth Profile	Purpose	Protocols Used
HSP (Headset Profile)	Connects headset for voice calls	RFCOMM, SDP
HFP (Hands-Free Profile)	Car kits, hands-free calling	RFCOMM, SDP, AT commands
A2DP (Advanced Audio Distribution Profile)	Stereo audio streaming	L2CAP, SBC codec, RTP
AVRCP (Audio/Video Remote Control Profile)	Play/pause/skip control for audio/video	L2CAP, AVRCP commands
SPP (Serial Port Profile)	Emulates RS-232 serial link	RFCOMM
OBEX (Object Exchange)	File transfer, contact exchange	RFCOMM, L2CAP
HID (Human Interface Device)	Keyboards, mice, game controllers	L2CAP, HID protocol
MAP (Message Access Profile)	Accessing SMS/email	RFCOMM, OBEX

Bluetooth Networks – Piconets & Scatternets

- **Piconet**: basic unit (i.e., building block) of networking in Bluetooth. All devices share the same frequency hopping pattern determined by Master. Both data and voice.
  - **Master:** determines the channel access, freq. hopping and timing. Time-Division Multiplexing (TDD) used.
  - **1 to 7 Slaves:** communicate only with master

- **Scatternet:** network of multiple interconnected piconets. Devices belonging to multiple piconets are called "bridge devices" acting as "relays" switching between piconets using time-sharing.



A scatternet of 2 piconets

Bluetooth Specifications

	Topology	Up to 7 simultaneous links in a logical star
Radio Specification	Modulation	GFSK
	Peak data rate	1 Mbps
	RF bandwidth	220 kHz (–3 dB), 1 MHz (–20 dB)
	RF band	2.4 GHz, ISM band
	RF carriers	23/79
Baseband Specification	Carrier spacing	1 MHz
	Transmit power	0.1 W
	Piconet access	FH-TDD-TDMA
	Frequency hop rate	1600 hops/s
	Scatternet access	FH-CDMA

- Specifications for **Basic Rate (BR) 1.1 (2002)**

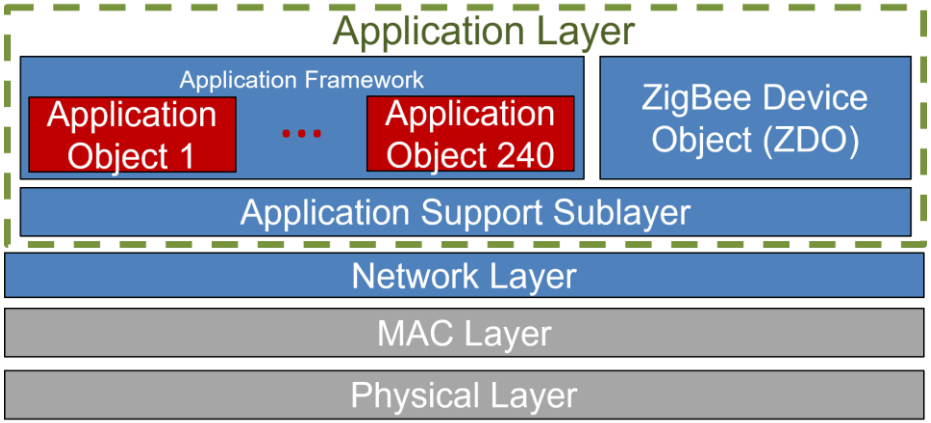
- Follow up versions:
  - **2.0 (2004):** Enhanced Data Rate (EDR)
  - **3.0 (2009):** High Speed with 802.11 Wi-Fi radio
  - **4.0 (2010):** Low-energy protocol
  - **5.0 (2016):** 4X range, 2x speed, 8x message capacity + IoT
  - **5.4 (2023):** Last subversion: security and performance enhancements

IEEE 802.15.4 – ZigBee

- **IEEE 802.15.4**: PHY and MAC for low-rate WPAN in ISM bands – e.g., 868 MHz, 915 MHZ, and 2.4 GHz.

- **ZigBee:** a protocol suite based on 802.15.4 maintained by **Zigbee Alliance** for small, low-power radio.
  - **Applications:** low data-rate, long battery life, secure networking.
  - **Versions:** ZigBee, and ZigBee Pro
  - **Spec. add-ons:**
    - ZigBee IP specification (ZigBee over IPv6)
    - ZigBee Radio Frequency for Consumer Electronic Devices (RF4CE)

- IEEE 802.15.4 defined
- ZigBee defined
  - **ZDO** keeps device role, manage request to join the network, discover devices, and manage security
  - **ZCL:** Zigbee Cluster Library; defines standard clusters, attributes, and commands so Zigbee devices can interoperate across manufacturers.
  - **APS:** Reliable delivery, binding, group management.
  - **NWK:** Addressing, routing, network formation, security
- End manufacturer defined

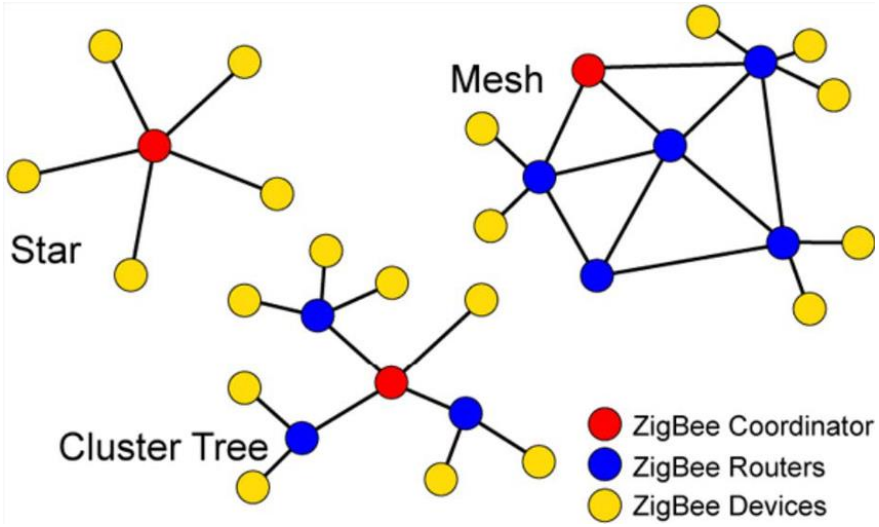


ZigBee Topologies

- Three main topologies: star, mech and cluster tree.
  - Coordinator manages the network, assigns addresses
  - Routers relay messages

- ZigBee automatically constructs low-speed ad-hoc network
  - **Mesh:** Ad hoc On-Demand Distance Vector (AODV) Like Routing simplified for low-power (AODVjr)
  - **Tree:** tree-based routing, hierarchical

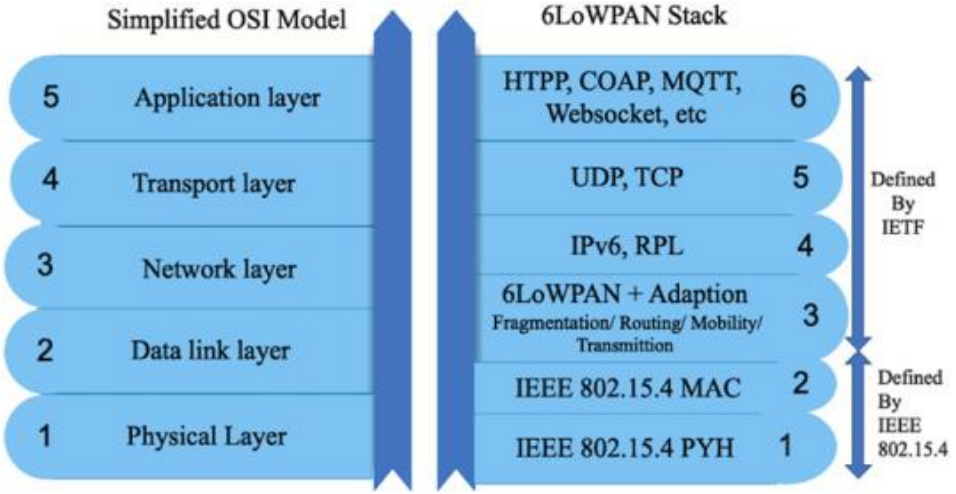
- Two types of networks:
  - **Non-beacon-based networks**
    No time sync, routers always on, mesh topology
  - **Beacon-based networks**
    Periodic beacons, star or tree topology



6LoWPAN

- **6LoWPAN:** IPv6 over Low-Power Wireless Personal Area Networks
  - IP over small, resource-constrained, low-power (IoT) devices
  - IEEE 802.15.4 as PHY/MAC layers
  - IETF base specification is RFC4944
  - How to transmit IPv6 datagrams (elephants) over low power IoT devices (mice)?

- **6LoWPAN Adaptation Layer**
  - Header compression and fragmentation (RFC6282)
  - Mapping from IPv6 to IEEE 802.15.4 frames
    - *Maximum Transmission Unit (MTU)* from 1280B to 127B
    - *Address resolution* from 128 bits to 64 or 16 bits short MAC addresses



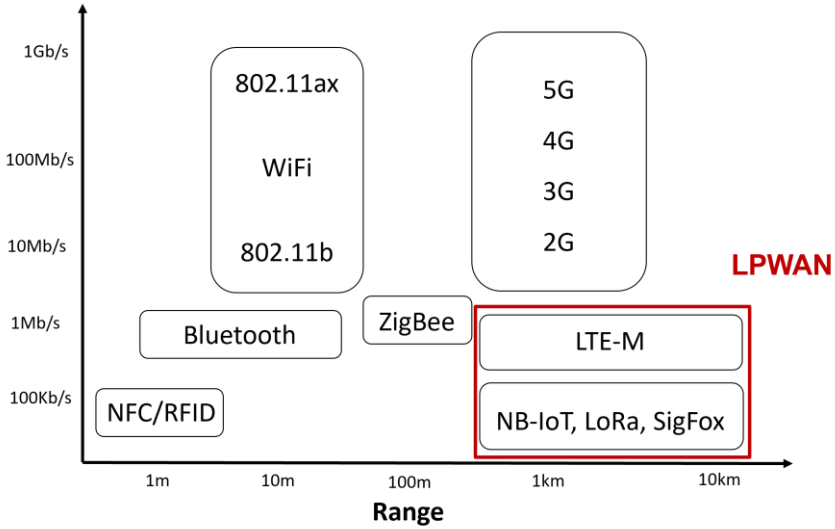
Source: https://www.sciencedirect.com/science/article/pii/S1084804523001789

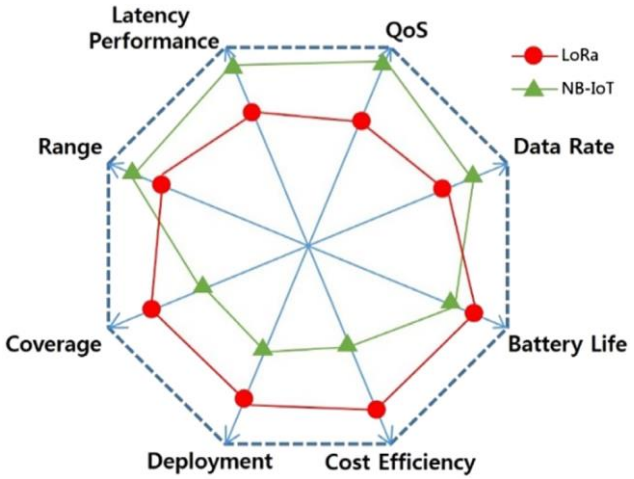
Universitetet i Stavanger

LP-WAN

LP-WAN

- **Low Power Wide Area Networks (LP-WAN) characteristics:**
  - Long-range
  - Low data-rate
  - High connectivity
  - Low power (i.e., “things” with battery)
  - Low Cost!

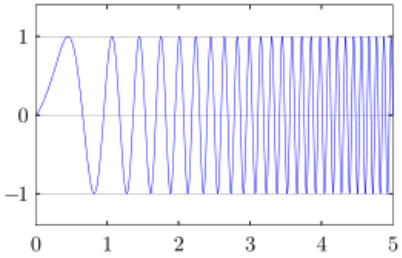




Source: Rashmi Sharan Sinha, Yiqiao Wei, Seung-Hoon Hwang; A survey on LPWA technology: LoRa and NB-IoT; ICT Express, Volume 3, Issue 1,2017, Pages 14-21

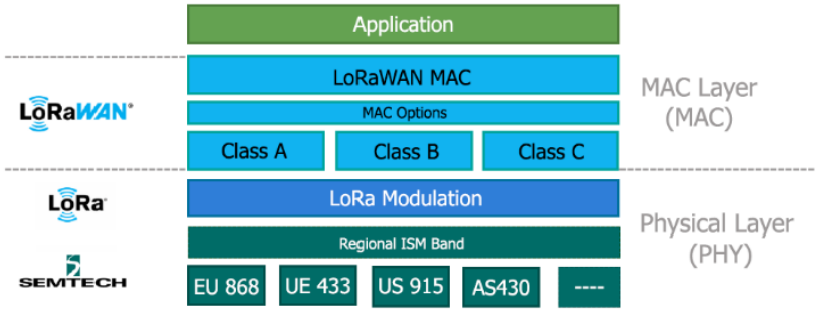
LoRa

- **LoRa (Long-Range technology):**
  - **Proprietary**, developed by Semtech Corporations. Maintained by LoRa Alliance
  - **Range:** 2-5km in urban areas and 15km in rural areas
  - Devices can run for years on small batteries!
  - Optimized for small packets of data – rates of 0.3 Kbps – 27 Kbps.
  - Operating in sub-GHz ISM-bands (868 MHz, 915 MHz, and 433 MHz)
  - **Chirp Spread Spectrum Modulation (CSS)** modulation enabling long-range communication. Modulating frequency over time (chirping)
  - Sweeping from *low-to-high* (upchirp) or *high-to-low* (down-chirp)
  - Cheaper than DSSS (no accurate sync needed.)
  - Uses **FEC codes** for resilience against interference



  - **LoRA:** PHY/modulation technology
  - **LoRAWAN:** MAC and network layers

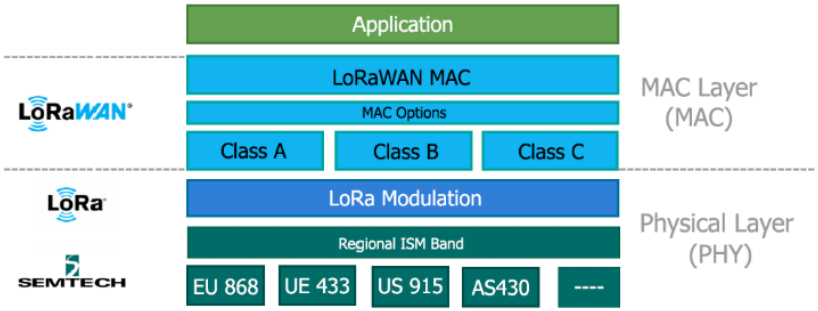
  - **LoRa Geolocation:** locating devices using network metrics – e.g., TDoA, RSSI – or GNSS module.



Source: https://www.iieta.org/journals/isi/paper/10.18280/isi.270401

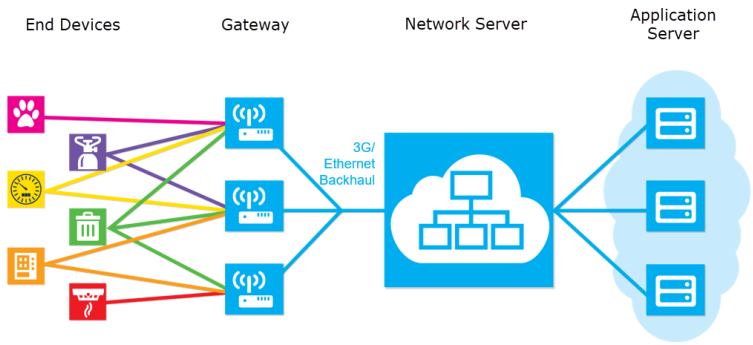
LoRaWAN

- **LoRaWAN** – a *cloud-based* MAC protocol architecture, centralized control via a network server.



Source: https://www.iieta.org/journals/isi/paper/10.18280/isi.270401

- LoRaWAN MAC acts as network protocol.
  - Management and communication between gateways and end-devices
- Devices are async, transmit to multiple gateways, and follow classes A, B, C for uplink/downlink timing.
  - **Class A:** Uplink first, downlink only after uplink (most energy-efficient)
  - **Class B:** Scheduled downlink windows
  - **Class C:** Almost always listening

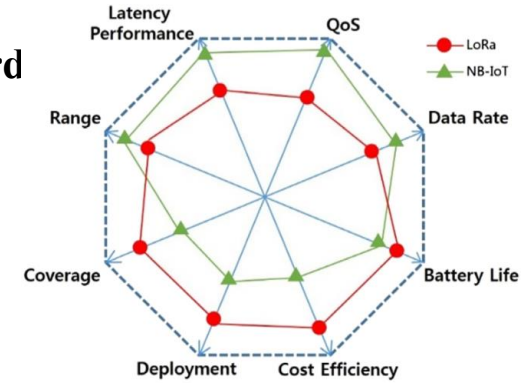


Source: https://tech-journal.semtech.com/understanding-the-lorawan-architecture

- **Network servers:** Message Consolidation; Routing; Network Control; Network and Gateway Supervision
- Data is forwarded to application servers.

NarrowBand IoT (NB-IoT)

- From 3rd Generation Partnership Project (3GPP)
  - 3GPP Release 13 (2016) and 14 (2017)
- Based on a subset of **LTE standard**
  - Licensed LTE bandwidth
- Single narrowband of **180kHz**
- MAC layer
  - **Downlink:** OFDMA: Multi-user OFDM
  - **Uplink:** SC-FDMA: Single Carrier – Frequency Division Multiple Access
- Data rate
  - Downlink: 26 Kbps (Release 13) – 127 Kbps (Release 14)
  - Uplink: 16.9/66 Kbps (Release 13) – 159 Kbps (Release 14)



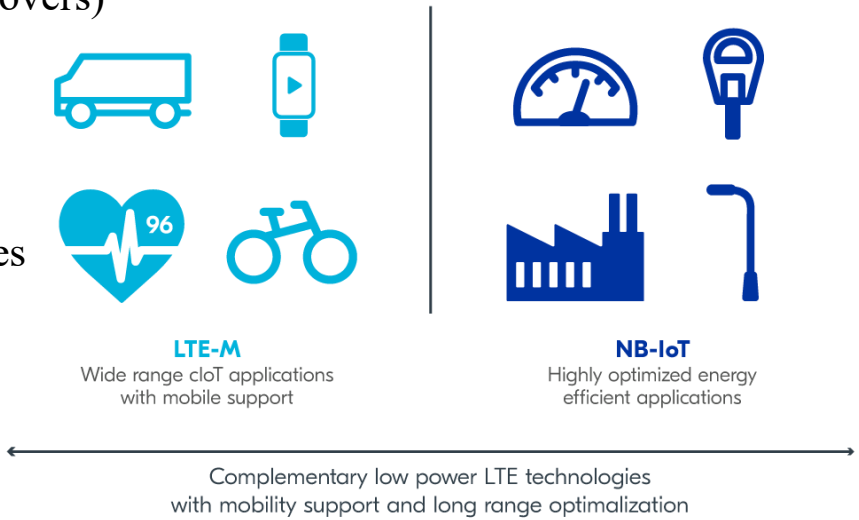
OFDM: split the available bandwidth into many orthogonal (non-interfering) subcarriers.

OFDMA: multiple users share subcarriers at the same time; different subset of subcarriers to different users. OFDMA has high peak-to-average power ratio (PAPR).

SC-FDMA: user data passes through a DFT, spreading data across subcarriers, lowering (PAPR). Better for UE.

LTE-M

- From 3GPP as well
  - 3GPP Release 12 (2015), 13 (2016), and 14 (2017), Cat-M1
- Based of LTE standard
  - Licensed LTE bandwidth (1.4 MHz)
- Difference with NB-IoT
  - Higher data rate (DL: 1 Mbps – UL: 1 Mbps)
  - Higher mobility (full mobility with handovers)
  - Higher bandwidth (> 1MHz)
  - Higher cost
  - Voice support
- Suitable for wearables, trackers, VoLTE devices



Universitetet i Stavanger

Q&A