1. Cellular Network Generations (1G to 4G/SAE)

This evolution moved from analog voice to digital voice, eventually eliminating the circuit-switched domain entirely for an all-IP network structure.

Generation	Year	Key Technology/Service	Data Rate	Core Architecture	Key Features
1G	1980s	Analog Voice (AMPS, NMT, TACS) 1111	Analog (Data < 9.6 Kbps) 222	Analog switching 3	Voice only 4, low security 5, poor voice quality 6
2G	1990s	Digital Voice, SMS/MMS (GSM, CDMA, GPRS) 7777	Digital (Data < 128 Kbps) 8	Digital traffic channels 9, encryption 10101010, error correction 11	Introduction of SIM (Subscriber Identity Module) 12121212
2.5G	~2000	Packet-oriented services (GPRS) 13	Max 150 Kbps 14	Packet transport service, new entities like SGSN and GGSN 15	**PDP Context** for tunnel-based data transmission 16
3G	2000s	Broadband Mobile Data (UMTS/W-CDMA) 17171717	Max 384 Kbps (global), Max 2 Mbps (local) 18	Core split into **Circuit-Switched** (voice) and **Packet-Switched** (data) domains 19	Uses Wideband Code Division Multiple Access (W-CDMA) 20
4G	2010s	Broadband Data Massification (LTE/SAE) 21212121	Data < 1 Gbps 22	Fully **Packet Switching** (EPC/E-UTRAN) 23, no dedicated circuit-switched domain 24	Achieved higher data rates and lower latency 25through an all-IP network26.

2. Wireless Sensor Networks (WSNs) and IoT

Wireless Sensor Networks (WSNs)

- **Definition:** WSNs are wireless networks using sensors to cooperatively monitor physical or environmental conditions27.
- **Composition:** Typically consist of many small, battery-powered, wireless devices28.
- **Core Challenges:** Severe energy constraint 29, need for self-organization and self-healing30.
- **Energy Wastage:** The major sources of energy wastage are collisions, overhearing, control packet overhead, and **idle listening**31.
- **S-MAC:** A medium-access control (MAC) protocol for WSNs that periodically puts nodes to sleep and wakes them up, trading energy efficiency for lower throughput and higher latency323232323232323232.

ZigBee (IEEE 802.15.4)

- **Standard and Layers:** Based on **IEEE 802.15.4** (Low Rate WPAN)33333333. ZigBee defines the Network, Security, and Application layers atop the 802.15.4 MAC and PHY34343434.
- **Key Features:** Low power consumption, low cost 35, supports large networks (up to $65,536$ nodes in a mesh) 36, and a maximum data rate of 250 kbps37.
- **Device Classes (802.15.4):**
    - **Full Function Device (FFD):** Can be a PAN coordinator or router; supports any topology3838383838383838.
    - **Reduced Function Device (RFD):** Optimized for low power and cost; restricted to a star topology and communicates only with a coordinator39393939.
- **MAC Modes:**
    - **Beacon-enabled:** Coordinator sends a beacon periodically; suitable for the lowest energy consumption as devices can sleep40404040. Uses **slotted CSMA/CA**41414141.
    - **Non-Beacon:** Coordinator/routers must stay awake42. Uses **unslotted CSMA/CA**43434343.

    - **GTS (Guaranteed Time Slot):** Allows a device in the active period of a superframe to transmit in a reserved, dedicated time slot44444444.

LPWAN Technologies

- **LPWAN Overview:** Technologies like Sigfox, LoRaWAN, NB-IoT, and LTE-M are primarily used for sensor networks in wide areas or low-power scenarios45454545.

Feature	Sigfox	LoRaWAN	NB-IoT	LTE-M
Max Data Rate	100 bps 46	50 kbps 47	200 kbps 48	1 Mbps 49
Modulation	Ultra Narrow Band (UNB) 50	Chirp Spread Spectrum (CSS) 51	QPSK 52	HD-FDD, BPSK/QPSK 53
Spectrum	Unlicensed ISM 54	Unlicensed ISM 55	Licensed LTE 56	Licensed LTE 57
Mobility	Stationary only 58	Stationary/Limited 59	No 60	Yes 61
Architecture	Proprietary network of Gateways to a Network Server 62	Star-of-stars topology (Gateways $\ rightarrow$ Network Server) 63	Integrated into LTE architecture (EPC/E-UTRAN) 64	Integrated into LTE architecture (EPC/E-UTRAN) 65

- **LoRa (PHY Layer):** The spreading factor (**SF**) dictates the trade-off between range and data rate. A higher SF requires more time-on-air but increases the link budget (sensitivity) for greater distance66666666.
- **LoRaWAN Classes:**
    - **Class A:** Devices schedule their own transmissions (uplink) and open two receive windows afterward. Lowest power consumption67.
    - **Class C:** Module is always listening. Adapted to modules with continuous power, allowing the server to initiate transmission almost anytime68.
- **NB-IoT & LTE-M (Cellular LPWAN):** Both derived from LTE. NB-IoT is optimized for very low data rates and stationery devices, while LTE-M supports moderate data rates and mobility69. NB-IoT operates using a narrow band (200KHz) within a GSM/LTE resource block70.

3. 5G System Architecture and Procedures

5G Use Cases and Core Architecture

- **Usage Scenarios (The 5G Triangle):** eMBB (Enhanced Mobile Broadband - speed) 71, mMTC (Massive Machine Type Communications - density) 72, and URLLC (Ultra-Reliable, Low Latency Communications - trustable and responsive)73737373.
- **Architecture:** Based on **SBA (Service-Based Architecture)**74.
    - **Control Plane (CP):** Composed of **stateless NFs** that communicate using **RESTful APIs** (HTTP/2, JSON)75.
    - **User Plane (UP):** Handled by the **UPF**, which is decoupled from the Control Plane76.

Key Network Functions (NFs)

NF	Role
AMF (Access and Mobility Mgmt Function) 77	Termination of **NAS** signaling, registration, connection/mobility management, and security context (contains **SEAF**)7878787878787878787878787878.
SMF (Session Management Function) 79	Manages **PDU Sessions**, IP address allocation, and **UPF** configuration via **PFCP**80.
UPF (User Plane Function) 81	Packet routing/forwarding, QoS handling, anchor point for mobility, and external PDU session point of interconnect to the **DN**82.
PCF (Policy Control Function) 83	Supports a unified policy framework and provides policy rules to the Control Plane (e.g., SMF) to enforce them84.
UDM (Unified Data Management) 85	Centralized subscriber database for authentication/key agreement credentials and subscription data (contains **ARPF**)86868686.
AUSF (Authentication Server Function) 87	Acts as an authentication server for 3GPP and non-3GPP access88.
NRF (NF Repository Function) 89	Supports service discovery by maintaining the profile of available NF instances and their supported services90.

User Connectivity: PDU Sessions and QoS

- **PDU Session:** The logical connection between the UE and the **DN** (Data Network) via the **UPF** and a specific **Network Slice**91.
    - A single UE can have multiple PDU Sessions to different DNNs/Slices92.
- **QoS Flows:** Exists within a PDU Session to group traffic requiring the same QoS93.
    - **5QI (5G QoS Identifier):** A scalar value that identifies a specific set of QoS characteristics (e.g., priority, Packet Delay Budget, Packet Error Rate)94949494.
    - **PDR (Packet Detection Rule):** Instructs the UPF how to detect and classify traffic to map it to the correct QoS Flow95959595.

Mobility, States, and Security

- **UE States (3 Layers):**
    - **Registration Management (RM): RM-REGISTERED / RM-DEREGISTERED** (between UE and 5GC)96969696.
    - **Connection Management (CM): CM-CONNECTED / CM-IDLE** (active or no NAS connection with 5GC)97979797.
    - **RRC States: RRC_CONNECTED** (active RRC connection, sending data) / **RRC_INACTIVE** (dormant power saving state, keeps context for fast resume) / **RRC_IDLE** (lowest power, no RRC connection)989898989898989898.
- **Paging:** Used to notify a dormant UE (in RRC_Idle or RRC_Inactive states) of incoming data999999999999999999.
- **Authentication:** The network-side process is anchored in the Home Network via the UDM/ARPF and AUSF100100100100.
    - **SUCI (Subscription Concealed Identifier):** An encrypted form of the permanent **SUPI** (IMSI) used over the air to prevent location tracking (IMSI-catcher style attacks)101101101101.

5G Protocols

- **SBA Communication: HTTP/2** (for multiplexing and performance) and **JSON** (lightweight data-interchange format)102102102102102102102102102.
- **N2 Interface (gNB-AMF) Protocols: SCTP** (reliable transport over IP, supporting multi-streaming/multi-homing) and **NG-AP** (application layer for registration, handovers, context setup)103103103103103103103103103.
- **N4 Interface (SMF-UPF) Protocol: PFCP (Packet Forwarding Control Protocol)**. Enables the SMF to dynamically configure the UPF's data plane forwarding rules (**PDRs, FARs, QERs, URRs**)104104104104104104104104104.
- **N3/N9 User Plane Protocol: GTP-U (GPRS Tunneling Protocol - User Plane)**. Encapsulates user IP packets in tunnels identified by **TEIDs** for forwarding data between RAN and UPF nodes105105105105105105105105105.

4. Network Virtualization and Software Defined Networking

Network Function Virtualization (NFV)

- **Definition:** NFV simulates network hardware/appliances in software (**VNFs**) running on generic commercial off-the-shelf (COTS) hardware106106106106.
- **Benefits:** Lower CAPEX (less specialized hardware) and OPEX (less upgrades/licenses)107107107107.
- **Core Concepts (ETSI NFV):**
    - **VNF:** A virtualized Network Function108.
    - **NFVI:** The underlying physical and virtualized compute, storage, and network resources109.
    - **NS (Network Service):** A service composed of interconnected VNFs forming a **VNFFG (VNF Forwarding Graph)**110110110110.
    - **MANO (Management and Orchestration):** The framework to manage the lifecycle of VNFs and NSs, consisting of the **NFVO**, **VNFM**, and **VIM**111.

Software Defined Networking (SDN)

- **Principle:** Separates the **Control Plane** (intelligence, e.g., SDN Controller) from the **Data Plane** (packet forwarding, e.g., switch hardware)112112112112112112112112112.
- **Objective:** To enable a higher degree of **centralized** and **dynamic** control over network devices and traffic flow via programmable mechanisms113113113113113113113113113.
- **Architecture:**
    - **Controller Platform:** The brain, containing the logic and services (e.g., Topology Manager, Device Manager)114114114114.
    - **Northbound Interface:** The API to management applications (e.g., REST, Java, Python)115.
    - **Southbound Interface:** The API to the forwarding devices (e.g., **OpenFlow**, NETCONF, P4Runtime)116.
    - **Data Plane Elements:** The switches and forwarding devices117.

- **OpenFlow:** A protocol allowing the controller to manage a switch's **Flow Tables**, which define **Rules** (matches on headers), **Actions** (forward, drop, modify), and **Statistics**1181181181181181181181181181181181181181181181181181181.
- **P4:** A high-level language designed to explicitly **program the switch forwarding behavior** (parser and tables) 119119119119, making the data plane truly reconfigurable and protocol-independent120.