Teletalk Bangladesh Limited

Assistant Manager (Technical) Complete Preparation Notes

Exam: 16 October 2026 | Organiser: BUET

The whole journey of these notes

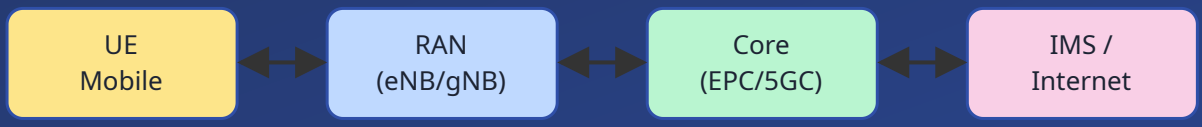


Figure 0.1: Radio → RAN / Backhaul → Core → Voice (IMS) → Database → Power

What is in these notes

- All circular topics in order — 14 technical chapters + Communication Skill + Aptitude
- Each chapter: concept → formula/math → diagram → solved example → MCQs (with explained answers)
- At the end: formula summary, abbreviation table, model tests

Contents and Preparation Strategy

What to read first, and how much time to give each topic

Chapter	Subject	Circular topic
1	Telecom Basics	Telecom Basics
2	Radio Communication Basics	Radio Communication Basics
3	Basic Concept of Cellular Networks	Basic Concept of Cellular Networks
4	Mobile Core and Backhaul Architecture	Mobile Core and Backhaul Architectures
5	Packet-Switched Mobile Networks	Packet-Switched Mobile Networks
6	NFV	Network Function Virtualization
7	C-RAN and O-RAN	Cloud RAN & Open RAN
8	5G Network Slicing	5G Network Slicing
9	Packet switching, call control, circuit to EPC/5GC	Packet Switching, Call Control, Evolution
10	Call flow, session management, mobility	Call Flow, Session, Mobility
11	IMS Architecture	IMS for Voice and Multimedia
12	User data management and authentication (HLR/HSS/UDM)	Mobile User Data, Authentication
13	Telecom Power System	Power System for Telecom
14	Scripting for simulation and configuration	Scripting for Simulation and Configuration
15	Telecom Industry of Bangladesh	Telecom Industry of Bangladesh
16	Communication Skill	Communication skill
17	Aptitude (maths, logic, data interpretation)	Aptitude
Appendix	Formula summary, abbreviation table, model tests	

First, a caution about the exam pattern

> **What is not confirmed**
>
> The circular (Post No. 02 — Assistant Manager, Technical; pay Grade 9; BSc Engineering EEE/ECE/ETE/CSE; maximum age 32) does **not state the marks or the question pattern** of the written exam. What Gemini wrote — "BUET pattern = block diagram + math + point-form answers" — is a guess, not a verified fact. So confirm the question pattern from the admit card, the Teletalk notice and the job portal (jobs.teletalk.com.bd).
>
> **As per serials 07 and 10 of the circular, the exam has three stages: written, practical and viva.** For each stage you must carry the original copy of your National ID (NID). The circular does not say what the "practical" exam will be — it is probably computer/scripting/configuration or simulation-based work, so do not neglect Chapter 14 (this is my guess).

These notes are built for two types of questions: **(a) MCQ** — so every chapter ends with MCQs; **(b) short written / numerical questions** — so there are formulas, step-by-step solutions and hand-drawable diagrams. What you must write is somewhat technology-centred engineering thinking. BUET questions usually test *understanding, not memorisation*, so learn the answers to "why" questions with understanding.

Priority: how important is each topic

Time is short (today is 14 October, the exam is on 16 October), so the topics are arranged in three tiers. The circular lists every topic as equally important, but for an EEE/ETE graduate the order below is practical:

Tier	Chapters	Why
A — First of all	3, 4, 5, 9, 10, 11, 12	Core network, call flow, IMS, authentication — more than half of the circular topics come from here
B — Next	1, 2, 6, 7, 8, 13	Radio basics, maths (dB, Erlang, link budget), NFV / O-RAN / slicing, power
C — Scoring bonus	14, 15, 16, 17	Scripting, Bangladesh telecom, communication, aptitude — marks can be collected in a short time

Two-day routine (14 and 15 October)

Time	What to do
14 Oct — morning	Chapters 3 → 4 → 5 (cellular concepts, core/backhaul, packet core) — do the MCQs of each
14 Oct — afternoon	Chapters 9 → 10 → 11 → 12 (call flow, IMS, HSS/AKA) — draw the diagrams yourself by hand
14 Oct — night	Chapters 1 and 2 (dB, Shannon, link budget, Erlang formulas) — practise the maths
15 Oct — morning	Chapters 6, 7, 8 (NFV, O-RAN, slicing) + Chapter 13 (power, battery calculations)

15 Oct — afternoon	Chapters 14–17 (scripting, Bangladesh telecom, communication, aptitude)
15 Oct — night	Appendix model tests (against the clock); look through the formula and abbreviation tables once; sleep early
16 Oct — morning	Only run your eyes over the formula summary and the diagrams. Do not read anything new

How to study (in each chapter)

1. Read the **concept part** once — understand the definition and "why this is needed".
2. **Draw the diagram** yourself on paper (boxes + interface names).
3. Cover the **solved example**, solve it yourself, then compare.
4. Do the **MCQs** and write your mistakes in a separate notebook; on the last night read only those.

> **General MCQ trick**
>
> Keep interface/node names (e.g. S1-MME, N4, Cx, S6a) and abbreviations on the tip of your tongue — they are favourite places for MCQs. In maths, check units carefully (dB vs dBm, Mbps vs MBps).

Chapter 1 — Telecom Basics

Telecom Basics

This chapter is the foundation of the whole course. The concepts here (dB, Erlang, switching, multiplexing) are used in almost every later chapter.

1.1 Basic Structure of a Telecommunication System

Every communication system has five parts: **Source → Transmitter → Channel (medium) → Receiver → Destination**. **Noise** is added in the channel and damages the signal. The medium can be a wire (copper), optical fibre or air (radio).

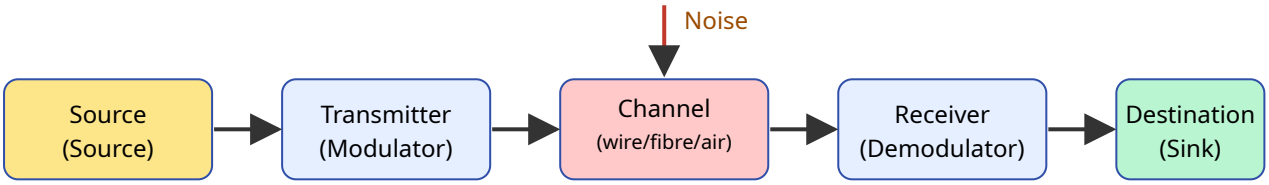


Figure 1.1: Block diagram of a communication system

1.2 Analog vs Digital and PCM

Voice is basically analog. To send it over a digital network there are three steps: **Sampling → Quantization → Encoding** (this is called PCM).

> **Nyquist Sampling Theorem**
>
> If the maximum frequency of a signal is $\mathbf{f_{max}}$, the sampling rate must be $\mathbf{f_s \geq 2\, f_{max}}$, otherwise aliasing occurs.

Example: Bit rate of a voice channel

Voice band ≈ 0.3–3.4 kHz; assume 4 kHz. Sampling = 2 × 4 = **8 kHz** (8000 samples/second). If each sample is 8 bits:

$$\textbf{Bit rate} = 8000 \times 8 = \textbf{64 kbps (this is DS0)}$$

One E1 line has 32 timeslots: 32 × 64 kbps = **2.048 Mbps** (30 voice + 1 frame sync + 1 signalling). T1 = 24 × 64 + 8 kbps = **1.544 Mbps**.

1.3 Decibel (dB) — the Most Needed Maths in Telecom

Signal levels vary over a very wide range (milliwatts to kilowatts), so a logarithmic scale is used.

$$\mathbf{dB = 10\log_{10}(P_2 / P_1)} \quad | \quad \mathbf{dBm = 10\log_{10}(P / 1\ mW)} \quad | \quad \mathbf{dBW = 10\log_{10}(P / 1\ W)}$$

Power ratio	dB	Memory trick
2 times	+3 dB	×2 = +3 dB, ÷2 = −3 dB
10 times	+10 dB	×10 = +10 dB
100 times	+20 dB	×100 = +20 dB
1000 times	+30 dB	1 W = 30 dBm (because 1 W = 1000 mW)
4 times	+6 dB	3+3
5 times	≈ +7 dB	10 − 3

Rules: dBm + dB = dBm (gain/loss can be added and subtracted); dBm − dBm = dB; dBm + dBm cannot be added directly (first convert to mW, then add). For voltage/current use 20 log.

Example: How many dBm is 40 W?

40 W = 40,000 mW → 10 log(40000) = 10 × 4.602 = **46.02 dBm**. Shortcut: 40 = 4×10 → 6 + 10 = 16 dBW → 16 + 30 = 46 dBm ✔

Example: Adding powers

Adding −30 dBm and −30 dBm? Each is 1 μW; total 2 μW → −30 + 3 = **−27 dBm** (not −60).

1.4 Noise and Shannon Capacity

Thermal noise floor: **N = kTB**. At room temperature (290 K):

$$N\ (\text{dBm}) = -174 + 10\log_{10}(B_{Hz}) + NF$$

$$\text{SNR (dB)} = P_{rx}\ (\text{dBm}) - N\ (\text{dBm})$$

Here −174 dBm/Hz is the noise density and NF is the Noise Figure of the receiver.

Shannon-Hartley Theorem

The maximum error-free data rate of a channel:

$$C = B \cdot \log_2(1 + \text{SNR}) \quad [\text{bps}]$$

Here SNR is the linear ratio, not dB. C increases if B or SNR is increased — that is why 5G needs wider bandwidth and MIMO.

Example: Shannon capacity of a 20 MHz channel

SNR = 15 dB → linear = $10^{1.5}$ = 31.62.

C = $20\times10^6 \times \log_2(1 + 31.62) = 20\times10^6 \times \log_2(32.62) = 20\times10^6 \times 5.03 \approx$ **100.6 Mbps**.

Noise floor: −174 + 10 log(20×10^6) = −174 + 73.01 = **−100.99 dBm**; with NF = 7 dB it is **−93.99 ≈ −94 dBm**.

1.5 Switching: Circuit vs Packet

Topic	Circuit switching (PSTN, 2G CS)	Packet switching (IP, 4G/5G)
Path	A dedicated path/resources are allocated at the start of the call	Each packet is routed independently
Resource use	Resources stay held even when silent (wastage)	Statistical multiplexing — efficient
Delay	Fixed and low, no jitter	Variable delay and jitter (QoS needed)
Failure	Call drops if the path breaks	Finds an alternative path
Suitable for	Traditional voice	Data, VoIP/VoLTE, video
Example protocols	SS7/ISUP	IP, SIP, GTP

1.6 Multiplexing and Transport

- **FDM** — divides by frequency (radio/TV channels).
- **TDM** — divides by time slots (E1, SDH, GSM).
- **WDM** — lights of different wavelengths on the same fibre (CWDM/DWDM).

SDH level	Bit rate	Remember
STM-1	155.52 Mbps	= 63 × E1 (2.048)
STM-4	622.08 Mbps	4 × STM-1
STM-16	2.488 Gbps	16 × STM-1
STM-64	9.953 Gbps	64 × STM-1

Optical fibre: Single-mode (SMF, core ≈ 9 µm, long distance; 1310/1550 nm) and Multi-mode (MMF, core 50/62.5 µm, short distance). Attenuation is lowest at 1550 nm (~0.2 dB/km). Optical link budget: $P_{rx} = P_{tx} - (\alpha \cdot L + \text{connector loss} + \text{splice loss})$.

1.7 OSI and TCP/IP Models

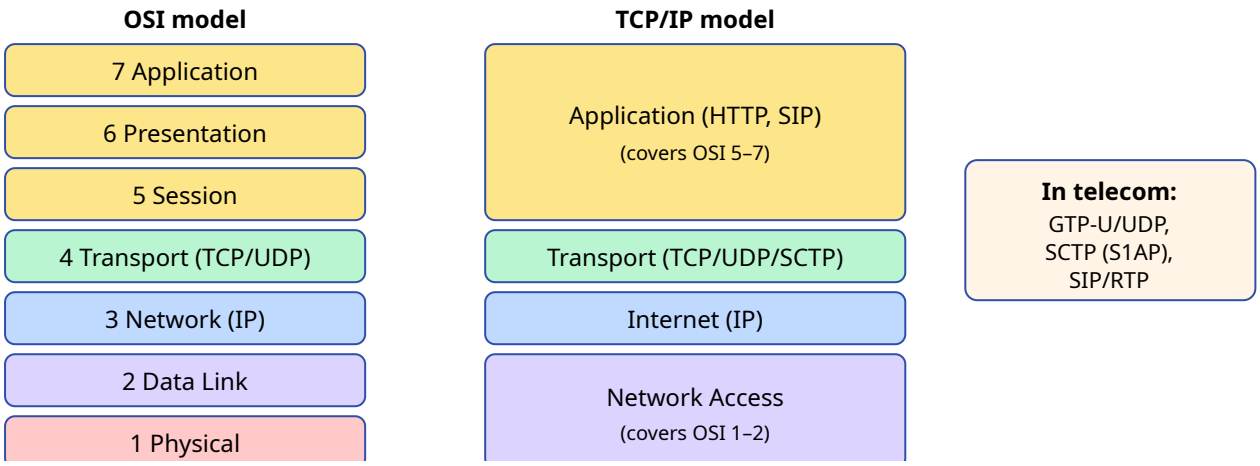


Figure 1.2: OSI vs TCP/IP layers

- **TCP** — reliable, connection-oriented (data/HTTP); **UDP** — fast, no reliability (voice RTP, GTP-U); **SCTP** — for signalling (S1AP, NGAP, Diameter).

Example: IPv4 subnetting

192.168.10.0/26 → subnet mask 255.255.255.192; host bits = 32 − 26 = 6; total addresses = 2^6 = 64; usable hosts = 64 − 2 = **62**. Network = .0, broadcast = .63, range .1–.62. IPv6 = 128 bits; IPv6 is important in the mobile core because IPv4 is running out.

1.8 Signalling Protocols — Who Is Where

Protocol	Function	Where used
SS7 (MTP, SCCP, ISUP, TCAP/MAP)	Traditional signalling	2G/3G CS core, with the HLR (MAP)
Diameter	AAA, subscriber data, charging	4G: S6a, Gx, Rx; IMS: Cx
SIP	Session control	IMS/VoLTE
GTP (GTP-C / GTP-U)	Tunnelling (control / user plane)	S11, S5/S8, S1-U, N3
S1AP / NGAP	RAN–core signalling	S1-MME / N2
NAS (EMM/ESM, 5GMM/5GSM)	UE–core signalling	UE ↔ MME/AMF
PFCP	Control-user plane separation	N4 (SMF–UPF), Sxa/Sxb
HTTP/2 + JSON	Service-based interface	5GC SBA

1.9 Network Performance (QoS and KPI)

- **Throughput**, **Latency** (delay), **Jitter** (variation in delay), **Packet loss**.
- **CSSR** (Call Setup Success Rate), **CDR/DCR** (Call/Drop Rate), **HOSR** (Handover Success Rate), **RRC/E-RAB Setup Success Rate**, **PRB utilization**, site **Availability**.
- For voice: delay < 150 ms (one way), loss < 1%; MOS scale 1–5 (4+ is good).

Example: Erlang — the unit of traffic

1 Erlang = one channel busy 100% of the time.

$$A = \lambda \times h$$

λ = number of calls per hour, h = average call duration (in hours). 1200 calls per hour, average 3 minutes → A = 1200 × (3/60) = **60 Erlang**. (Detailed in Chapter 3.)

Practice (MCQ)

1. What is the bit rate if a 4 kHz voice signal is PCM coded (8 bits/sample)?

(a) 32 kbps (b) 64 kbps
(c) 128 kbps (d) 2.048 Mbps

Answer: (b) — fs = 8 kHz, 8 bits → 64 kbps (DS0).

2. How many dBm is 1 W of power?

(a) 0 dBm (b) 10 dBm
(c) 30 dBm (d) 3 dBm

Answer: (c) — 1 W = 1000 mW → 10 log 1000 = 30 dBm.

3. −30 dBm + −30 dBm = ?

(a) −60 dBm (b) −27 dBm
(c) −33 dBm (d) −15 dBm

Answer: (b) — Double power = +3 dB.

4. In the Shannon capacity formula, in what form is SNR used?

(a) In dB (b) As a linear ratio
(c) In dBm (d) In nepers

Answer: (b) — $C = B \log_2(1+SNR)$, SNR is linear.

5. What is the bit rate of an E1 line?

(a) 1.544 Mbps (b) 2.048 Mbps
(c) 34 Mbps (d) 155 Mbps

Answer: (b) — 32 × 64 kbps = 2.048 Mbps. 1.544 is T1.

6. What is the bit rate of STM-1?

(a) 51.84 Mbps (b) 155.52 Mbps
(c) 622.08 Mbps (d) 2.048 Mbps

Answer: (b) — STM-1 = 155.52 Mbps ≈ 63 E1.

7. Which is a feature of circuit switching?

(a) Dedicated resources during the call
(b) Each packet routed separately
(c) Statistical multiplexing
(d) High jitter

Answer: (a) — In circuit switching, resources are allocated for the call in advance.

8. What is the approximate thermal noise floor at 20 MHz bandwidth (NF = 0)?

(a) −174 dBm
(b) −101 dBm
(c) −94 dBm
(d) −80 dBm

Answer: (b) — −174 + 73 = −101 dBm.

9. Which protocol is commonly used on the S1-MME interface?

(a) GTP-U
(b) S1AP over SCTP
(c) SIP
(d) PFCP

Answer: (b) — S1-MME = S1AP/SCTP.

10. How many usable hosts are in a /26 subnet?

(a) 64
(b) 62
(c) 30
(d) 126

Answer: (b) — $2^6 - 2 = 62$.

11. In which multiplexing are lights of different colours sent on the same fibre?

(a) TDM
(b) FDM
(c) WDM
(d) CDM

Answer: (c) — WDM = Wavelength Division Multiplexing.

12. According to Nyquist, what is the minimum rate to sample 20 kHz audio?

(a) 20 kHz
(b) 40 kHz
(c) 10 kHz
(d) 80 kHz

Answer: (b) — $f_s \geq 2 f_{max} = 40$ kHz.

Chapter 2 — Radio Communication Basics

2.1 Electromagnetic Spectrum and Waves

Radio waves travel at the speed of light ($c = 3\times10^8$ m/s). Relation between frequency (f) and wavelength (λ):

$$\lambda = c / f$$

Example: λ and quarter-wave antenna at 1800 MHz

$\lambda = 3\times10^8 / 1.8\times10^9$ = **0.1667 m = 16.7 cm**; quarter-wave = λ/4 ≈ **4.17 cm**. The higher the frequency, the smaller the antenna, but coverage and wall-penetration ability decrease.

Band	Frequency	Name / Use
VHF / UHF	30–300 MHz / 0.3–3 GHz	FM, TV, mobile (in UHF)
Low band (sub-1 GHz)	700/800/900 MHz	More coverage, good indoors — rural
Mid band	1.8, 2.1, 2.3, 2.6 GHz	Balance of coverage and capacity (3G/4G)
C-band / 3.5 GHz	3.3–3.8 GHz (n78)	Main mid-band of 5G
mmWave (FR2)	24–52 GHz	Very high speed, short range

Common GSM bands: **GSM-900** (UL 890–915, DL 935–960 MHz; duplex gap 45 MHz); **GSM-1800/DCS** (UL 1710–1785, DL 1805–1880 MHz; gap 95 MHz); **UMTS-2100** (UL 1920–1980, DL 2110–2170 MHz); **LTE B40** 2300–2400 TDD; **LTE B7** 2600 FDD.

2.2 Baseband and Modulation

Putting data (baseband) onto a carrier wave is called **modulation**: by changing the amplitude (ASK), frequency (FSK), phase (PSK) or amplitude + phase (QAM).

Scheme	Bits/symbol	Used for	Features
BPSK	1	Very weak signal	Most robust, low speed
QPSK	2	LTE/NR control, cell edge	Robust
16-QAM	4	Medium SINR	—
64-QAM	6	Good signal	—
256-QAM	8	Very good SINR (near the site)	Needs high SNR
GMSK	1 (special)	GSM	Constant envelope, low out-of-band emission

Adaptive Modulation and Coding (AMC): when the signal is good, a higher-order QAM is used; when it is poor, QPSK — so users near the site get higher speed. **Formula:** Bit rate ≈ symbol rate × $\log_2 M$ × code rate.

2.3 Multiple Access

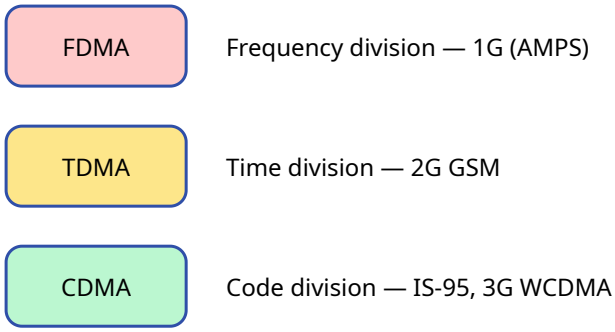


Figure 2.1: Multiple access methods

Method	What is divided	Where used	Main advantage / problem
FDMA	Frequency	1G	Simple; waste in guard bands
TDMA	Time slots	GSM (8 slots, 200 kHz)	Digital, needs synchronisation
CDMA	Spreading code	IS-95, WCDMA	Soft handover, frequency reuse 1; near-far problem → power control
OFDMA	Subcarrier × time	LTE DL, 5G NR	Multipath resistant, flexible
SC-FDMA	Single carrier	LTE UL	Low PAPR → saves mobile battery

Example: GSM TDMA calculation

GSM frame = 8 slots = 4.615 ms; one slot = 577 µs = 156.25 bits.
Gross rate = 156.25 × 8 / 4.615 ms = **270.8 kbps** per 200 kHz carrier. In a 25 MHz band: 25 MHz / 200 kHz = 125 carriers (124 usable) ⇒ 124 × 8 = **992 full-rate channels**.

Example: WCDMA processing gain

Chip rate = 3.84 Mcps; voice = 12.2 kbps. $G_p = 3.84\times10^6 / 12.2\times10^3 = 314.8 \rightarrow 10\log(314.8) = \approx$ **25 dB**.
Higher processing gain means decoding is possible even in the presence of interference.

2.4 OFDM — the Heart of 4G/5G

One wide channel is divided into many narrow, mutually **orthogonal** subcarriers. Each subcarrier carries symbols at a slow rate, so the effect of multipath delay spread is small. The **Cyclic Prefix (CP)** prevents ISI.

LTE Parameters

Subcarrier spacing = **15 kHz**; symbol time = 1/15 kHz = 66.7 µs; 1 Resource Block (RB) = 12 subcarriers = 180 kHz; 1 subframe = 1 ms = 14 OFDM symbols (normal CP); 20 MHz = **100 RB = 1200 subcarriers**; frame = 10 ms.

Example: Theoretical peak data rate of LTE 20 MHz

Resource elements (RE) per second = 1200 × 14 × 1000 = 16.8 million. With 64-QAM (6 bits): $16.8 \times 10^6 \times 6$ = **100.8 Mbps** (1 layer, without overhead). 4×4 MIMO (4 layers) ⇒ ≈ **403 Mbps**. In practice, due to control/reference signal overhead, ≈ 300 Mbps (close to the LTE Cat-6/9 limit).

5G NR Numerology

SCS = $15 \times 2^{\mu}$ kHz; slot time = 1 ms / 2^{μ}; 14 symbols per slot. µ=0 (15 kHz), 1 (30 kHz — common at 3.5 GHz), 2 (60), 3 (120 kHz — mmWave), 4 (240). Max channel BW: FR1 100 MHz, FR2 400 MHz. FR1 ≈ 410 MHz–7.125 GHz; FR2 ≈ 24.25–52.6 GHz.

2.5 Antenna and EIRP

- **dBi** = gain relative to an isotropic antenna; **dBd** = relative to a dipole; `dBi = dBd + 2.15`.
- **EIRP = $P_{tx} - L_{cable} + G_{tx}$** (dBm).
- **Sectorisation:** dividing a site into 3 sectors with 120° antennas — interference decreases, capacity increases.
- **Downtilt:** tilting the beam slightly downward limits coverage and reduces interference to neighbouring cells (electrical + mechanical).
- **Diversity/MIMO:** multiple antennas reduce the effect of fading; SU-MIMO increases speed, MU-MIMO serves multiple users at the same time; **Massive MIMO** (64T64R etc.) + **beamforming** is the key strength of 5G.

$$\text{MIMO capacity} \approx \min(N_t, N_r) \times B \log_2(1 + \text{SNR})$$

2.6 Radio Propagation and Path Loss

A signal suffers three kinds of loss with distance: (1) **path loss** (distance), (2) **shadowing** (buildings/trees, log-normal, slow), (3) **multipath fading** (fast, Rayleigh/Rician).

Free-Space Path Loss (FSPL)

$$\text{FSPL (dB)} = 32.44 + 20 \log_{10}(d_{km}) + 20 \log_{10}(f_{MHz})$$

Doubling the distance gives +6 dB; doubling the frequency gives +6 dB.

Example: FSPL of 1800 MHz at 2 km

= 32.44 + 20 log(2) + 20 log(1800) = 32.44 + 6.02 + 65.11 = **103.57 dB**.

Okumura–Hata Model (urban, 150–1500 MHz)

$$L\ (\text{dB}) = 69.55 + 26.16 \log f - 13.82 \log h_b - a(h_m) + (44.9 - 6.55 \log h_b) \log d$$

f = MHz, h_b = base antenna height (m), d = km, $a(h_m)$ = mobile-height correction (for small/medium cities $a = (1.1 \log f - 0.7)h_m - (1.56 \log f - 0.8)$). Additional reduction applies for suburban/rural areas.

Example: Hata

f = 900 MHz, h_b = 50 m, h_m = 1.5 m, d = 5 km → $a(h_m) \approx 0.016$ dB. $L = 69.55 + 26.16 \times 2.954 - 13.82 \times 1.699 - 0.016 + (44.9 - 6.55 \times 1.699) \times 0.699 = \approx$ **146.9 dB**.

Doppler Shift and Coherence

$$f_d = v \cdot f / c$$

Example: Doppler

Train at 100 km/h (= 27.78 m/s), f = 2 GHz → $f_d = 27.78 \times 2 \times 10^9 / 3 \times 10^8 \approx$ **185 Hz**. The OFDM subcarrier spacing (15 kHz) must be much larger than the Doppler shift.

Coherence bandwidth $B_c \approx 1/(5\sigma_\tau)$ (σ_τ = RMS delay spread). If signal BW > B_c → frequency-selective fading (OFDM handles this).

2.7 Link Budget

In a radio link, gains and losses are added and subtracted to find the received power and the margin.

$$P_{rx} = P_{tx} + G_{tx} - L_{cable} - PL - L_{other} + G_{rx} \quad (\text{dBm})$$
$$\text{Link Margin} = P_{rx} - \text{Receiver Sensitivity}$$

Example: Downlink budget

Tx = 43 dBm (20 W), antenna gain = 15 dBi, cable loss = 2 dB, path loss = 120 dB, body loss = 3 dB, UE gain = 0 dBi.

$P_{rx} = 43 + 15 - 2 - 120 - 3 + 0 =$ **−67 dBm**. Noise (20 MHz, NF 7 dB) = −94 dBm ⇒ SNR = −67 − (−94) = **27 dB**. If UE sensitivity is −100 dBm, then fade margin = −67 − (−100) = **33 dB**.

2.8 Duplex: FDD vs TDD

	FDD	TDD
UL/DL	Separate frequency pair	Same frequency, different time
Advantage	Low delay, equal UL/DL, large cell	UL:DL ratio can be changed, channel reciprocity (good for massive MIMO)
Problem	Needs paired spectrum	Guard period, synchronisation needed, limited cell radius

Example	GSM, LTE B1/B3/B7	LTE B40/B41, 5G n78

Practice (MCQ)

1. What is the wavelength of a 1800 MHz wave?

(a) 16.7 cm (b) 33 cm
(c) 1.67 m (d) 6 cm

Answer: (a) — $\lambda = c/f = 3\times10^8/1.8\times10^9 = 0.167$ m.

2. Which modulation carries 6 bits per symbol?

(a) QPSK (b) 16-QAM
(c) 64-QAM (d) 256-QAM

Answer: (c) — $64 = 2^6$.

3. How many time slots are there in one GSM carrier (200 kHz)?

(a) 4 (b) 8
(c) 16 (d) 32

Answer: (b) — 8 slots, frame 4.615 ms.

4. What is the subcarrier spacing in LTE?

(a) 7.5 kHz (b) 15 kHz
(c) 30 kHz (d) 60 kHz

Answer: (b) — LTE = 15 kHz; in 5G it is 15×2^μ.

5. How many RBs are there in a 20 MHz LTE channel?

(a) 50 (b) 75
(c) 100 (d) 110

Answer: (c) — 100 RB = 1200 subcarriers.

6. By how much does free-space path loss increase when the distance is doubled?

(a) 3 dB (b) 6 dB
(c) 10 dB (d) 20 dB

Answer: (b) — 20 log 2 = 6 dB.

7. Which access method is used in the LTE uplink?

(a) OFDMA (b) SC-FDMA
(c) CDMA (d) TDMA

Answer: (b) — For low PAPR.

8. What is the slot time in 5G NR at 30 kHz SCS?

(a) 1 ms (b) 0.5 ms
(c) 0.25 ms (d) 2 ms

Answer: (b) — μ=1 → 1 ms/2 = 0.5 ms.

9. What is the chip rate of WCDMA?

(a) 1.2288 Mcps
(b) 3.84 Mcps
(c) 270.8 kcps
(d) 5 Mcps

Answer: (b) — UMTS = 3.84 Mcps (IS-95 = 1.2288).

10. What is the approximate Doppler shift at 100 km/h and 2 GHz?

(a) 18.5 Hz
(b) 185 Hz
(c) 1.85 kHz
(d) 18.5 kHz

Answer: (b) — $f_d = vf/c \approx 185$ Hz.

11. Which duplex method is advantageous for Massive MIMO (channel reciprocity)?

(a) FDD
(b) TDD
(c) Both the same
(d) Neither

Answer: (b) — In TDD, UL/DL use the same frequency, so the channel is easy to estimate.

12. Tx 43 dBm, gain 15 dBi, total loss 125 dB (cable + path + other), UE gain 0 → P_rx?

(a) −67 dBm
(b) −82 dBm
(c) −55 dBm
(d) −110 dBm

Answer: (a) — 43 + 15 − 125 = −67 dBm.

Chapter 3 — Basic Concept of Cellular Networks

3.1 The Cellular Concept — Why Is It Needed?

If one huge tower covers a whole city, each frequency can be used only once — the number of users is limited. The cellular idea (Bell Labs, 1970s): divide the area into **small cells**, place low-power base stations in each, and **reuse the same frequency in distant cells** (frequency reuse). This lets a limited spectrum serve a very large number of users.

> **Key Terms**
>
> **Cell** = coverage area of one base station (theoretically a hexagon). **Cluster** = a group of N cells that together use the whole available frequency set once. **Co-channel cell** = another cell using the same frequency. **Handover** = transfer of service from one cell to another during a call.

3.2 Frequency Reuse and Cluster

In hexagonal geometry, the cluster size can take only specific values:

$$N = i^2 + i \cdot j + j^2 \quad (i, j = \text{non-negative integers})$$

(i, j)	N	Reuse factor
(1,0)	1	1 (in CDMA/OFDMA)
(1,1)	3	1/3
(2,0)	4	1/4
(2,1)	7	1/7 (common in GSM)
(3,0)	9	1/9
(2,2)	12	1/12

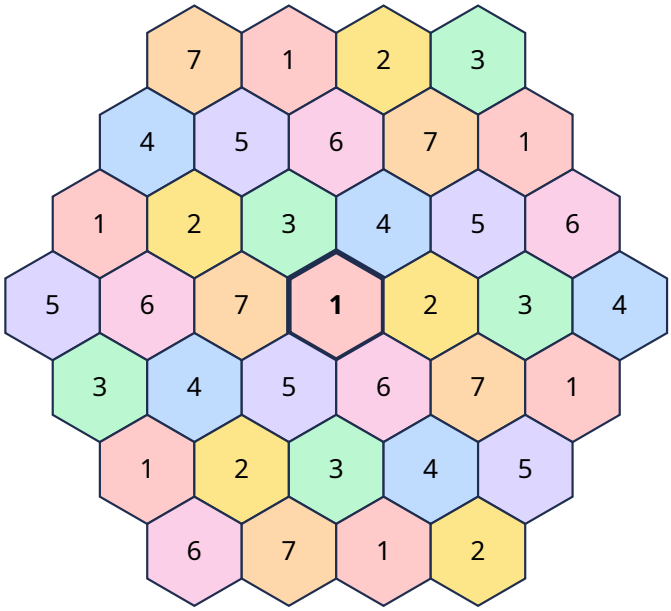


Figure 3.1: N = 7 cluster — cells with the same number use the same frequency set (the centre cell has a thick border)

Reuse Distance

$$D / R = \sqrt{(3N)} = Q \quad \text{(co-channel reuse ratio)}$$

D = distance between the centres of two co-channel cells, R = cell radius. The larger N, the larger Q, and the less interference — but the number of channels per cell decreases (capacity ↓). You must understand this **trade-off**.

Example: Q for N = 7

Q = √(3×7) = √21 = **4.583**. If R = 2 km, D = 4.583×2 = **9.17 km**.

3.3 SIR (Signal-to-Interference Ratio)

Assuming 6 co-channel interferers in the first tier (hexagonal layout) and path-loss exponent n:

$$S / I \approx (D/R)^n / 6 = (\sqrt{(3N)})^n / 6$$

Example: SIR calculation (n = 4)

N = 7: $(4.583)^4 = 441 \rightarrow 441/6 = 73.5 \rightarrow 10 \log(73.5) =$ **18.7 dB**.

N = 3: $(3)^4 = 81 \rightarrow 81/6 = 13.5 \rightarrow$ **11.3 dB**.

N = 4: $12^2/6 = 144/6 = 24 \rightarrow$ **13.8 dB**.

GSM voice quality needs ≈ 9–12 dB SIR, so N = 7 is safe (with sectorisation, N = 4/3 also works). In LTE, N = 1 (all cells use the same frequency) + interference is handled with ICIC/eICIC.

3.4 Ways to Increase Capacity

Technique	How it works	Result

Cell splitting	Divide a cell into smaller cells; reduce power	More channels per area — dense cities
Sectoring	Omni → 3 × 120° sectors	Interferers 6 → 2 (approx.), SIR ↑
Micro/Pico/Femto cells	Small stations (hot spot, indoor)	Capacity and indoor coverage
Frequency reuse ↓ (N ↓)	Smaller cluster	More channels per cell but more interference
Carrier aggregation, MIMO, high QAM	Spectral efficiency ↑	LTE-A/5G speeds

Example: Cell splitting — capacity

If the cell radius is halved (R → R/2), the number of cells in the same area becomes 4 times (area ∝ R^2) ⇒ capacity is about 4 times. The Tx power of the new cell is about $P/2^n$; for n = 4, using P/16 (= −12 dB) keeps the path loss the same.

3.5 Traffic Engineering — Erlang

Erlang B (blocked calls cleared): if no channel is free, the call is dropped. **Erlang C** (blocked calls delayed): the call waits in a queue (call centre). Formula (m channels, E = offered traffic):

$$P_B = B(E, m) = (E^m / m!) / \Sigma_{k=0..m} (E^k / k!)$$

$$\text{Recursion: } B(E,0) = 1; \quad B(E,m) = E \cdot B(E,m-1) / (m + E \cdot B(E,m-1))$$

GoS (Grade of Service) = blocking probability; 1–2% is common in telecom. The network is designed for Busy Hour traffic.

Channels (m)	Max traffic at GoS 1% (Erlang)	At GoS 2%
5	1.36	1.66
10	4.46	5.08
20	12.03	13.18
30	20.34	21.93
40	29.01	31.0

Note: when channels are doubled, traffic grows by more than double (**trunking efficiency**) — a larger channel pool is more efficient.

Example: How many users?

30 channels per cell, GoS = 2%. From the table, capacity ≈ 21.93 Erlang. If each user generates 25 mErlang (0.025 E) in the busy hour, users = 21.93 / 0.025 ≈ **877 users**.

Example: Finding blocking probability

E = 10 Erlang, m = 15 channels → by recursion B ≈ **0.0365 (3.65%)**. For E = 5 with m = 10 channels, B ≈ 1.84%.

Error in your Gemini note

There, "channels 1200, N = 7 ⇒ 171 channels per cell" is correct (1200/7 = 171.4). But "find GoS for 20 Erlang per cell" actually gives GoS ≈ zero (≈ 0%), because 20 Erlang is a very light load for 171 channels. To make the question realistic, the channels must be calculated per sector (1200/7/3 ≈ 57 channels); even then 20 E gives almost zero blocking. So in GoS questions, always check m (channels per sector/cell) together with E.

3.6 Handover (Handoff)

When a user moves and the signal of the serving cell becomes weak, the connection is moved to a new cell. Causes: weak signal, load balancing, interference.

Type	Description	Where
Hard handover	Break the old link, then make the new link (break-before-make)	GSM, LTE
Soft handover	Connected to 2+ cells at the same time (make-before-break)	CDMA, WCDMA
Softer	Between 2 sectors of the same site	WCDMA
Intra-/Inter-frequency, Inter-RAT	Same/different frequency or different technology (LTE→3G)	LTE
Inter-MSC/Inter-MME	Change of mobile switching centre/MME	—

Decision: In LTE, **Event A3** (neighbour cell RSRP better than serving cell by more than an offset) most often triggers a handover. **Hysteresis** and **Time-to-Trigger** are used to prevent *ping-pong*. Detailed flow in Chapter 10.

3.7 Comparison of Mobile Generations

Generation	Year (approx.)	Technology	Access	Data	Core
1G	1980	AMPS (analog)	FDMA	—	—
2G	1991	GSM (GMSK)	TDMA/FDMA	9.6–14.4 kbps (CSD)	CS (MSC/HLR)
2.5G/2.75G	2000	GPRS / EDGE	TDMA	~115 / ~384 kbps	+SGSN/GGSN
3G	2001	UMTS/WCDMA, HSPA	WCDMA	384 kbps → HSPA+ 42 Mbps	CS + PS

4G	2009	LTE / LTE-A	OFDMA / SC-FDMA	100 Mbps–1 Gbps	EPC (all-IP)
5G	2019	NR	OFDMA (CP-OFDM)	peak 20 Gbps	5GC (SBA)

Three Main Uses of 5G (IMT-2020)

eMBB (massive speed), **URLLC** (1 ms latency, ultra-reliable), **mMTC** (1 million devices per km^2). Detailed in Chapter 8.

3.8 GSM Architecture (in Brief)

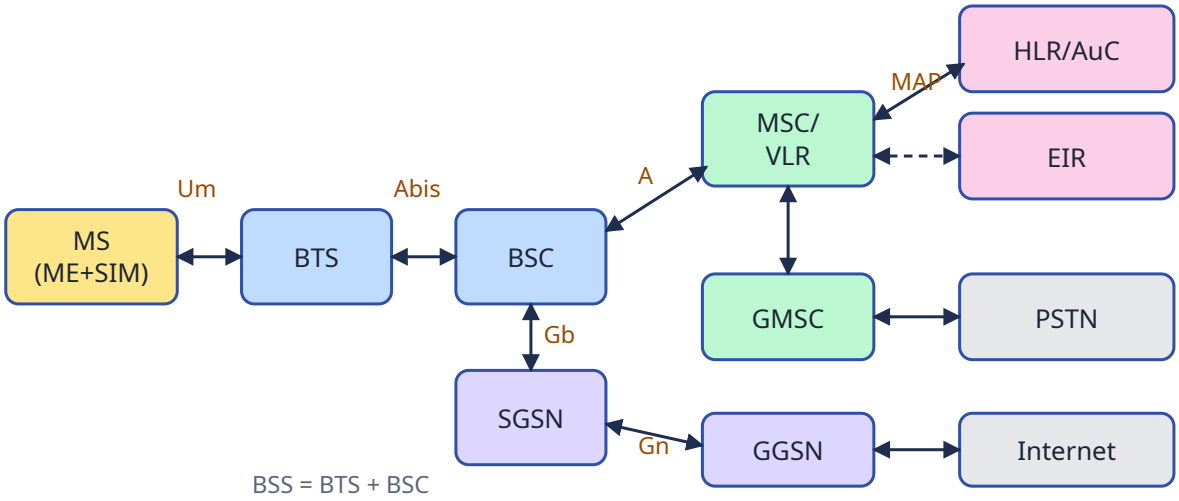


Figure 3.2: GSM/GPRS network architecture

- **MS** = ME (mobile device, IMEI) + SIM (IMSI, Ki).
- **BTS** radio transceiver; **BSC** controls 100+ BTS, handover/power control, radio resources; **TRAU/Transcoder** voice coding.
- **MSC** call switching; **VLR** (temporary visitor data); **GMSC** gateway to external networks.
- **HLR** permanent subscriber data; **AuC** authentication keys; **EIR** checks stolen/blacklisted IMEI.
- **GPRS: SGSN** (packet mobility + authentication) and **GGSN** (Internet gateway). This is the prototype of 4G EPC: SGSN ≈ MME + SGW, GGSN ≈ PGW.

Practice (MCQ)

1. In the formula $N = i^2 + ij + j^2$, what is N for (i,j) = (2,1)?

(a) 4 (b) 7

(c) 9 (d) 12

Answer: (b) — 4+2+1 = 7.

2. What is D/R for N = 7?

(a) 3 (b) 4.58

(c) 5.2 (d) 7

Answer: (b) — $\sqrt{21} = 4.583$.

3. What happens if N is increased (everything else unchanged)?

(a) Interference increases, capacity increases (b) Interference decreases, capacity per cell decreases

(c) Both increase (d) Nothing

Answer: (b) — D/R increases so SIR ↑, but channels per cell = total/N ↓.

4. Which is the assumption of Erlang B?

(a) Blocked calls wait in a queue (b) Blocked calls are dropped

(c) Calls are never blocked (d) Only for data traffic

Answer: (b) — Erlang B = blocked calls cleared; Erlang C = delayed.

5. 600 calls per hour, average 2 minutes → traffic?

(a) 10 E (b) 20 E

(c) 30 E (d) 1200 E

Answer: (b) — 600×(2/60) = 20 E.

6. If the cell radius is halved, the number of cells becomes how many times?

(a) 2 (b) 3

(c) 4 (d) 8

Answer: (c) — Area ∝ R^2.

7. Which handover is make-before-break?

(a) GSM hard (b) LTE hard

(c) WCDMA soft (d) None

Answer: (c) — In CDMA/WCDMA, connected to 2+ cells at the same time.

8. Where is the permanent data of a subscriber stored in GSM?

(a) VLR (b) HLR

(c) BSC (d) EIR

Answer: (b) — HLR is permanent; VLR is temporary.

9. Which is the Internet gateway in GPRS?

(a) SGSN (b) GGSN

(c) MSC (d) BSC

Answer: (b) — GGSN ≈ 4G PGW.

10. For N = 3, n = 4, what is the approximate SIR (6 interferers)?

(a) 11.3 dB
(b) 18.7 dB
(c) 24 dB
(d) 6 dB

Answer: (a) — $(3)^4/6 = 13.5 \rightarrow 11.3$ dB.

11. What is the main purpose of sectorisation?

(a) Increase power
(b) Reduce interference and increase SIR/capacity
(c) Make cells smaller
(d) Reduce frequency

Answer: (b) — Directional antennas instead of omni.

12. Which node checks the IMEI blacklist?

(a) AuC
(b) HLR
(c) EIR
(d) VLR

Answer: (c) — Equipment Identity Register.

Chapter 4 — Mobile Core and Backhaul Architectures

4.1 The Big Picture: Access – Transport – Core

View a mobile network in three parts: **Access (RAN)** — the radio connection with the user; **Transport/Backhaul** — the links from the site to the core; **Core** — authentication, mobility, sessions, routing and billing. The circular's "Mobile Core and Backhaul Architectures" means these last two parts.

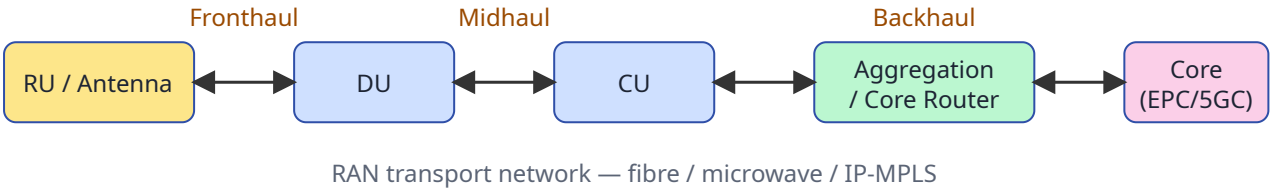


Figure 4.1: RAN transport — Fronthaul/Midhaul/Backhaul

4.2 3G UMTS Architecture (Quick Revision)

Node	Function	Interface
Node B	Base station (WCDMA)	Uu (UE–NodeB), Iub (NodeB–RNC)
RNC	Radio control, soft handover, power control	Iur (RNC–RNC), Iu-CS (→MSC), Iu-PS (→SGSN)
MSC/VLR, HLR	CS voice	—
SGSN/GGSN	PS data	Gn, Gi

In 4G the **RNC is removed** — its functions moved into the eNB (flat architecture), so delay is lower.

4.3 4G EPC Architecture

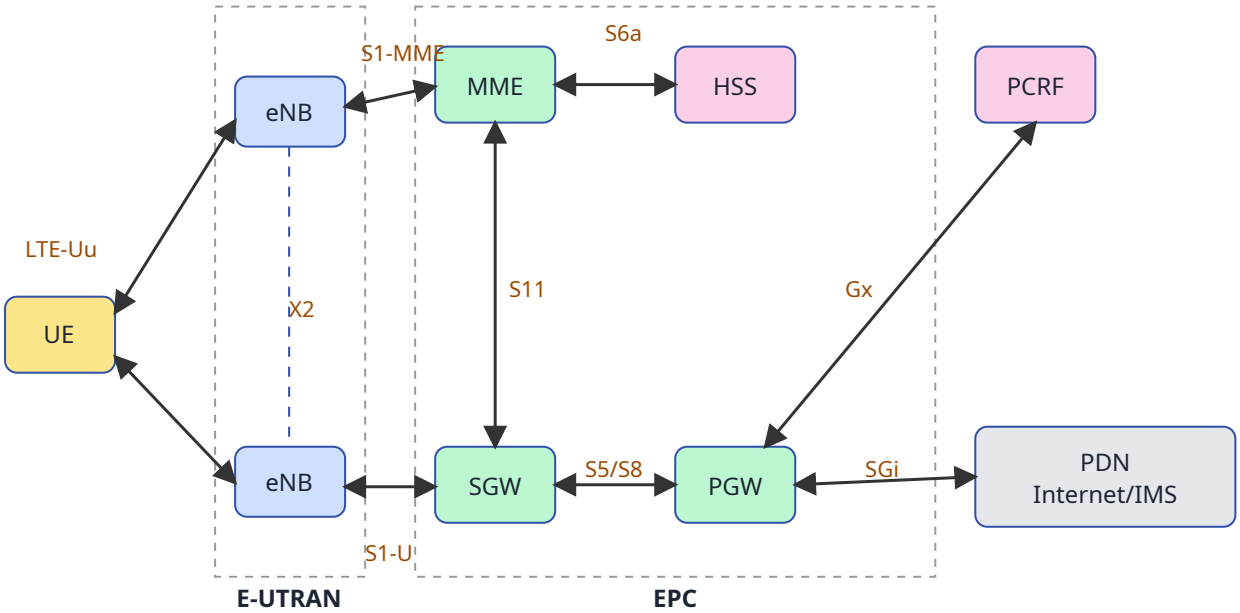


Figure 4.2: LTE/EPC architecture and interfaces

Node	Key function (exam points)
eNodeB	Radio resource management, scheduling, handover decisions, encryption, RRC/PDCP/RLC/MAC/PHY; MME and SGW selection (S1-flex)
MME	Control plane only — attach, authentication (with HSS), NAS security, tracking area management, paging, bearer setup, SGW/PGW selection
SGW	Local mobility anchor for user-plane traffic (during eNB handover); downlink buffering and paging trigger in IDLE state
PGW	Connection to the external PDN; allocates the IP address to the UE; policy enforcement (PCEF); charging; packet filtering
HSS	Subscriber profile and authentication vectors (Chapter 12)
PCRF	Decides QoS and charging policy (PCC)

Interface	Connects	Protocol
LTE-Uu	UE – eNB	RRC/PDCP/RLC/MAC
S1-MME	eNB – MME	S1AP / SCTP
S1-U	eNB – SGW	GTP-U / UDP
S11	MME – SGW	GTP-C
S5/S8	SGW – PGW (S5 = same operator, S8 = roaming)	GTP / PMIP
S6a	MME – HSS	Diameter
Gx	PCRF – PGW	Diameter
SGi	PGW – PDN	IP
X2	eNB – eNB	X2AP (data forwarding during handover)
S10	MME – MME	GTP-C

> **Memory Trick**
>
> **MME** = 'M' for Mobility (control), **SGW** = 'S' for Serving (local anchor), **PGW** = 'P' for PDN (the outside world). S1-**MME** = signalling, S1-**U** = user data.

4.4 5G Core (5GC) — Service-Based Architecture (SBA)

The 5G core is cloud-native: every network function (NF) is a **service** that talks to the others through HTTP/2 REST APIs. The control plane and user plane are fully separate (**CUPS**).

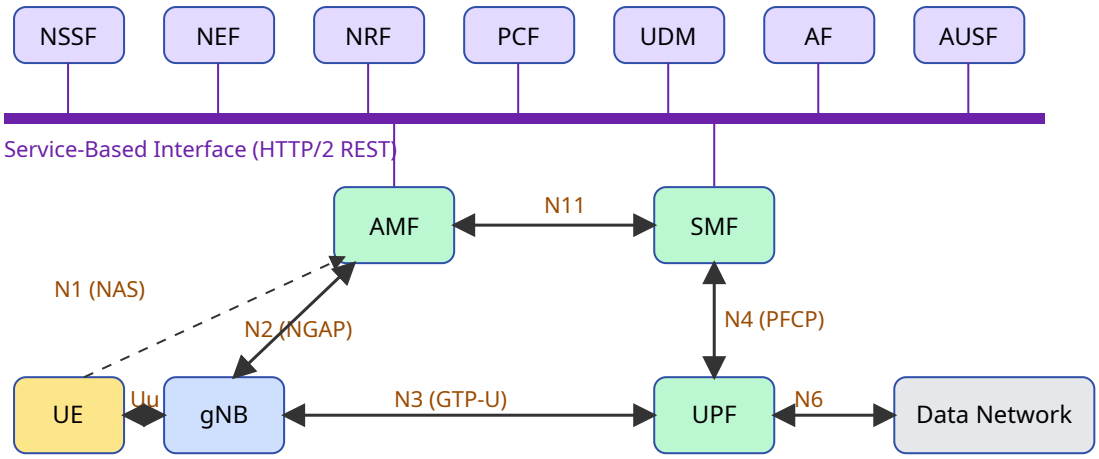


Figure 4.3: 5GC SBA — reference points and service bus

5G NF	Full form	Function	4G equivalent
AMF	Access and Mobility Management Function	Registration, connection, mobility, NAS security, paging	MME (mobility part)
SMF	Session Management Function	PDU session, IP allocation, UPF selection/N4 control	MME (session) + SGW-C/PGW-C
UPF	User Plane Function	Packet forwarding, QoS, traffic reporting, edge	SGW-U/PGW-U
UDM / UDR	Unified Data Management/Repository	Subscriber data, authentication credentials	HSS
AUSF	Authentication Server Function	Performs 5G-AKA/EAP-AKA'	HSS (part)
PCF	Policy Control Function	Policy	PCRF
NRF	NF Repository Function	Service discovery/registration	None (new)
NSSF	Network Slice Selection Function	Slice selection	None (new)
NEF	Network Exposure Function	Securely exposes APIs to external applications	SCEF
CHF	Charging Function	Converged charging	OCS/OFCS

Reference point	Connects
N1	UE – AMF (NAS)
N2	gNB – AMF (NGAP)
N3	gNB – UPF (GTP-U)
N4	SMF – UPF (PFCP)
N6	UPF – Data Network
N9	UPF – UPF

N11	AMF – SMF
N8/N10/N12/N13	AMF–UDM / SMF–UDM / AMF–AUSF / AUSF–UDM
Xn	gNB – gNB (handover)

NSA vs SA

NSA (Non-Standalone, Option 3x): 5G NR radio but a 4G EPC core (fast deployment, limited features). **SA (Standalone, Option 2):** 5G NR + 5GC — slicing, URLLC and full SBA benefits are available only in SA.

4.5 Backhaul: Media and Technology

Medium	Characteristics	Best suited for
Optical fibre	Highest capacity (10–100G+), low delay; costly and right-of-way problems	City, macro sites, 5G
Microwave (6–42 GHz) / E-band (71–86 GHz)	Fast deployment, no fibre needed; requires LOS, fades in rain (more at high bands)	Villages, hills, across rivers
Satellite (VSAT, LEO)	Remote areas; high delay (GEO ≈ 500+ ms RTT)	Off-grid, disaster areas
Copper (xDSL), PON	Limited	Fixed / small cells

Technology: legacy PDH/SDH (E1, STM-n) → **Carrier Ethernet (MEF)** → **IP/MPLS** (L2VPN/L3VPN, service isolation) → in the future **Segment Routing/SRv6**, **OTN/DWDM** (fibre capacity), **FlexE** (hard isolation for slicing). Topology: star, ring (fast protection < 50 ms), tree.

Synchronization — the Invisible Hero of Backhaul

- For FDD, **frequency sync**: ±50 ppb (at the base station air interface). For TDD (LTE-TDD/5G NR) and CoMP, **phase sync ±1.5 µs**.
- Sources: **GNSS (GPS)**, **SyncE** (frequency), **IEEE 1588v2 PTP** (phase + time). If GPS is not available, use a PTP grandmaster.

Microwave Link: Fresnel Zone

LOS is not just a straight line — at least 60% of the first Fresnel zone must be free of obstruction:

$$r_1 = 17.3 \sqrt{(d_1\, d_2 / (f \cdot d))} \quad [\text{m; } d_1, d_2, d = \text{km; } f = \text{GHz}]$$

Example: Fresnel Radius

d = 10 km, midpoint $d_1 = d_2 = 5$ km, f = 7 GHz → $r_1 = 17.3 \times \sqrt{(25/(7\times10))} = 17.3 \times 0.5976 =$ **10.3 m**.
60% = 6.2 m clearance required.

Backhaul Capacity Planning

Example: Backhaul of a 3-Sector Site

Busy-hour average per sector = 40 Mbps, peak = 150 Mbps. Common design rule (NGMN-style):

$$\text{Required} \approx \max(\Sigma \text{ average},\ \text{Peak}_{\text{1 sector}} + \Sigma \text{ average}_{\text{remaining}})$$

= max(3×40, 150 + 2×40) = max(120, 230) = **230 Mbps**; adding ~10–20% GTP/IPsec overhead ≈ 260–275 Mbps → a 1 GbE link is enough; for a 5G site assume 10 GbE. (This is an example of a design rule; it varies slightly between operators.)

4.6 Core Redundancy

- **Pooling:** several MME/AMF in one pool; the eNB/gNB can choose any one (S1-flex / N2-flex); load sharing + failover.
- **Geo-redundancy:** backup in a separate data centre — disaster resistance.
- **Availability:** series and parallel systems (formulas in Chapter 6). Telecom-grade target: "five nines" = 99.999% (≈ 5.26 minutes downtime per year).

Practice (MCQ)

1. Which interface connects the MME and eNB in LTE?

(a) S1-U (b) S1-MME
(c) S11 (d) S6a

Answer: (b) — S1-MME = signalling; S1-U = data.

2. Which nodes does the S6a interface connect?

(a) MME–HSS (b) SGW–PGW
(c) eNB–SGW (d) PGW–PCRF

Answer: (a) — S6a = MME–HSS, Diameter.

3. Which node connects to the external internet and allocates IP addresses?

(a) MME (b) SGW
(c) PGW (d) HSS

Answer: (c) — PGW (in 5G, UPF + SMF).

4. Which interface is between SMF and UPF in the 5G core?

(a) N2 (b) N3
(c) N4 (d) N6

Answer: (c) — N4 — PFCP.

5. Which is the user-plane interface between gNB and UPF?

(a) N1 (b) N2
(c) N3 (d) N9

Answer: (c) — N3 (GTP-U).

6. Which is completely new in the 5GC and has no 4G equivalent?

(a) AMF (b) NRF
(c) UPF (d) UDM

Answer: (b) — NRF/NSSF are new; the others have 4G equivalents.

7. What phase sync accuracy is normally required in TDD networks?

(a) ±1.5 µs (b) ±15 ms
(c) ±1 s (d) Not required

Answer: (a) — ±1.5 µs for TDD/NR.

8. Which of the following was removed in 4G and its functions moved into the eNB?

(a) MSC (b) RNC
(c) HLR (d) GGSN

Answer: (b) — The RNC's functions are in the eNB.

9. What is the downtime per year at five-nines (99.999%) availability?

(a) ≈ 5 minutes (b) ≈ 53 minutes
(c) ≈ 9 hours (d) ≈ 3.5 days

Answer: (a) — (1−0.99999)×525600 ≈ 5.26 minutes.

10. Which is a feature of 5G SA?

(a) Uses a 4G EPC core (b) Uses 5GC and supports slicing
(c) mmWave only (d) No core

Answer: (b) — SA = NR + 5GC.

11. What minimum fraction of the first Fresnel zone should be clear on a microwave link?

(a) 20% (b) 40%
(c) 60% (d) 100%

Answer: (c) — The general rule is 60%.

12. Which technology carries phase and time sync in the backhaul?

(a) SyncE (b) IEEE 1588v2 (PTP)
(c) E1 (d) STM-1

Answer: (b) — SyncE carries frequency only.

Chapter 5 — Packet-Switched Mobile Networks

5.1 Why Packet-Switched Mobile Networks?

In 2G, data was circuit-switched (CSD, slow). Mobile **packet data** arrived with GPRS (2.5G) — resources are used only while sending data, and the user stays "always-on". In 4G the whole network is **all-IP** — even voice travels as IP packets (VoLTE). In 5G it is even more flexible and virtualized.

	2.5G GPRS	3G UMTS PS	4G EPS	5G
Access	BSS	UTRAN	E-UTRAN	NG-RAN
Mobility/session	SGSN	SGSN	MME + SGW	AMF + SMF
Gateway	GGSN	GGSN	PGW	UPF
Session name	PDP context	PDP context	EPS bearer	PDU session
QoS	—	Traffic class	QCI	5QI / QoS Flow

5.2 The Bearer Concept (EPS Bearer)

Bearer = a logical data pipe with a specific QoS (UE ↔ PGW). Each EPS bearer has three parts: Radio bearer + S1 bearer + S5/S8 bearer.

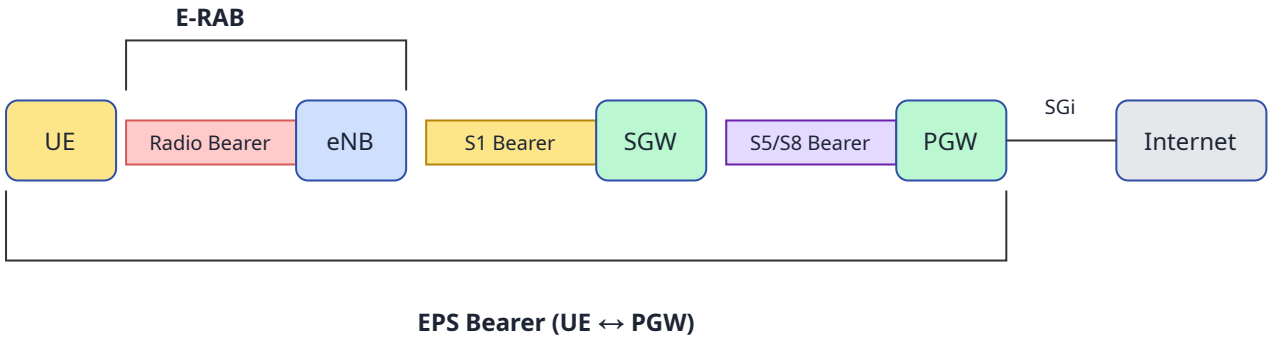


Figure 5.1: Structure of an EPS bearer (E-RAB = radio bearer + S1 bearer)

- **Default bearer:** created automatically at Attach; gives the UE its IP; non-GBR (usually QCI 9); always stays active.
- **Dedicated bearer:** an additional bearer when special QoS is needed (e.g., VoLTE QCI 1); GBR or non-GBR.
- **GBR** (Guaranteed Bit Rate) — guaranteed bandwidth; **Non-GBR** — best effort.

QCI	Type	Delay budget	Loss rate	Example
1	GBR	100 ms	10^{-2}	Conversational voice (VoLTE)
2	GBR	150 ms	10^{-3}	Video call
3	GBR	50 ms	10^{-3}	Real-time gaming

4	GBR	300 ms	10^{-6}	Buffered video
5	Non-GBR	100 ms	10^{-6}	IMS signalling (SIP)
6	Non-GBR	300 ms	10^{-6}	TCP-based video/web
7	Non-GBR	100 ms	10^{-3}	Voice/video/game (live)
8/9	Non-GBR	300 ms	10^{-6}	Premium / default (best effort)

In 5G: QoS is flow-based — inside a PDU session there are several **QoS Flows** (identified by QFI), each with a **5QI**; 5QI 1 = voice, 5QI 5 = IMS signalling, 5QI 9 = default; delay-critical GBR for URLLC (e.g., 5QI 82–85).

5.3 GTP Tunnelling

Inside the core, the UE's IP packet is not routed directly; it is wrapped in a **GTP-U tunnel**. Each tunnel is identified by a **TEID** (Tunnel Endpoint ID, 32 bits). So core routing stays simple even when the UE's IP changes or the endpoint changes due to mobility.

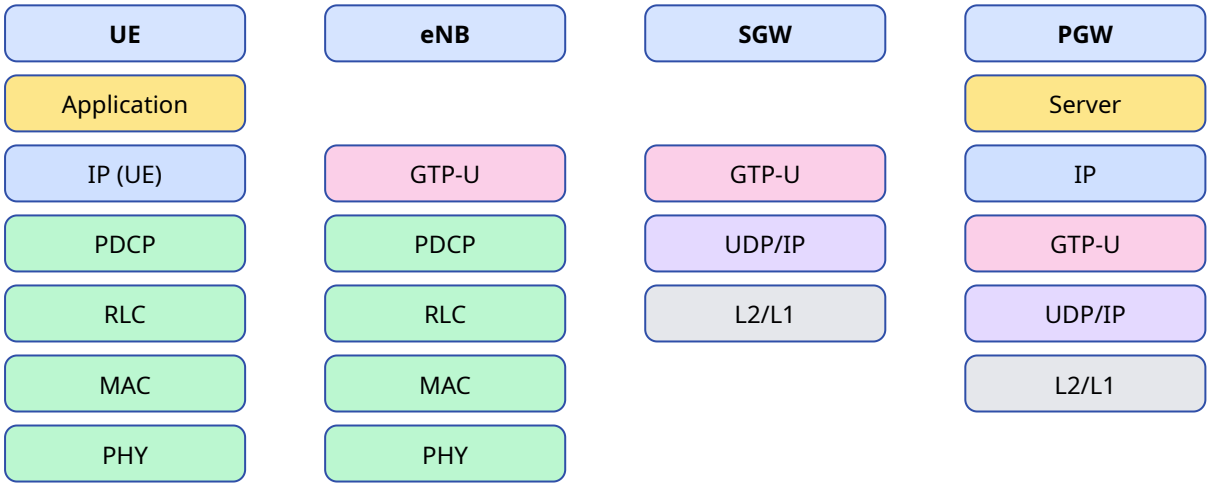


Figure 5.2: LTE user-plane protocol stack

Example: GTP Overhead

GTP-U header 8 bytes, UDP 8 bytes, outer IPv4 20 bytes ⇒ total **36 bytes** extra (56 bytes with IPv6 transport). If the UE packet is 1400 bytes, the transport packet = 1436 bytes; overhead = 36/1436 ≈ **2.5%**. For small packets (e.g., 72-byte VoIP) the overhead is 33% — so voice needs ROHC header compression (Chapter 11). To avoid MTU problems, the UE MTU is usually set to about 1358–1400.

5.4 IP Address, APN, NAT

- **APN** (Access Point Name; **DNN** in 5G): the name of the network to connect to (Internet, IMS, corporate), e.g., `internet`, `ims`. The UE keeps separate PDN connections for Internet and IMS.
- IP allocation: by the PGW/SMF itself, or from DHCP/RADIUS; IPv4, IPv6 (SLAAC /64), or dual-stack.

- Because of IPv4 shortage, operators use **CGNAT** (Carrier-Grade NAT) — many users share one public IP. IPv6 is the solution to this problem.

5.5 Policy and Charging (PCC)

PCRF (4G) / **PCF** (5G) decides what QoS and charging apply to which traffic. **PCEF** (in PGW/UPF) enforces it (Gx). Charging: online (prepaid, **OCS**, Gy) and offline (postpaid, **OFCS**/CDR, Gz); in 5G, **CHF** (converged). FUP/throttling and data-saver are also done through PCC.

5.6 Performance: Bandwidth-Delay Product

For TCP to run at full speed, enough data must be in flight to fill the network "pipe":

BDP = Bandwidth × RTT

Example: BDP

Link 100 Mbps, RTT = 50 ms → BDP = $100 \times 10^6 \times 0.05 / 8$ = **625,000 bytes ≈ 610 KB**. If the TCP window is smaller than this, speed is stuck below the link capacity. So in 5G, latency directly affects TCP throughput.

Practice (MCQ)

1. Which bearer is created automatically at Attach?

(a) Dedicated (b) Default
(c) GBR (d) S11

Answer: (b) — Default bearer — the IP address is allocated.

2. Which QCI is used for VoLTE voice packets?

(a) 1 (b) 5
(c) 8 (d) 9

Answer: (a) — QCI 1 GBR. QCI 5 = IMS signalling.

3. Which field identifies a GTP-U tunnel?

(a) IMSI (b) TEID
(c) APN (d) QCI

Answer: (b) — Tunnel Endpoint Identifier.

4. Which 5G NF is equivalent to the PGW?

(a) AMF (b) UPF (with SMF)
(c) NRF (d) NSSF

Answer: (b) — PGW-C ≈ SMF, PGW-U ≈ UPF.

5. What is the total extra overhead of GTP-U + UDP + IPv4?

(a) 20 (b) 28
(c) 36 (d) 56

Answer: (c) — 8+8+20 = 36.

6. What is the internal QoS unit of a PDU session in 5G?

(a) EPS bearer (b) QoS Flow (QFI)
(c) APN (d) PDP context

Answer: (b) — QoS Flow, identified by QFI.

7. What is the 5G equivalent of APN?

(a) DNN (b) SUCI
(c) TAC (d) PLMN

Answer: (a) — Data Network Name.

8. What do operators use to cope with the IPv4 shortage?

(a) CGNAT (b) DHCP-Relay
(c) OSPF (d) ARP

Answer: (a) — Carrier-grade NAT; IPv6 in the long term.

9. What is the BDP for 100 Mbps and RTT 40 ms?

(a) 250 KB (b) 500 KB
(c) 4 MB (d) 1 MB

Answer: (b) — 100e6×0.04/8 = 500,000 B.

10. Which node decides the QoS/charging policy (4G)?

(a) PCRF (b) HSS
(c) SGW (d) eNB

Answer: (a) — PCRF → informs the PGW over Gx.

Chapter 6 — NFV — Network Function Virtualization

Network Function Virtualization in Cellular Systems

6.1 The Problem: Why NFV?

Earlier, MME, PGW, firewall, SBC — each was a separate **proprietary hardware appliance** (vendor lock-in). It took months to install, capacity was wasted when load was low, and scaling was hard.

> **What is NFV?**
>
> **Network Function Virtualization:** separating network functions from hardware and running them as **software (VNFs)** in virtual machines/containers on standard (COTS) servers. The concept was proposed by the ETSI NFV ISG (2012); the architecture standard is ETSI GS NFV.

Benefit	Explanation
CAPEX ↓	Cheap COTS hardware, shared resources
OPEX ↓	Automation, less power/space
Fast service	New service deployed in hours
Elastic scaling	Add VNF instances when load rises, reduce when it falls
Vendor independence	Hardware and software from different vendors

6.2 ETSI NFV Architecture

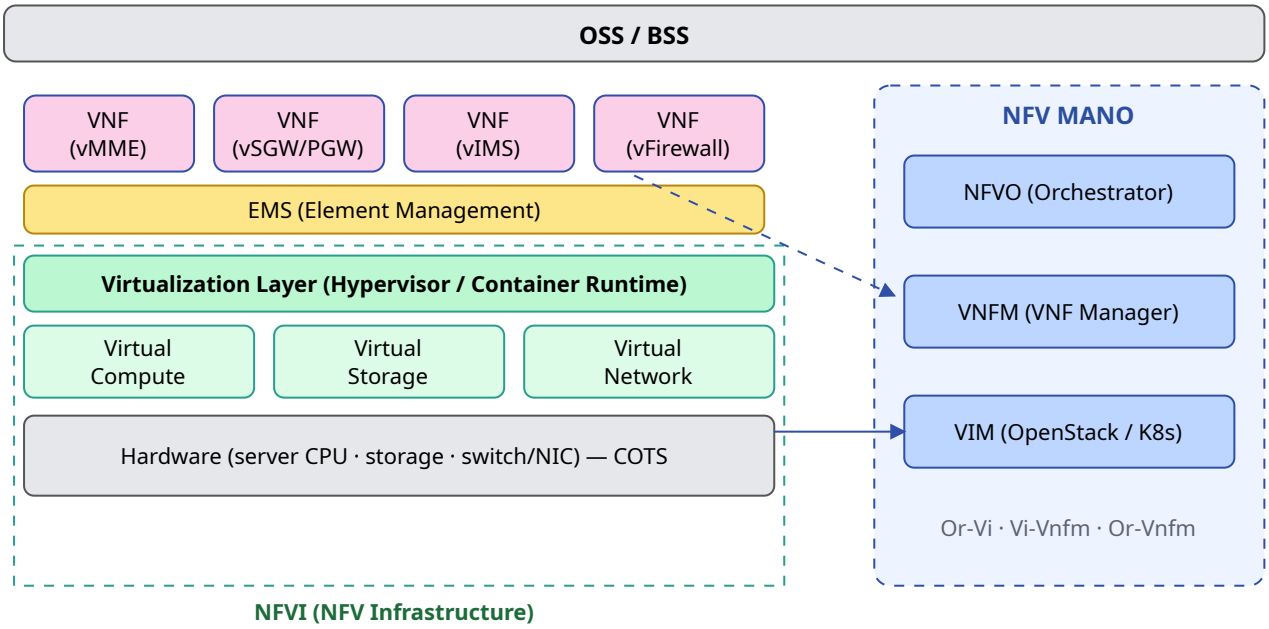


Figure 6.1: ETSI NFV architecture (NFVI + VNF + MANO)

- **VNF** — virtual network function (vEPC, vIMS, vRouter, vFW, vCPE, vBBU). **EMS** manages the FCAPS of the VNF.

- **NFVI** — the infrastructure on which VNFs run: hardware + virtualization layer (hypervisor KVM/VMware; or container runtime).
- **MANO** (Management and Orchestration): **NFVO** — network service orchestration, resource coordination; **VNFM** — VNF lifecycle (instantiate, scale, heal, terminate); **VIM** — controls hardware resources (OpenStack, Kubernetes).

VM vs Container (VNF vs CNF)

	VM (VNF)	Container (CNF)
Isolation	Strong (full OS)	Light (shared kernel)
Boot time	Minutes	Seconds
Resources	More	Less
Tool	OpenStack/KVM	Kubernetes/Docker
5G core	Initial	**Cloud-native 5GC = CNF, microservices**

Technologies to increase performance: DPDK (kernel bypass, fast packet processing in user space), **SR-IOV** (presents the NIC directly to a VM as a virtual function), **CPU pinning/NUMA**, **SmartNIC/FPGA offload**.

6.3 NFV vs SDN

	NFV	SDN
Core idea	Separate functions from hardware	Separate the control plane and data plane
What is virtualized	Router, firewall, EPC, etc.	The intelligence of the switch/router goes to a central controller
Protocols	—	OpenFlow, NETCONF/YANG, P4
Relationship	Independent, but most effective together (SDN provides network connectivity, NFV runs the functions)	

Service Function Chaining (SFC): sending packets through VNFs in a specified order (e.g., firewall → DPI → NAT → internet), set up dynamically with SDN.

6.4 Maths: Scaling and Availability

Example: How many VNF instances are needed?

Each vUPF instance = 10 Gbps; peak traffic = 35 Gbps; redundancy N+1. N = ⌈35/10⌉ = 4; +1 ⇒ **5 instances**. When traffic falls, scale-in saves resources.

Availability: in series (works only if all work): $A_s = A_1 \cdot A_2 \cdot \ldots$; in parallel (works if any one works): $A_p = 1 - (1-A_1)(1-A_2)\ldots$.

Example: Availability

One VNF has A = 99.9% (0.999). Two in parallel: $1 - (0.001)^2 = 0.999999$ = **99.9999%**. Three 99.9% links in series: $0.999^3 = 0.997$ = **99.7%** — the longer the chain, the lower the availability, so redundancy is needed.

NFV Challenges

- Performance (is it equal to hardware?) · multi-vendor interoperability · security (hypervisor attacks) · skill gap · MANO complexity.

Practice (MCQ)

1. What is the core idea of NFV?

(a) Separate control/data plane
(b) Run network functions as software on COTS
(c) Use only fibre
(d) Make radio virtual

Answer: (b) — The core idea of SDN is separating the planes.

2. Who manages the VNF lifecycle (instantiate/scale/terminate)?

(a) NFVO
(b) VNFM
(c) VIM
(d) EMS

Answer: (b) — VNFM; VIM = hardware resources, NFVO = service orchestration.

3. In which MANO role is OpenStack normally used?

(a) NFVO
(b) VNFM
(c) VIM
(d) OSS

Answer: (c) — Virtualized Infrastructure Manager.

4. Which is the popular orchestrator for container-based cloud-native functions?

(a) Kubernetes
(b) KVM
(c) OpenFlow
(d) SNMP

Answer: (a) — CNF → Kubernetes.

5. What does DPDK do?

(a) Reduces radio interference
(b) Fast packet processing by bypassing the kernel
(c) Voice codec
(d) IP addressing

Answer: (b) — High-speed packet processing in user space.

6. What is the availability when two 99.9% units are in parallel?

(a) 99.8%
(b) 99.99%
(c) 99.9999%
(d) 99.9%

Answer: (c) — $1-0.001^2 = 0.999999$.

7. For 25 Gbps traffic, 10 Gbps per instance and N+1, how many instances?

(a) 3 (b) 4

(c) 2 (d) 5

Answer: (b) — ⌈2.5⌉ = 3, +1 = 4.

8. What does the NFVI contain in ETSI NFV?

(a) Only VNFs (b) Hardware and virtualization layer

(c) OSS/BSS (d) Only EMS

Answer: (b) — NFVI = compute/storage/network + virtualization layer.

9. OpenFlow is related to which technology?

(a) NFV (b) SDN

(c) IMS (d) CDMA

Answer: (b) — SDN controller–switch protocol.

Chapter 7 — C-RAN and O-RAN

Cloud RAN & Open Radio Access Networks

7.1 Limitations of Traditional RAN (D-RAN)

In Distributed RAN, every site has the antenna + RRU + BBU together. Each site needs its own room, AC, power and maintenance. When the load drops, the spare capacity of one site cannot be used by other sites. Inter-cell interference coordination (CoMP) is also difficult.

7.2 C-RAN (Centralized / Cloud RAN)

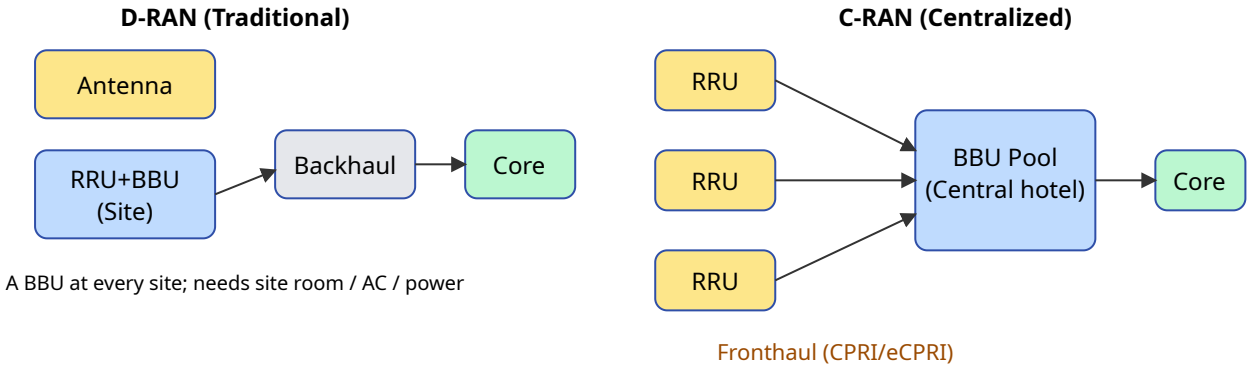


Figure 7.1: D-RAN vs C-RAN

In C-RAN, the BBUs are brought together in one place (a **BBU pool/hub**) and run on virtualized servers. Only the antenna and the **RRU/RRH** stay at the site. The RRU–BBU link is called **Fronthaul**.

Advantages	Challenges
Resource pooling — statistical multiplexing gain	Huge bandwidth on the fronthaul (CPRI)
Lower site cost / power	Strict latency (≈ 100 µs–250 µs round-trip budget)
CoMP and inter-cell interference coordination are easier	Fibre availability and cost
Fast rollout/upgrade	Large pool = single point of failure

Example: CPRI Fronthaul Bitrate

Sampling rate for LTE 20 MHz = 30.72 MS/s; I and Q → ×2; 15 bits/sample; control overhead ×16/15; 8b/10b encoding ×10/8.

Per antenna = $30.72 \times 10^6 \times 2 \times 15 \times (16/15) \times (10/8)$ = **1228.8 Mbps** (= CPRI Option 2). With 4T4R = **4.9152 Gbps** (Option 5).

For 5G 100 MHz (122.88 MS/s), per antenna ≈ 4.9152 Gbps; with **64T64R massive MIMO** ≈ **314.6 Gbps** — impossible on fibre! So CPRI (split option 8) does not scale to 5G; **eCPRI / functional split 7.2** is needed.

Functional Split

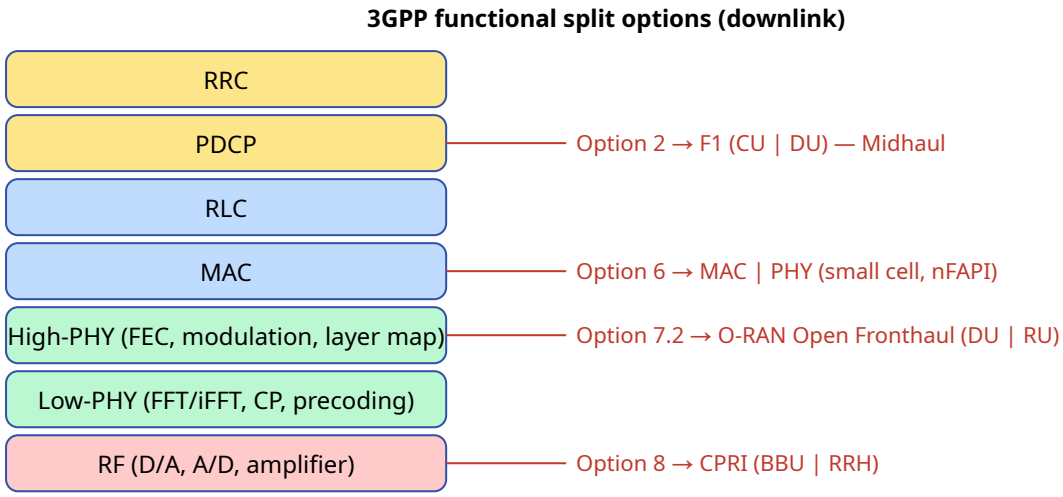


Figure 7.2: RAN functional split options. Splitting lower = more fronthaul bandwidth, but more centralization benefit.

In 5G NG-RAN, gNB = **CU** (Central Unit: RRC, PDCP) + **DU** (Distributed Unit: RLC, MAC, high-PHY) + **RU** (Radio Unit: low-PHY, RF). Link names: **Fronthaul** (RU–DU), **Midhaul** (DU–CU, F1), **Backhaul** (CU–Core, NG). The CU can be split further into CU-CP and CU-UP (E1 interface).

7.3 Open RAN and O-RAN

> **Concept**
>
> In conventional RAN, the RU–DU–CU come from the same vendor and the interfaces are proprietary. **Open RAN** = open, interoperable interfaces, so RU/DU/CU from different vendors work together. The **O-RAN Alliance** (founded 2018 by AT&T, China Mobile, Deutsche Telekom, NTT DOCOMO, Orange) is the body that writes the specifications (merger of C-RAN Alliance + xRAN Forum). Goal: **Open (open interfaces) + Virtualized (vRAN) + Intelligent (RIC) + Interoperable**.

Difference: vRAN = RAN software virtualized; C-RAN = centralized architecture; O-RAN = open interfaces + RIC. They are separate concepts but can be used together.

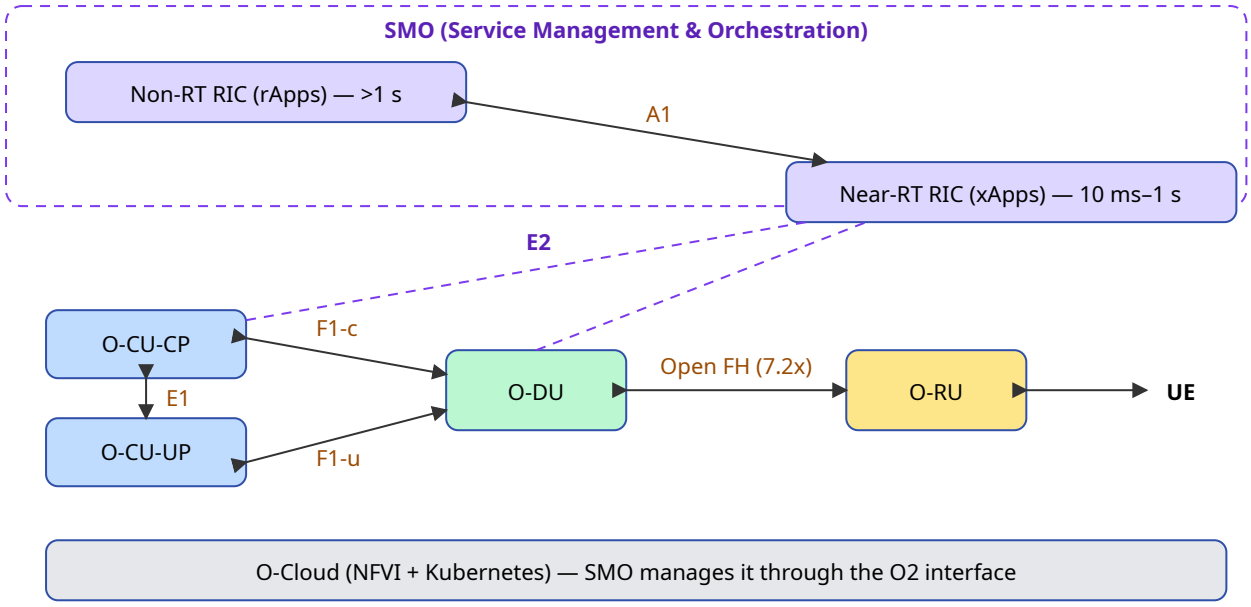


Figure 7.3: O-RAN logical architecture. O1: SMO ↔ all O-RAN nodes (FCAPS) | A1: policy/AI models | E2: Near-RT RIC ↔ CU/DU control

Component / Interface	Function
O-RU / O-DU / O-CU	Radio / Distributed / Central Unit with open interfaces
Near-RT RIC	RAN Intelligent Controller — 10 ms–1 s control loop; runs **xApps** (load balancing, handover optimization, interference management)
Non-RT RIC	Inside the SMO; >1 s loop; **rApps**; trains AI/ML models and creates policies
SMO	Service Management and Orchestration — automation and management of the whole network
O-Cloud	Cloud infrastructure (NFVI) that runs the O-RAN functions
Open Fronthaul	O-DU–O-RU, split 7.2x, C/U/S/M-plane (Control, User, Sync, Management)
E2	Near-RT RIC ↔ O-CU/O-DU (control and telemetry)
A1	Non-RT RIC → Near-RT RIC (policy, ML models)
O1	SMO ↔ O-RAN nodes (FCAPS management)
O2	SMO ↔ O-Cloud
F1 / E1 / Xn / NG	3GPP interfaces (CU–DU / CU-CP–CU-UP / gNB–gNB / gNB–Core)

Advantages and Challenges

- **Advantages:** less vendor lock-in, lower cost through competition, innovation (self-automated optimization with AI/ML), supply-chain diversity (important for security/geopolitical reasons).
- **Challenges:** multi-vendor integration complexity, power efficiency, interoperability testing, unclear responsibility (who is the integrator), new security attack surface.

> **For Drawing in the Exam**
>
> In an O-RAN diagram, at least write: SMO (Non-RT RIC) ↔ A1 ↔ Near-RT RIC ↔ E2 ↔ CU/DU; DU ↔ Open FH ↔ RU; SMO ↔ O1 ↔ all nodes; SMO ↔ O2 ↔ O-Cloud.

Practice (MCQ)

1. What is the link between the RRU and the BBU in C-RAN called?

(a) Backhaul
(b) Midhaul
(c) Fronthaul
(d) Sidehaul

Answer: (c) — RRU–BBU = Fronthaul.

2. What is the CPRI rate for LTE 20 MHz, 1 antenna?

(a) 614.4 Mbps
(b) 1228.8 Mbps
(c) 2457.6 Mbps
(d) 4915.2 Mbps

Answer: (b) — 30.72M×2×15×16/15×10/8.

3. In the O-RAN Alliance architecture, what time scale does the Near-RT RIC control loop use?

(a) < 1 ms
(b) 10 ms – 1 s
(c) > 1 s
(d) Several hours

Answer: (b) — Near-RT = 10 ms–1 s; Non-RT > 1 s.

4. Where is the A1 interface?

(a) Near-RT RIC – CU
(b) Non-RT RIC – Near-RT RIC
(c) DU – RU
(d) SMO – O-Cloud

Answer: (b) — It carries policy/ML models.

5. Which nodes does the E2 interface connect?

(a) SMO–O-Cloud
(b) Near-RT RIC – O-CU/O-DU
(c) RU–DU
(d) CU–Core

Answer: (b) — Control and telemetry.

6. Which split does O-RAN use for Open Fronthaul?

(a) Option 2
(b) Option 6
(c) Option 7.2x
(d) Option 8

Answer: (c) — Option 7.2x is the O-RAN split; Option 8 = CPRI.

7. Where is the F1 interface?

(a) CU–DU
(b) DU–RU
(c) gNB–gNB
(d) UE–gNB

Answer: (a) — Option 2 split — Midhaul.

8. Where does an xApp run?

(a) Non-RT RIC
(b) Near-RT RIC
(c) O-RU
(d) UPF

Answer: (b) — xApp = Near-RT, rApp = Non-RT.

9. What is the main reason CPRI does not scale in Massive MIMO?

(a) Low latency
(b) Fronthaul bitrate grows linearly with the number of antennas
(c) Low frequency
(d) Low power

Answer: (b) — About 4.9 Gbps per antenna × 64.

10. What is the function of the O1 interface?

(a) User data
(b) SMO ↔ node management (FCAPS)
(c) UE control
(d) Charging

Answer: (b) — O1 = Operations & Maintenance.

Chapter 8 — 5G Network Slicing

8.1 The Idea: One Network, Different Purposes

5G must deliver 3 completely different types of service with conflicting requirements. It is hard to fit them all into one network. So we use **Network Slicing**: one physical network is divided logically into several **isolated end-to-end virtual networks** (slices), each tuned for a specific service.

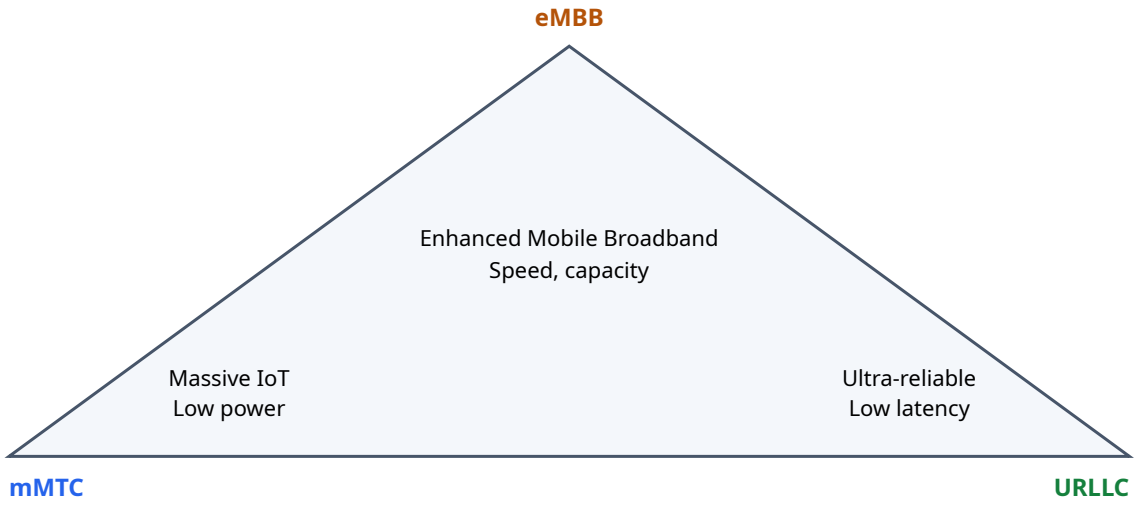


Figure 8.1: The three 5G usage scenarios (IMT-2020 triangle)

Area	Target	Examples
eMBB	Peak data rate DL 20 Gbps / UL 10 Gbps; user-experienced rate 100/50 Mbps	4K/8K video, AR/VR, FWA
URLLC	Air-interface latency 1 ms; reliability ≈ 99.999%	Autonomous driving, remote surgery, factory automation
mMTC	1 million devices/km^2; low power, long battery life	Smart meters, agriculture sensors, trackers

Other IMT-2020 targets: mobility 500 km/h, spectral efficiency 3× IMT-Advanced, area traffic capacity 10 Mbps/m^2.

8.2 Structure of a Slice

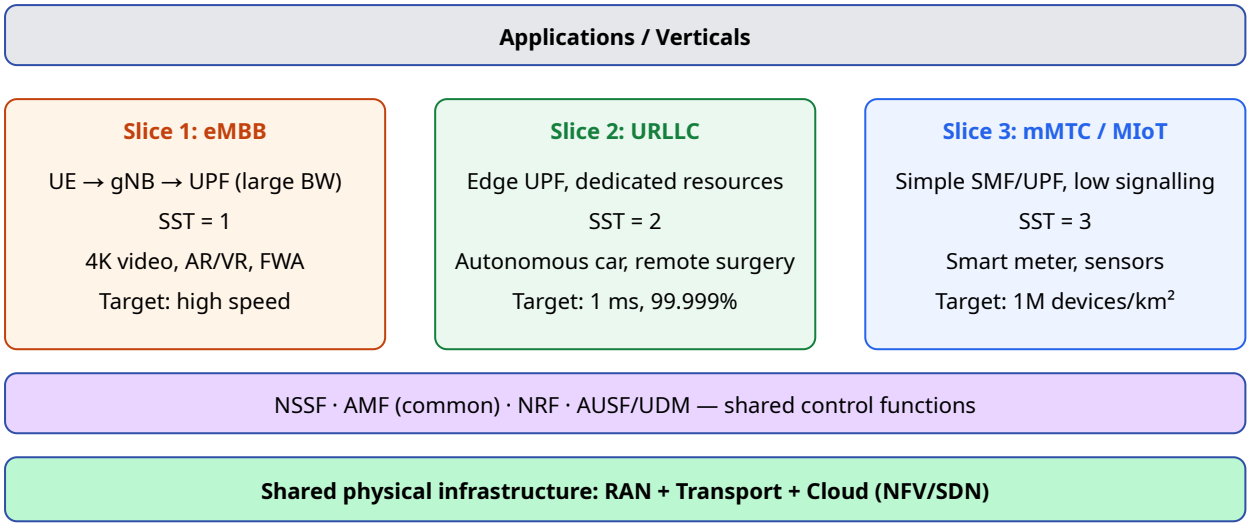


Figure 8.2: Three slices on a shared infrastructure

Each slice can have its own **RAN resources** (share of PRBs/capacity), **transport** (VLAN/VPN/Segment Routing/FlexE), and **core NFs** (separate SMF/UPF). Together they form an **end-to-end** slice.

> **S-NSSAI and Terminology**
>
> **S-NSSAI** (Single Network Slice Selection Assistance Information) = **SST** (Slice/Service Type, 8 bits) + optional **SD** (Slice Differentiator, 24 bits). Standard SST values: **1 = eMBB, 2 = URLLC, 3 = MIoT (mMTC), 4 = V2X**. **NSSAI** = a set of S-NSSAIs. In registration the UE sends the Requested NSSAI; the network returns the Allowed NSSAI. **NSI** = Network Slice Instance.

8.3 How Is a Slice Selected?

1. The UE sends the Requested NSSAI in the **Registration Request**.
2. The **AMF** checks the subscription (Subscribed S-NSSAI from the UDM); if needed it asks the **NSSF** which slice/AMF set is suitable.
3. The AMF tells the UE the **Allowed NSSAI** (Registration Accept).
4. In **PDU Session Establishment** the UE requests a specific S-NSSAI; the AMF finds the **SMF** of the right slice through the **NRF**; the SMF selects the relevant **UPF**.

> **Role of the NSSF**
>
> The decision: "which slices this UE gets and which AMF/NSI will serve it".

8.4 Enabling Technologies

Technology	Role in slicing
NFV	Instant deployment and scaling of VNF/CNF

SDN	Dynamic path and QoS in the transport network
SBA (5GC)	Modular NFs — a custom NF set per slice
RAN sharing	PRB partitioning, slice-aware scheduler
MANO/Orchestrator	Slice lifecycle (create → activate → modify → terminate)

Slice lifecycle: Preparation → Commissioning → Operation (monitoring, modification) → Decommissioning. Slice characteristics (latency, throughput, isolation) are described in the GSMA **GST/NEST** template.

Isolation and SLA

- Overload in one slice must not affect the others (resource, security and management isolation).
- **SLA** of each slice: latency, jitter, throughput, availability.

Example: Business Case

An operator gives a factory a URLLC slice: edge UPF (next to the factory), 5QI delay-critical GBR, latency < 10 ms, 99.999% availability. At the same time, ordinary users on the same RAN watch video in the eMBB slice — neither disturbs the other. The operator can sell each slice at a different price (Network-as-a-Service).

Practice (MCQ)

1. What are the two parts of S-NSSAI?

(a) SST and SD
(b) SUPI and SUCI
(c) TAC and PLMN
(d) QFI and 5QI

Answer: (a) — SST (Slice/Service Type) + SD (Slice Differentiator).

2. SST = 2 means which type of slice?

(a) eMBB
(b) URLLC
(c) MIoT
(d) V2X

Answer: (b) — 1 eMBB, 2 URLLC, 3 MIoT, 4 V2X.

3. Which NF helps in slice selection?

(a) NSSF
(b) UPF
(c) PCF
(d) EIR

Answer: (a) — Network Slice Selection Function.

4. What is the air-interface latency target of URLLC?

(a) 10 ms
(b) 1 ms
(c) 100 ms
(d) 1 s

Answer: (b) — IMT-2020: 1 ms.

5. What is the device density target of mMTC?

(a) 10^3/km² (b) 10^4/km²

(c) 10^6/km² (d) 10^9/km²

Answer: (c) — 1 million/km².

6. What is the peak downlink target of 5G eMBB?

(a) 1 Gbps (b) 10 Gbps

(c) 20 Gbps (d) 100 Gbps

Answer: (c) — IMT-2020 peak DL 20 Gbps.

7. Which technology can give hard isolation at the transport layer for slices?

(a) FlexE (b) ARP

(c) DHCP (d) STP

Answer: (a) — FlexE channelization.

8. Who informs the UE of the Allowed NSSAI?

(a) AMF (b) UPF

(c) gNB (d) HSS

Answer: (a) — The AMF, in Registration Accept.

9. How is the suitable SMF for a slice found?

(a) Discovery through the NRF (b) Manually

(c) DNS only (d) ARP

Answer: (a) — NF discovery — NRF.

Chapter 9 — Packet Switching, Call Control and Evolution from Circuit to Packet Core

Packet Switching and Call Control · Evolution to EPC & 5GC

9.1 Packet Switching and Call Control

Call control means controlling the life cycle of a call: *setup → ongoing → release*, together with number analysis, routing, billing and services (call forwarding, waiting). In the old circuit network, call control was in the **MSC** (ISUP signalling), with bearer and signalling bound together. In a packet network, the **IMS** does this job using **SIP**, and the voice packets (RTP) travel separately in the user plane.

> **Softswitch / Decomposition (3GPP R4)**
> The MSC is split into an **MSC Server** (control) and an **MGW** (Media Gateway — bearer/transcoding). Between MSC-S and MGW: **H.248/MEGACO**; between MSC-S ↔ MSC-S: **BICC/SIP-I**. This paved the way for IMS: control and media are separate.

9.2 Circuit to Packet Core: Evolution

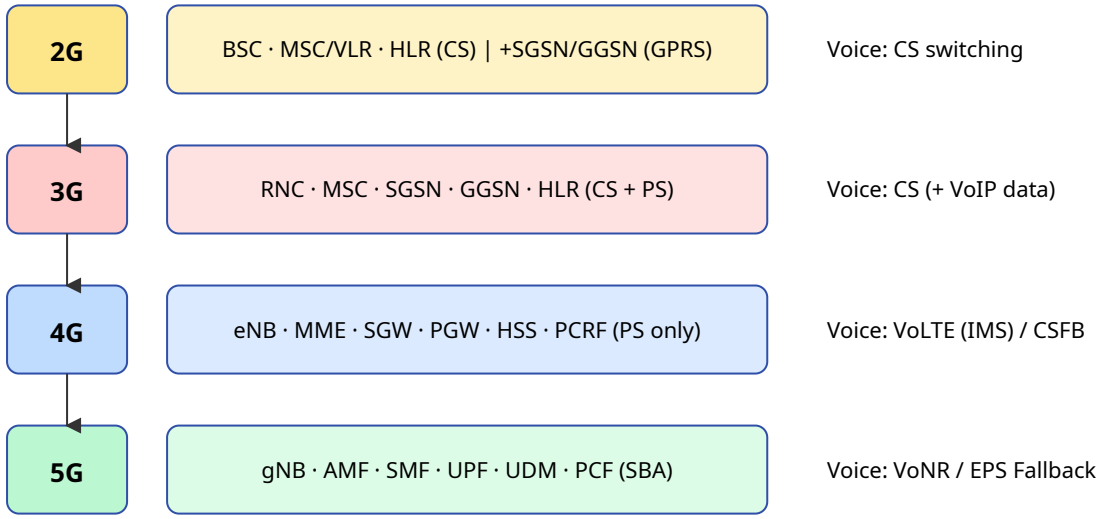


Figure 9.1: Core evolution from 2G to 5G

- **Why evolve?** Data traffic explosion, a single IP network (lower CAPEX/OPEX), lower latency, fewer nodes (flat), voice-data convergence.
- **3G → 4G:** RNC disappears; IMS replaces the MSC; SGSN/GGSN → MME + SGW + PGW; the whole network is IP.
- **4G → 5G:** EPC core functions are broken into microservices; SBA (HTTP/2); CUPS; slicing; cloud-native.

Topic	EPC (4G)	5GC
Architecture	Point-to-point interfaces (S1, S5, S6a…)	Service-Based (Nxxx services, REST)

Signalling protocol	GTP-C, Diameter, S1AP	HTTP/2 + JSON, NGAP, PFCP (N4)
Mobility + session	Together in the MME	AMF (mobility) and SMF (session) separate
QoS model	Bearer-based (QCI)	Flow-based (QFI/5QI)
User ID	IMSI, GUTI	SUPI (concealed: SUCI), 5G-GUTI
Slicing	Limited (DECOR)	Native (S-NSSAI)
Deployment	VNF/VM	CNF/container, cloud-native
Access	3GPP only (LTE)	3GPP + non-3GPP (Wi-Fi, N3IWF)

9.3 How Does Voice Work in 4G?

LTE is PS only, so the core has no CS voice. Solutions:

Method	How	Advantage / Disadvantage
CSFB (CS Fallback)	On an incoming/outgoing call the UE drops to 2G/3G and the call is carried by CS there	More delay (≈ 1–2 s extra setup); LTE data stops or slows down
VoLTE	Voice on LTE itself through IMS (QCI 1 bearer)	HD voice (AMR-WB), fast setup, data at the same time
SRVCC	When LTE coverage ends during a VoLTE call, handover to CS (MSC-S Enhanced)	Call is not dropped
VoNR / EPS Fallback	Direct IMS voice in 5G / if there is no 5G coverage, fall back to LTE	In SA networks the primary method is EPS Fallback

9.4 Evolution of the Signalling Network

- **SS7** (MTP, SCCP, TCAP, ISUP, MAP) → **SIGTRAN** (SS7 over IP: M3UA, SCTP) → **Diameter** (4G) → **HTTP/2 SBI** (5G).
- For routing and load balancing in Diameter: **DRA** (Diameter Routing Agent); in 5G: **SCP** (Service Communication Proxy).
- **SEPP** (Security Edge Protection Proxy) — signalling security between roaming partners in 5G.

Example: Signalling Load Estimate

One MME can process 5000 attach/TAU/service-request per second. In the busy hour, 2 million users, each user averaging 3 signalling events per hour ⇒ total = 6×10^6/hour = 1667/second. Load on one MME ≈ 33%; with N+1 redundancy and 50% maximum utilization, 2 MMEs are enough. (The numbers are only an example — use whatever is given in the question.)

Practice (MCQ)

1. Into which two parts is the MSC split in 3GPP R4?

(a) MSC Server and MGW
(b) MME and SGW
(c) SGSN and GGSN
(d) BSC and RNC

Answer: (a) — Control and bearer separated.

2. Which protocol is used between the MSC Server and the MGW?

(a) SIP
(b) H.248/MEGACO
(c) GTP
(d) BGP

Answer: (b) — Mc interface — H.248.

3. Which node has disappeared in 4G?

(a) BSC
(b) RNC
(c) HLR
(d) MSC

Answer: (b) — RNC (3G) merged into the eNB.

4. What is the main disadvantage of CSFB?

(a) HD voice
(b) Call setup delay increases
(c) Data speed increases
(d) Core cost decreases

Answer: (b) — During the fall to 2G/3G.

5. Which method saves a call when the LTE signal ends during a VoLTE call?

(a) CSFB
(b) SRVCC
(c) CGNAT
(d) SON

Answer: (b) — Single Radio Voice Call Continuity.

6. What is the main signalling protocol in 5GC?

(a) Diameter
(b) HTTP/2 (SBI)
(c) SS7
(d) SIP only

Answer: (b) — SBA = HTTP/2 + JSON.

7. What is the protected form of SUPI in 5G?

(a) GUTI
(b) SUCI
(c) TMSI
(d) MSISDN

Answer: (b) — Subscription Concealed Identifier.

8. Which node is used for Diameter routing?

(a) DRA
(b) SCP
(c) EIR
(d) GMSC

Answer: (a) — SCP in 5G; SEPP for roaming security.

9. In the 5G core, which functions separate mobility and session management?

(a) AMF and SMF
(b) MME and SGW
(c) UDM and AUSF
(d) NRF and NSSF

Answer: (a) — AMF = mobility; SMF = session.

Chapter 10 — Call Flow, Session Management and Mobility Control

10.1 Preparation: Identities and States

Before studying call/session flows, know which ID is used by whom (details in Chapter 12):

ID	Meaning	Used by
IMSI/SUPI	Permanent identity of the SIM	HLR/HSS/UDM
TMSI / GUTI / 5G-GUTI	Temporary identity (keeps IMSI hidden)	VLR, MME, AMF
MSISDN	Phone number	User/billing/routing
IMEI	Device identity	EIR
TAI / LAI	Tracking/Location Area	Paging

Mobility/Connection States

Layer	States	Meaning
RRC (LTE)	IDLE / CONNECTED	Whether an RRC connection exists; in IDLE the UE saves battery and does cell reselection by itself
RRC (NR)	IDLE / **INACTIVE** / CONNECTED	INACTIVE: fast resume, low signalling — new in 5G
NAS (4G)	EMM-DEREGISTERED/REGISTERED; ECM-IDLE/CONNECTED	Whether registered in the network; whether a signalling connection exists
NAS (5G)	RM-DEREGISTERED/REGISTERED; CM-IDLE/CONNECTED	RM = Registration Management, CM = Connection Management

10.2 GSM Mobile Originated Call (MOC)

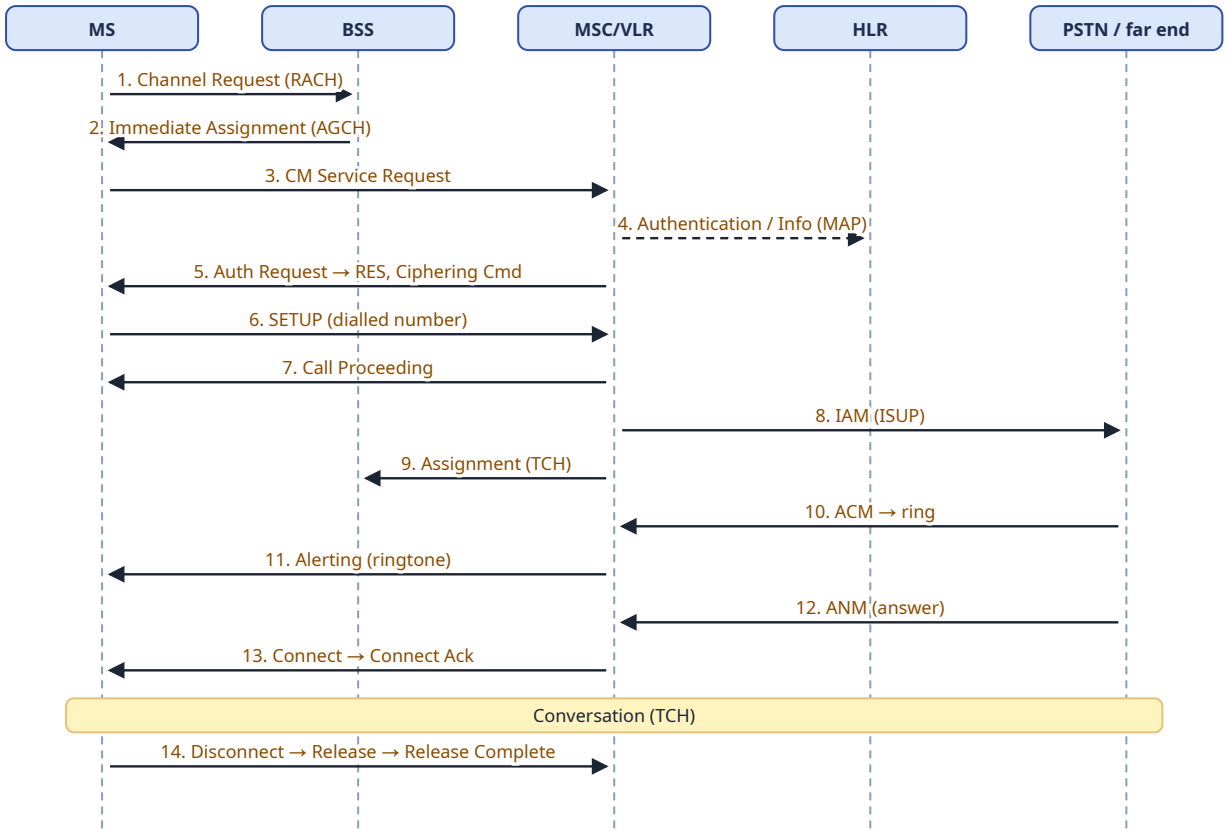


Figure 10.1: GSM MOC call flow (simplified)

Mobile Terminated Call (MTC) — key idea: (1) The calling network reaches the **GMSC**. (2) The GMSC asks the **HLR** (**SRI** — Send Routing Information). (3) The HLR knows which VLR/MSC the MS is in; it sends **PRN** (Provide Roaming Number) to that VLR. (4) The VLR allocates a temporary **MSRN**. (5) The HLR returns the MSRN to the GMSC; the GMSC routes the call to the visited MSC. (6) The MSC **pages** the MS; when the MS answers, the call is set up. *Key idea: ask the HLR "where is the user", then route using the MSRN.*

10.3 LTE Attach Procedure

This happens when the phone is switched on or airplane mode is turned off. The steps are: **RRC connection → NAS Attach → Authentication → Security → Location update (HSS) → Session/bearer creation (SGW/PGW) → IP allocation → Radio bearer setup.**

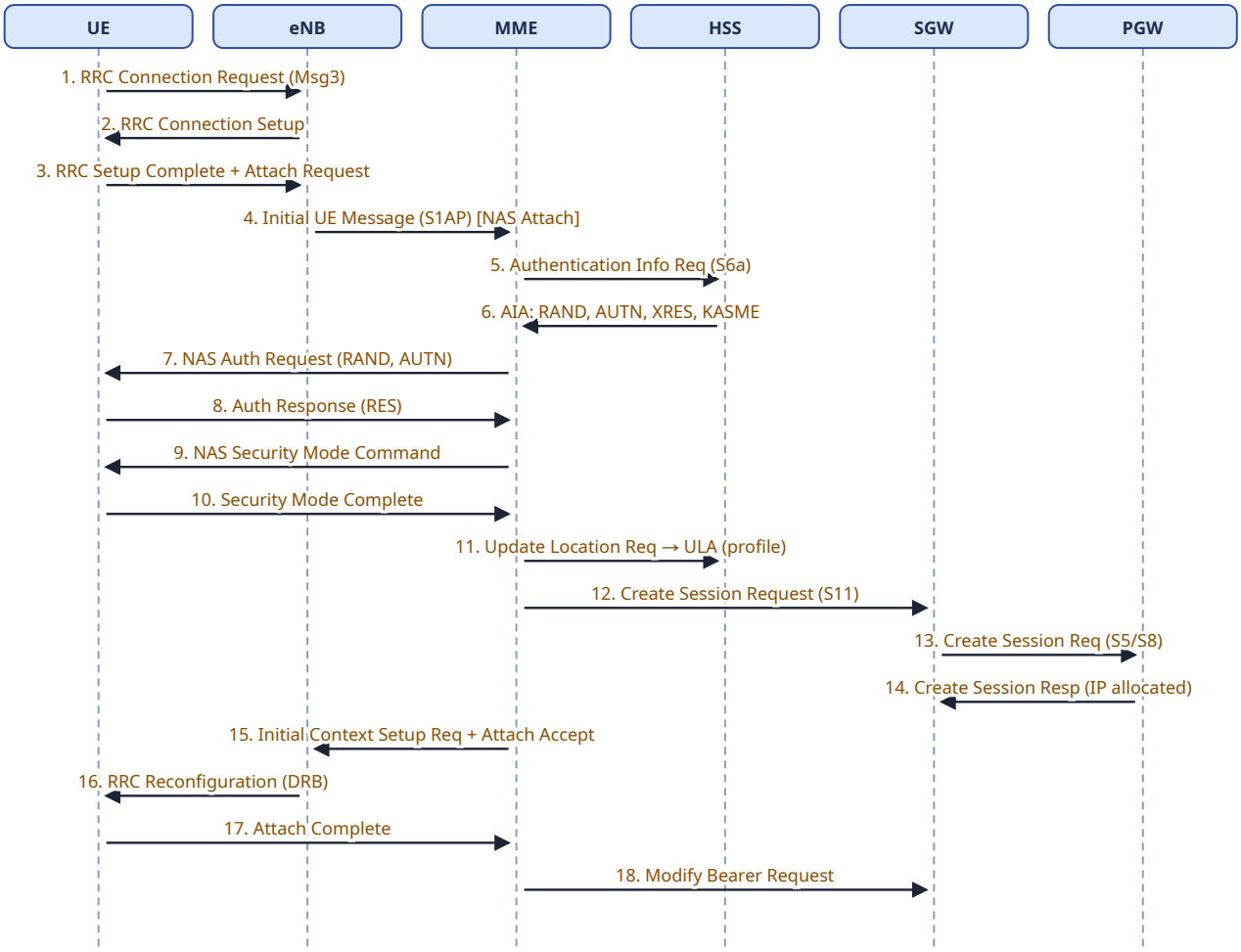


Figure 10.2: LTE Initial Attach (simplified)

Random Access (RACH) — 4 steps: Msg1 (preamble, one of 64) → Msg2 (RAR — timing advance, grant) → Msg3 (RRC Connection Request) → Msg4 (Contention Resolution/RRC Setup).

Timing Advance: TA = 2d / c (In LTE, 1 TA step = 16 T_s ≈ 0.52 μs ≈ 78 m distance)

Example: Round-trip delay

User is 10 km from the cell: one-way delay = 10,000 / (3×10^8) = 33.3 μs; round-trip = **66.7 μs**. In LTE, the maximum cell radius ≈ 100 km (PRACH format 3); in GSM the TA limit is ≈ 35 km.

10.4 5G Registration and PDU Session

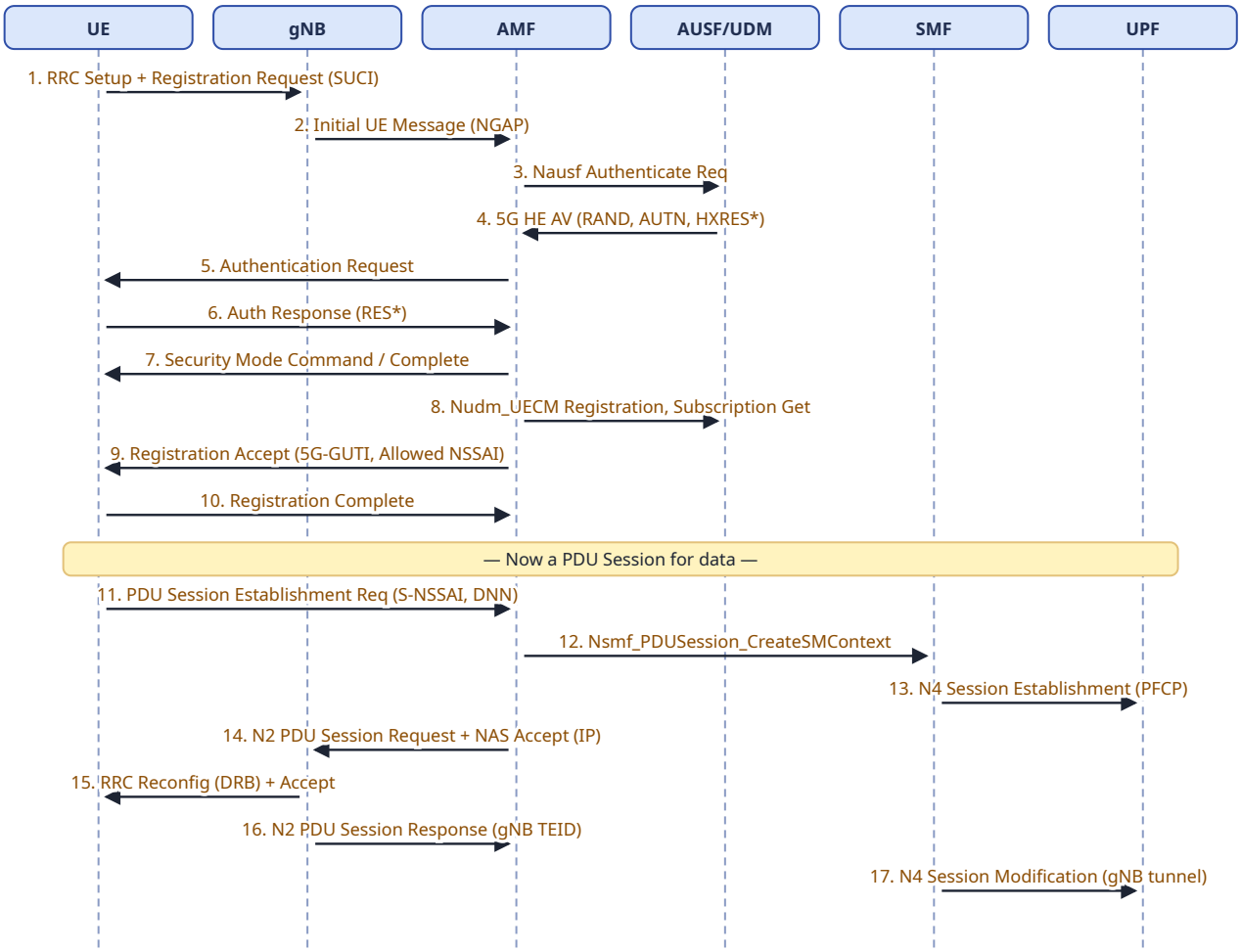


Figure 10.3: 5G Registration and PDU Session Establishment (simplified)

- **Registration** (RM-REGISTERED): the UE is made known to the network; authentication, Allowed NSSAI, 5G-GUTI.
- **PDU Session**: the data pipe — IP address is obtained, UPF is selected, QoS flows. Types: IPv4, IPv6, IPv4v6, Ethernet, Unstructured.
- **SSC mode:** 1 = IP anchor stays fixed; 2 = break-before-make; 3 = make-before-break.

10.5 Idle Mobility: Cell Reselection, TAU, Paging

- **Cell reselection** — the UE itself picks a better cell using radio measurements (RSRP/RSRQ) with priority and hysteresis.
- **TAU (Tracking Area Update)** — the UE informs the network when it enters a new Tracking Area (or on a periodic timer). In 5G: **Registration Update**.
- **Paging** — the network searches for an IDLE UE; the page is sent in all cells of the whole **TA list**. Large TA ⇒ fewer TAUs but more paging load; small TA ⇒ the opposite. (Trade-off!)

10.6 Connected Mobility: Handover

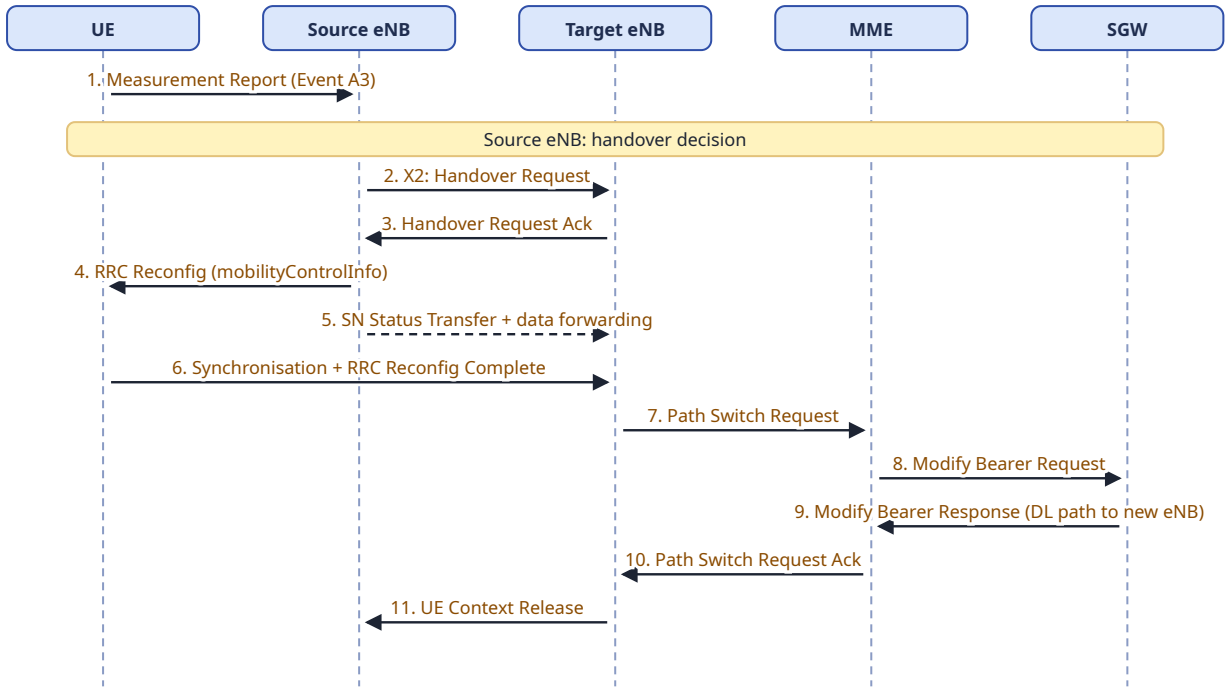


Figure 10.4: LTE X2 handover (simplified)

Event A3 condition

$$M_n + O_{fn} + O_{cn} - Hys \;>\; M_s + O_{fs} + O_{cs} + Off$$

M = RSRP; n = neighbour; s = serving; Hys = hysteresis; Off = offset. The Measurement Report is sent if the condition stays true for the **Time-to-Trigger (TTT)** duration.

Example: Will the A3 event trigger?

M_s = −95 dBm, Hys = 1 dB, Off = 3 dB (O_f, O_c = 0).

(a) M_n = −92: −92 − 1 = −93 > −95 + 3 = −92 ? **No** (−93 > −92 is false).

(b) M_n = −89: −89 − 1 = −90 > −92 ? **Yes** ⇒ report.

That is, the neighbour must be better than the serving cell by more than Off + Hys = 4 dB → fewer ping-pongs.

- **X2 handover:** direct eNB-to-eNB; MME unchanged; Path Switch at the end. **S1 handover:** through the MME when X2 is absent or the MME changes.
- **Data forwarding:** during handover, buffered packets are sent source → target so no data is lost (lossless).
- **Inter-RAT:** LTE ↔ 3G/2G/NR. 5G: **Xn** handover (gNB–gNB) or **N2** (via the AMF).
- **KPI:** HOSR (Handover Success Rate) target ≥ 98–99%; call drops mostly come from bad handovers/interference.

Practice (MCQ)

1. In GSM MTC, whom does the GMSC send SRI to?

(a) VLR
(b) HLR
(c) BSC
(d) EIR

Answer: (b) — HLR → PRN → MSRN.

2. Who allocates the MSRN?

(a) HLR
(b) VLR
(c) GMSC
(d) AuC

Answer: (b) — VLR (on the HLR's PRN request).

3. What is Msg3 in LTE RACH?

(a) Preamble
(b) RAR
(c) RRC Connection Request
(d) Contention Resolution

Answer: (c) — Msg1 preamble, Msg2 RAR, Msg3 RRC Conn Req, Msg4 resolution.

4. In LTE Attach, which node completes the default bearer and IP allocation?

(a) eNB
(b) PGW
(c) HSS
(d) EIR

Answer: (b) — The PGW gives the IP in the Create Session Response.

5. Which message changes the path at the end of an X2 handover?

(a) Path Switch Request
(b) Paging
(c) TAU
(d) Attach

Answer: (a) — eNB → MME → SGW bearer path update.

6. Which RRC state is new in 5G?

(a) RRC_IDLE
(b) RRC_INACTIVE
(c) RRC_CONNECTED
(d) RRC_SLEEP

Answer: (b) — INACTIVE.

7. What usually happens when the TA is made smaller?

(a) TAU decreases, paging increases
(b) TAU increases, paging decreases
(c) Both increase
(d) Nothing

Answer: (b) — Smaller TA → more TAU, fewer paging cells.

8. What does Event A3 indicate?

(a) Serving cell is very good
(b) Neighbour cell is better than serving by an offset
(c) Cell density is high
(d) UE battery is low

Answer: (b) — A3 = neighbour becomes offset better.

9. Who sends the 5G PDU session establishment request (NAS) from the UE?

(a) AMF (N1), which forwards it to the SMF
(b) Directly to the UPF
(c) UDM
(d) NRF

Answer: (a) — The NAS 5GSM message goes via the AMF to the SMF.

10. Round-trip propagation delay for a user 15 km from the cell?

(a) 50 μs
(b) 100 μs
(c) 150 μs
(d) 300 μs

Answer: (b) — $2\times15000/3\times10^{8}$ = 100 μs.

11. What is used to reduce ping-pong handover?

(a) Hysteresis and TTT
(b) More power
(c) FDD
(d) MIMO

Answer: (a) — Hys + Time-to-Trigger.

Chapter 11 — IMS Architecture (Voice and Multimedia Switching)

11.1 What is IMS and Why?

IMS (IP Multimedia Subsystem) is the 3GPP IP-based service platform that delivers **voice, video, messaging and RCS** over one IP core. It is access-independent (LTE, NR, Wi-Fi, fixed). The 4G/5G core only gives a "pipe"; the call logic (who is called, where to route, which service, billing) lives in IMS. Signalling protocol: **SIP** (RFC 3261); media: **RTP/RTCP**; description: **SDP**; AAA: **Diameter**.

11.2 IMS Architecture

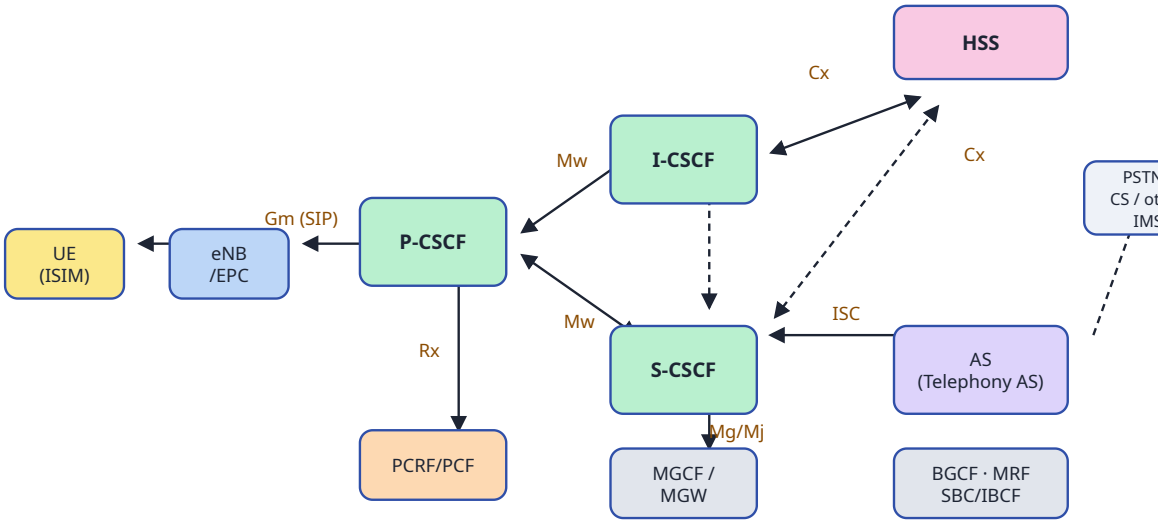


Figure 11.1: IMS architecture (simplified)

Node	Role
P-CSCF (Proxy)	The UE's **first point of contact** (inbound/outbound SIP proxy); IPsec security, SIP compression, emergency call detection; requests QoS (bearer) from the PCRF/PCF over Rx
I-CSCF (Interrogating)	**Entry gate** of the home network; queries the HSS (Cx) to find which S-CSCF; topology hiding
S-CSCF (Serving)	The **brain** of IMS — Registrar + session control; downloads the profile (iFC) from the HSS; triggers the AS (ISC); routing
HSS	IMS subscriber data (IMPU, IMPI, iFC), authentication vectors
AS (Application Server)	Service logic: **TAS** (Telephony AS — call forwarding/waiting), SCC AS, RCS AS
MGCF / MGW	IMS ↔ PSTN/CS interworking (SIP ↔ ISUP; RTP ↔ TDM; codec transcoding)
BGCF	Decides where the PSTN breakout happens

MRF	Media resources (conference, announcements, IVR)
SBC / IBCF	Network-edge security, interconnect (operator-to-operator), NAT
ENUM / DNS	Telephone number (E.164) → SIP URI mapping

> **Remember**
>
> **P** = closest to the UE; **I** = door of the home network; **S** = service decisions. Only I and S talk to the HSS (Cx), not P.

IMS Identity

- **IMPI** (Private User Identity) — used for authentication; an NAI such as `user@ims.mnc004.mcc470.3gppnetwork.org`.
- **IMPU** (Public User Identity) — what others dial; `sip:+8801XXXXXXXXX@domain` or `tel:+8801XXXXXXXXX`.
- **ISIM** — the IMS application on the UICC (if absent, a temporary IMSI-based identity is derived from the USIM).
- Domain format: `ims.mnc<MNC>.mcc<MCC>.3gppnetwork.org` (MNC padded to 3 digits; e.g. Teletalk MCC 470 / MNC 04 → mnc004.mcc470).

11.3 SIP Basics

Method	Purpose
REGISTER	Registration
INVITE	Request to start a session
ACK	Confirms the final response
BYE	Ends the session
CANCEL	Cancels a pending INVITE
PRACK	Reliable ACK of a provisional response
UPDATE	Updates session parameters (pre-condition)
OPTIONS / MESSAGE / SUBSCRIBE / NOTIFY / REFER	Capability query / text / event subscription / notification / transfer

Response class	Examples
1xx (provisional)	100 Trying, 180 Ringing, 183 Session Progress
2xx (success)	200 OK
3xx (redirect)	302 Moved Temporarily
4xx (client error)	401 Unauthorized, 404 Not Found, 408 Timeout, 486 Busy Here
5xx (server error)	500 Server Internal Error, 503 Service Unavailable
6xx (global failure)	603 Decline

SDP exchanges media type, codec, port and IP (offer/answer model). **Preconditions**: before ringing, make sure the QoS bearer is ready at both ends — otherwise the voice would be lost even though the phone rings.

11.4 IMS Registration

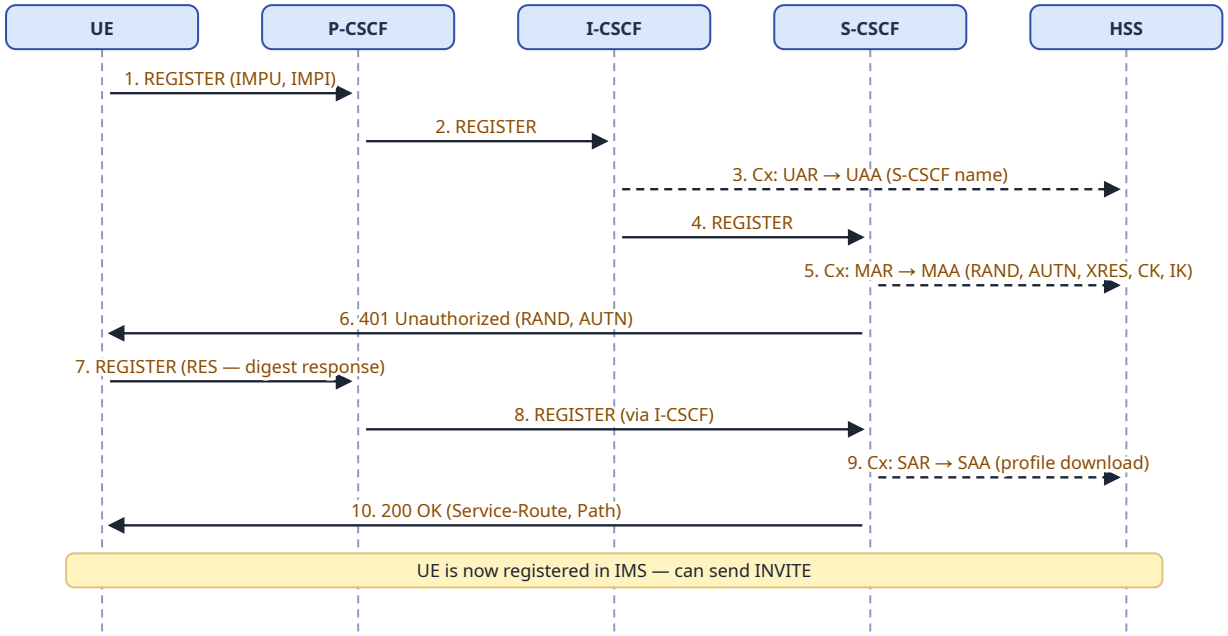


Figure 11.2: IMS registration (IMS-AKA, two-step)

The first REGISTER has no authentication data, so a 401 comes back (with RAND, AUTN). The UE computes RES with the ISIM/USIM and sends the second REGISTER. On success: 200 OK. After that, an **IPsec** SA is established between the UE and the P-CSCF.

11.5 VoLTE Call Flow

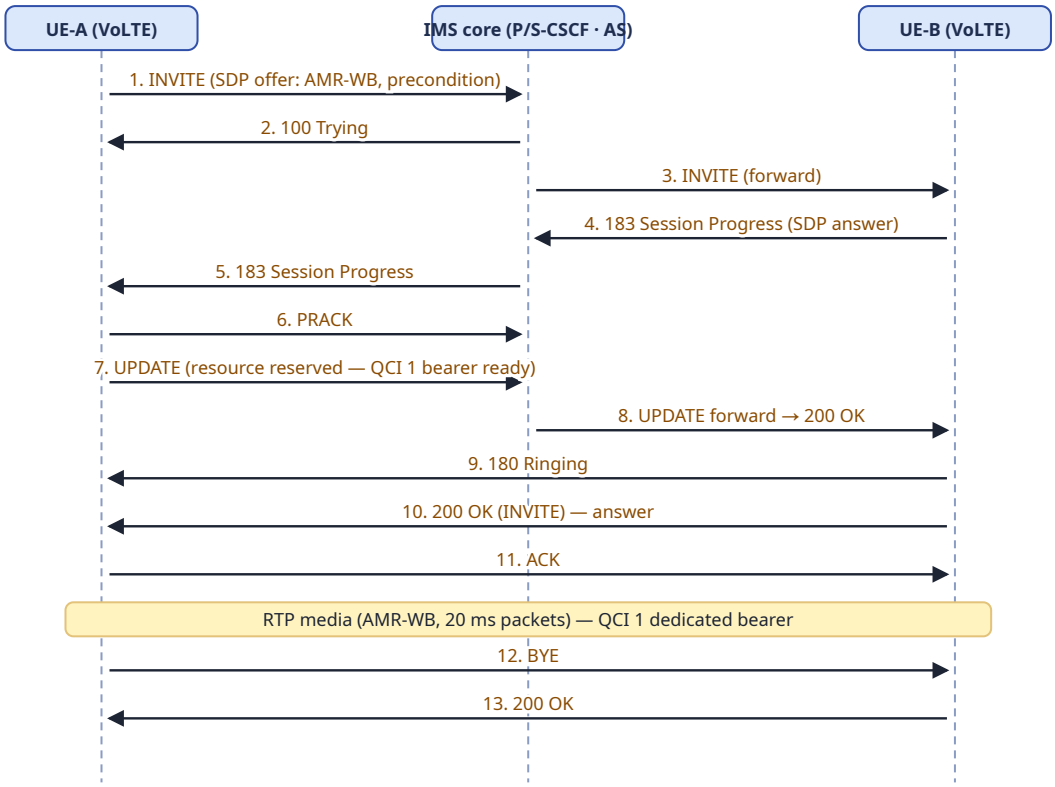


Figure 11.3: VoLTE call setup and release (simplified)

- **Signalling:** QCI 5 bearer (IMS default, non-GBR). **Voice:** QCI 1 dedicated bearer (GBR) — delay ≤ 100 ms, loss ≤ 10^{-2}.
- **Codecs:** AMR-NB (4.75–12.2 kbps, 8 kHz), **AMR-WB** (6.6–23.85 kbps, 16 kHz — HD Voice), **EVS** (5.9–128 kbps, super-wideband; 3GPP R12).
- **ROHC:** compresses the RTP/UDP/IP header (40 bytes for IPv4) to ≈ 2–4 bytes — essential because the voice payload is small.
- **SPS/DRX:** Semi-persistent scheduling and C-DRX — reduce control overhead and battery use. **TTI bundling** improves coverage.

Example: VoLTE bandwidth

AMR-WB 12.65 kbps; one frame every 20 ms ⇒ payload = $12.65\times10^{3} \times 0.02 / 8 \approx$ **31.6 bytes** ≈ **32 bytes**.
Without ROHC: (32 + 40) bytes × 8 / 0.02 s = **28.8 kbps** (55% of it is header overhead!). **With ROHC** (header ≈ 3 bytes): (32+3)×8/0.02 = **14.0 kbps**. This is why VoLTE is spectrally efficient.

11.6 Emergency, SRVCC and Interworking

- **Emergency call (999):** possible even without SIM/registration; the P-CSCF recognises the number and sends it to the E-CSCF/PSAP; location information is included.
- **SRVCC:** when a VoLTE call leaves LTE coverage, eNB → MME → MSC Server Enhanced performs handover to CS; the call stays anchored in IMS (SCC AS), so it does not drop.
- **VoWiFi:** the same IMS over Wi-Fi (via the ePDG); **ViLTE, VoNR, RCS** also run on IMS.

Practice (MCQ)

1. What is the UE's first SIP contact point in IMS?

(a) I-CSCF
(b) S-CSCF
(c) P-CSCF
(d) HSS

Answer: (c) — P-CSCF (Gm interface).

2. Which node downloads the subscriber profile from the HSS and triggers services?

(a) P-CSCF
(b) S-CSCF
(c) MGCF
(d) BGCF

Answer: (b) — S-CSCF (SAR/SAA, iFC).

3. Which is the control node for IMS–PSTN interworking?

(a) MGCF
(b) I-CSCF
(c) SGW
(d) HSS

Answer: (a) — MGCF + MGW.

4. Which QCI is used for VoLTE voice?

(a) 1
(b) 5
(c) 7
(d) 9

Answer: (a) — QCI 1 GBR; signalling uses QCI 5.

5. What is 180 in SIP?

(a) Trying
(b) Ringing
(c) OK
(d) Busy

Answer: (b) — 180 Ringing; 486 Busy Here.

6. What is the response to the first REGISTER in IMS registration?

(a) 200 OK
(b) 401 Unauthorized
(c) 404
(d) 603

Answer: (b) — The IMS-AKA challenge (RAND, AUTN).

7. With which node is the P-CSCF connected through the Rx interface?

(a) PCRF/PCF
(b) HSS
(c) MME
(d) AS

Answer: (a) — QoS/bearer request.

8. AMR-WB 12.65 kbps, 20 ms frame → how many payload bytes?

(a) ≈ 16
(b) ≈ 32
(c) ≈ 64
(d) ≈ 128

Answer: (b) — 12650×0.02/8 = 31.6.

9. Which SIP method ends a session?

(a) BYE
(b) ACK
(c) INVITE
(d) PRACK

Answer: (a) — BYE.

10. What is the purpose of SRVCC?

(a) Keep a VoLTE call continuous in CS when it leaves LTE
(b) Increase data speed
(c) IP allocation
(d) Number portability

Answer: (a) — Single Radio Voice Call Continuity.

11. Which is an example of an IMPU?

(a) sip:+8801xxxxxxxxx@domain
(b) IMSI
(c) IMEI
(d) TEID

Answer: (a) — IMPU = public identity (SIP URI/tel URI).

Chapter 12 — Mobile User Data Management and Authentication

HLR, HSS, UDM and Registry Systems · Authentication

12.1 Subscriber Database: HLR → HSS → UDM

A mobile network must know: **Who are you? Is your SIM genuine? Which services do you get? Where are you now?** This information is kept in a central, permanent database. Its name changes with each generation:

Generation	Name	Protocol	Customer/Service
2G/3G CS	**HLR** (+ **AuC**)	MAP (SS7)	Voice, SMS
4G	**HSS**	Diameter (S6a, Cx)	LTE + IMS (VoLTE)
5G	**UDM** + **UDR** + **AUSF** (+ ARPF)	HTTP/2 (Nudm, Nausf)	5G, slicing, 4G/IMS

What does an HLR/HSS store?

IMSI, MSISDN, subscription profile (APN, QoS, data plan, roaming permission, voice/SMS/VoLTE facility), **current serving node (VLR/MME/AMF address)**, authentication keys (K/OPc, AuC data), IMS data (IMPU/IMPI/iFC), and restrictions (barring). **VLR** = a temporary copy for the visitor's area.

Why centralised? Keeping data in one place makes provisioning simple. But it is also the most sensitive node. So Geo-redundancy (multiple sites), encrypted data, and a separate FE (Front End) / BE (Back End/UDR) architecture (Layered/Cloud-native) are used.

12.2 Identifiers

ID	Structure	Remark
IMSI	**MCC** (3) + **MNC** (2/3) + **MSIN**; maximum 15 digits	Bangladesh MCC = **470**; MNC: GP 01, Robi 02, Banglalink 03, Teletalk 04
MSISDN	CC + NDC + SN; maximum 15 digits	+880 1X XXXXXXXX (Bangladesh CC = 880)
IMEI	15 digits = TAC (8) + SNR (6) + Check digit (1, Luhn)	Shown by dialling *#06#; stolen devices are blocked in the EIR
TMSI / P-TMSI / GUTI	Temporary; allocated by the network	Protects privacy by not sending the IMSI repeatedly over the air
MSRN	Roaming number (given by the VLR, for call routing)	Valid only for a short time
SUPI / SUCI	5G: permanent IMSI-like ID / encrypted form (ECIES)	Stops IMSI-catcher attacks
PLMN ID	MCC + MNC	Identifies the network (e.g. 470-04)

TAI / TAC, Cell ID (ECI/NCI)	PLMN + TAC; PLMN + eNB/gNB ID + cell	Location/paging

Example: IMEI Luhn check digit

First 14 digits of the IMEI: `49015420323751`. From the right, double the first digit (×2), the next ×1, and so on, alternately (×2, ×1, ×2…). If a doubled product has 2 digits, add the two digits (or subtract 9). Add everything to get S. **Check digit = (10 − S mod 10) mod 10.** Here the result is **8** ⇒ IMEI = 490154203237518 ✔ (this is a well-known valid example).

12.3 Authentication — Why and How?

Purpose: (1) the network makes sure the SIM belongs to a valid subscriber; (2) in modern systems the user also makes sure the network is genuine (mutual); (3) the keys for air-interface encryption are produced.

2G (GSM) — One-way

The SIM has **Ki** (128 bit). The network sends a **RAND** (128 bit). Both sides use **A3** to compute **SRES** (32 bit) and **A8** to compute **Kc** (64 bit, the encryption key). The HLR/AuC supplies a **triplet** (RAND, SRES, Kc). Weakness: it verifies only the network user, not the network; a fake base station (IMSI catcher) is possible.

3G/4G — Mutual (UMTS AKA / EPS-AKA)

The SIM and AuC hold **K** (128 bit), (usually **OPc**) and **SQN** (sequence number — stops replay). The AuC builds a **quintet/vector**: **RAND, XRES, CK, IK, AUTN**.

AUTN = (SQN ⊕ AK) || AMF || MAC-A

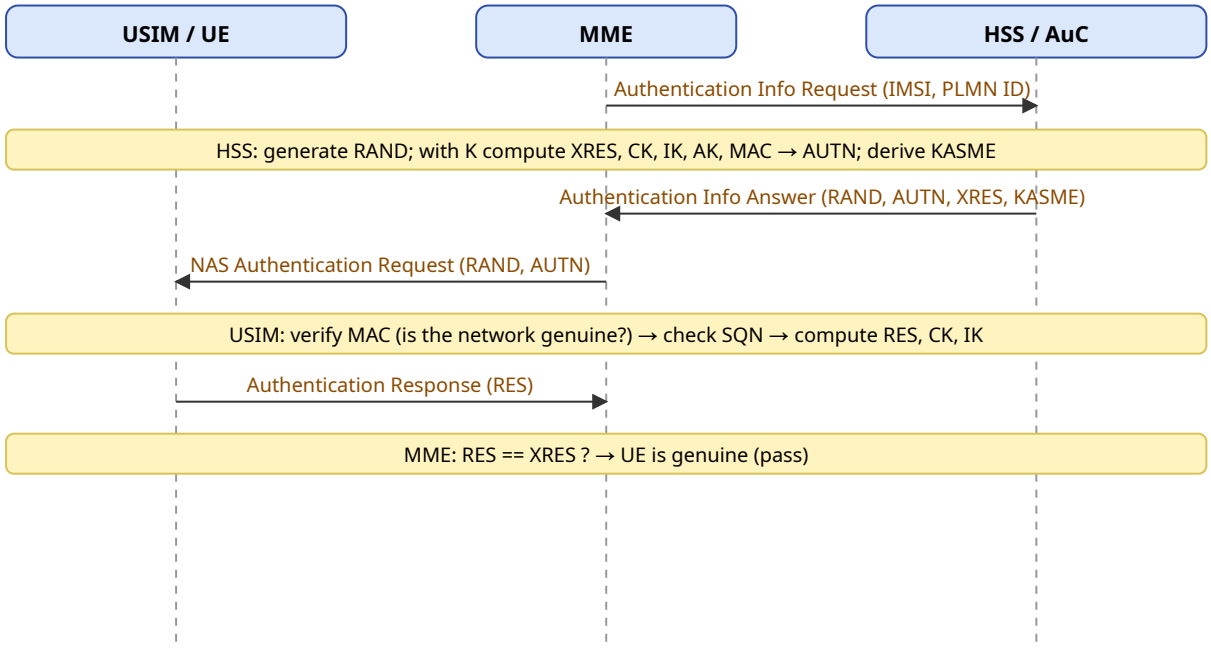


Figure 12.1: 4G AKA authentication

- The USIM checks the **MAC** to verify the network + checks whether SQN is fresh (replay protection). If not matched: Sync Failure/MAC Failure.
- The USIM sends **RES**; the MME compares it with **XRES**. If they match, the UE is authenticated.
- Both sides compute **CK, IK** on their own → **K_{ASME}** → NAS/AS keys (separate for encryption and integrity).

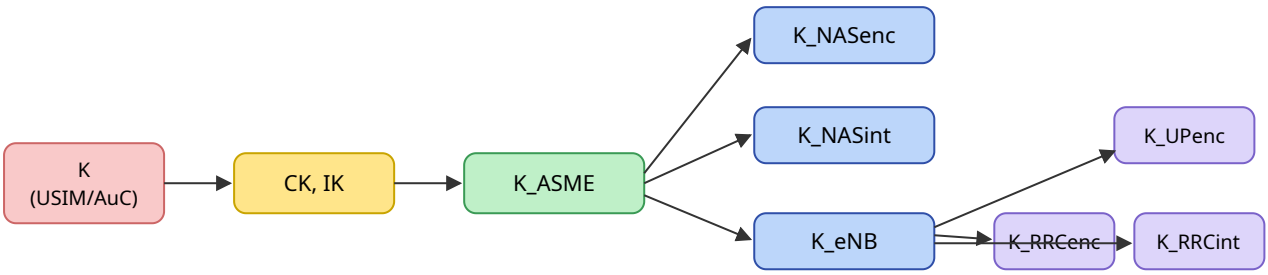


Figure 12.2: 4G key hierarchy

4G key hierarchy: K → (CK, IK) → K_ASME → NAS/AS keys (K_NASenc, K_NASint, K_eNB → K_RRCenc, K_RRCint, K_UPenc). K never leaves the USIM/AuC.

Encryption algorithms (LTE): EEA1 (SNOW 3G), EEA2 (AES), EEA3 (ZUC); integrity EIA1/2/3. 5G also uses NEA/NIA.

Example: How big is the key space?

K = 128 bit ⇒ possible keys = $2^{128} \approx 3.4\times10^{38}$. Even at 10^9 key checks per second it takes ≈ 1.1×10^{22} years — brute force is impossible. The real risk is not in the algorithm but in the protocol and implementation (e.g. SS7 weakness).

5G — 5G-AKA and EAP-AKA'

- The UE does not send **SUPI** directly; it sends **SUCI** (encrypted with ECIES using the home network's public key); the **SIDF** in the UDM decrypts it.
- Nodes: **SEAF** (in the AMF, serving network anchor), **AUSF** (decision in the home network), **UDM/ARPF** (vector generation). Interfaces: N12 (AMF–AUSF), N13 (AUSF–UDM).
- Benefit: **Home network control** — in roaming, the visitor's network cannot decide alone. Key hierarchy: K → CK/IK → K_{AUSF} → K_{SEAF} → K_{AMF} → NAS/gNB keys.

	GSM	UMTS/LTE	5G
Authentication	User→Network	Mutual	Mutual + Home control
User ID over the air	IMSI/TMSI	IMSI/GUTI	**SUCI** (encrypted)
Vector	Triplet	Quintet	5G HE AV
Encryption key	Kc (64)	CK/IK (128)	128/256 bit
Node	HLR/AuC	HSS	UDM/ARPF + AUSF

12.4 Interface Summary

Interface	Connection	Protocol	Function
MAP (C, D, Gr)	MSC/VLR/SGSN – HLR	MAP/SS7	Location, authentication, SRI
S6a	MME – HSS	Diameter	ULR/AIR — location update, authentication data
Cx	I/S-CSCF – HSS	Diameter	IMS registration (UAR/MAR/SAR)
N8	AMF – UDM	HTTP/2	Registration, subscription
N10	SMF – UDM	HTTP/2	Session subscription data
N12	AMF – AUSF	HTTP/2	Authentication
N13	AUSF – UDM	HTTP/2	Fetching vectors
S13	MME – EIR	Diameter	IMEI check

Security trends: SIM-swap fraud (BTRC/operators have made biometric verification mandatory), IMSI catcher, SS7/Diameter attacks (firewall/signalling security), eSIM.

Practice (MCQ)

1. What is the structure of the IMSI?

(a) MCC + MNC + MSIN
(b) CC + NDC + SN
(c) TAC + SNR + CD
(d) PLMN + TAC

Answer: (a) — maximum 15 digits.

2. What is the MCC of Bangladesh?

(a) 404
(b) 470
(c) 460
(d) 410

Answer: (b) — 470; India 404/405, China 460, Pakistan 410.

3. Which interface lies between the MME and HSS in 4G?

(a) S6a
(b) S11
(c) Cx
(d) Gx

Answer: (a) — S6a — Diameter.

4. What does the USIM use in AKA to verify the network?

(a) XRES
(b) MAC (part of AUTN)
(c) TMSI
(d) Kc

Answer: (b) — the MAC in AUTN.

5. Which one stops replay attacks?

(a) SQN
(b) TMSI
(c) APN
(d) TEID

Answer: (a) — Sequence Number.

6. The MME compares the UE's RES with which value to check it?

(a) RAND
(b) XRES
(c) AUTN
(d) KASME

Answer: (b) — RES == XRES.

7. Which ID does the UE send over the air in 5G (instead of SUPI)?

(a) SUCI
(b) MSISDN
(c) IMEI
(d) MSRN

Answer: (a) — Subscription Concealed Identifier.

8. Which is the AMF–AUSF interface in 5G?

(a) N8
(b) N10
(c) N12
(d) N13

Answer: (c) — N12; AUSF–UDM = N13.

9. How many digits does an IMEI have in total, and what is the last digit?

(a) 15, Luhn check digit
(b) 14, serial
(c) 16, TAC
(d) 10, MNC

Answer: (a) — TAC(8)+SNR(6)+CD(1).

10. What is the size of Ki in GSM?

(a) 64 bit
(b) 128 bit
(c) 256 bit
(d) 32 bit

Answer: (b) — 128 bit; Kc = 64 bit, SRES = 32 bit.

11. Which temporary number does the HLR use to route a roaming call?

(a) MSRN
(b) IMEI
(c) ICCID
(d) TAC

Answer: (a) — VLR → HLR → GMSC.

Chapter 13 — Power Systems in Telecom

13.1 Why −48 V DC in Telecom?

If power fails at a telecom site, the network goes down — that means loss of revenue and service. So the power system is **DC-based and battery-backed**. Historical reason: old exchange relays/electronics ran on −48 V; with the battery connected directly to the bus, supply continues **without any switchover delay** (zero-break). Reason for negative polarity: when the positive side is grounded, corrosion/decay (galvanic) is reduced.

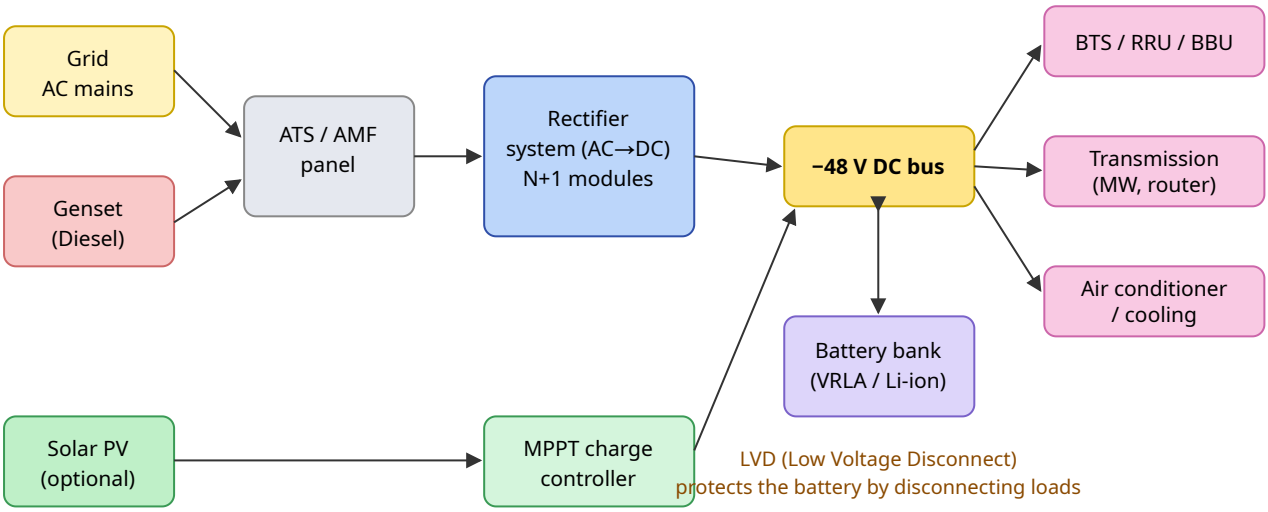


Figure 13.1: Telecom site power system

13.2 Main Components

- **AC input and ATS/AMF:** When the grid fails, the Automatic Transfer Switch / Auto Mains Failure panel starts the genset and moves the load. Bangladesh: 3-phase 400 V (phase-to-neutral 230 V), 50 Hz.
- **Rectifier (SMPS):** AC → −48 V DC (float ≈ 53.5–54.5 V). Modular (hot-swap), efficiency ≈ 95–98%. **N+1** redundancy. Usually also supplies the battery charge current.
- **Battery bank:** 24 cells of 2 V in series = 48 V nominal. Types: **VRLA** (AGM/Gel, maintenance-free, cheap, life 3–5 years, temperature-sensitive), **Lithium-ion ($LiFePO_4$)** (light, long life 8–12 years, higher DoD, costly). Humid heat shortens VRLA life quickly (life ≈ halves for every 10°C rise).
- **Diesel genset:** Used for long load-shedding; ≈ 0.25–0.3 L diesel per kWh.
- **Solar/hybrid:** PV array + MPPT controller; reduces diesel dependency and carbon; essential at off-grid sites.
- **LVD (Low Voltage Disconnect):** Disconnects the load (≈ 43.2 V or 1.8 V/cell) to prevent deep discharge of the battery; cuts non-priority loads first.
- **UPS / Inverter:** For AC loads (core/data centre, computers). An **online double-conversion** UPS suits telecom/servers.

- **Earthing and surge protection:** Lightning rod on the tower; **SPD** (Surge Protection Device) on AC and DC lines; the lower the earth resistance the better (generally ≤ 5 Ω, 1–5 Ω per operator standard); a **single grounding bus** bonding all points (equipotential).
- **Cooling:** AC or free-air cooling in the shelter; heat exchanger in the outdoor cabinet; cooling takes a large share of total power.

Battery	VRLA (Lead-acid)	$LiFePO_4$
Cell voltage	2 V (float ≈ 2.25 V/cell)	3.2 V (15 cells ≈ 48 V)
Usable DoD	≈ 50–80%	≈ 80–100%
Life (cycles)	≈ 300–1000	≈ 3000–6000
Weight/space	Heavy	≈ 1/3 of the weight
Cost	Low (initial)	Higher (but total cost of ownership can be lower)
Temperature sensitivity	High	Low

13.3 Calculations: Load, Battery and Rectifier

$$P = V \times I \;\;|\;\; I_{DC} = P_{load} / V \;\;|\;\; E\,(kWh) = P\,(kW) \times t\,(h)$$

Example: Load current

Site load (DC part of BTS + transmission + cooling) = 1.5 kW, −48 V bus. I = 1500/48 = **31.25 A**.

Battery sizing formula

$$C\,(Ah) = I_{load} \times t_{backup} / (DoD \times \eta_{temp}) \times K_{aging}$$

I = load current, t = backup hours, DoD = allowed depth of discharge (0.8 = 80%), K_{aging} = ageing/design margin (usually 1.2–1.25).

Example: Battery bank — 4 hours backup

I = 30 A, t = 4 h, DoD = 80%, aging factor = 1.25.
Ah = (30 × 4) / 0.8 = 150 Ah; × 1.25 = **187.5 Ah** ⇒ choose a 200 Ah bank in the market (24 cells × 2 V, 48 V).
Usable energy ≈ 48 V × 150 Ah = 7.2 kWh (assuming DoD); load energy = 1.44 kW × 4 = 5.76 kWh.

Example: Rectifier sizing

Load = 30 A; battery charge current = 0.1 C_{10} = 0.1 × 200 = 20 A; total need = **50 A**. If each module is 50 A, 1 is needed; with **N+1** redundancy ⇒ **2 modules** (or 25 A × (2+1)). Module slots are kept free for future expansion (load grows when 5G radio is added).

Example: Battery voltage limits

24 cells: float = 24 × 2.25 = **54 V**; boost = 24 × 2.35 ≈ 56.4 V; end of discharge (EOD) = 24 × 1.75 = **42 V**; LVD ≈ 43.2 V (24 × 1.8).

Example: Solar array sizing

Load = 1.5 kW all day ⇒ daily energy = 1.5 × 24 = 36 kWh. Average peak sun hours in Bangladesh ≈ 4.5 h; system efficiency (derating) 0.75. PV size = 36 / (4.5 × 0.75) = ≈ **10.7 kWp**. (In practice, with a hybrid — grid/genset — only part of the load is covered by solar.)

Example: Genset fuel

Load 1.5 kW, 6 hours load-shedding ⇒ energy = 9 kWh. Fuel rate ≈ 0.28 L/kWh ⇒ ≈ **2.5 L** (in practice more, because of the genset's minimum load factor and low-load efficiency). Running a large genset on a small load is wasteful.

Efficiency and PUE

Rectifier efficiency η = P_{out}/P_{in}; for a 1 kW DC load with η = 96%, AC input = 1/0.96 = 1.042 kW. For a data centre, **PUE** = total facility power / IT power (ideal 1.0; good ≈ 1.2–1.5). At telecom sites, reducing cooling and **direct use** of DC are the main ways to save energy.

13.4 Green Telecom and Modern Trends

- Solar-hybrid sites, Li-ion batteries, server-level power saving (deep sleep mode, traffic-based shutdown), free cooling.
- **Remote monitoring (SNMP/digital FSU):** battery voltage, temperature, genset run hours, fuel level, door open — visible from the NOC.
- **Tower sharing (TowerCo):** several operators use the same tower/power — reduces CAPEX/OPEX.
- **5G and power:** massive MIMO radios use more power (several kW), so a power upgrade is essential.

Safety

DC short-circuit current is dangerous (hundreds of amperes); do not drop tools on battery terminals; use the correct fuse/MCB, insulated tools and PPE. Use a safety harness when working at height (tower).

Practice (MCQ)

1. What is the usual nominal voltage of a DC power system in telecom?

(a) −12 V
(b) −24 V
(c) −48 V
(d) +110 V

Answer: (c) — −48 V DC.

2. What is the total nominal voltage when 24 cells of 2 V are connected in series?

(a) 24 V
(b) 48 V
(c) 12 V
(d) 96 V

Answer: (b) — 24×2 = 48 V.

3. What is the current of a 1.5 kW load on a −48 V bus?

(a) 15.6 A
(b) 31.25 A
(c) 62.5 A
(d) 72 A

Answer: (b) — 1500/48 = 31.25 A.

4. For 30 A, 4 h, DoD 80%, how many Ah are needed (without aging)?

(a) 96
(b) 120
(c) 150
(d) 187.5

Answer: (c) — 120/0.8 = 150 Ah.

5. What does N+1 mean in a rectifier?

(a) N more
(b) 1 extra module beyond the requirement
(c) N years of warranty
(d) One battery

Answer: (b) — supply continues even if one fails.

6. What is the function of the LVD?

(a) Prevent battery overcharge
(b) Cut the load to prevent deep discharge of the battery
(c) Raise the voltage
(d) Start the genset

Answer: (b) — Low Voltage Disconnect.

7. Which battery needs less maintenance and has a long life in telecom?

(a) Flooded lead-acid
(b) $LiFePO_4$
(c) Ni-Cd (old)
(d) None of these

Answer: (b) — Li-ion ($LiFePO_4$) has longer life and higher DoD.

8. What is the usual float voltage of a VRLA cell?

(a) 1.75 V
(b) 2.00 V
(c) 2.25 V
(d) 3.2 V

Answer: (c) — 24 cells ⇒ ≈ 54 V.

9. Which is the most suitable for a "zero-break" supply?

(a) Direct from the genset
(b) DC bus with battery connected
(c) Grid only
(d) Solar only

Answer: (b) — the battery is always connected to the bus.

10. In solar sizing with 36 kWh/day, PSH 4.5 and derating 0.75, what PV size is needed?

(a) 8 kWp
(b) 10.7 kWp
(c) 16 kWp
(d) 24 kWp

Answer: (b) — 36/(4.5×0.75).

11. What is an SPD?

(a) Surge Protection Device
(b) Solar Power Device
(c) Signal Processing Device
(d) Site Power Distribution

Answer: (a) — protection from lightning/surges.

Chapter 14 — Scripting for Simulation, Modelling and Configuration

Scripting for Simulation, Modeling and Configuration of Cellular Systems

14.1 Why Scripting?

A telecom engineer needs scripts for three jobs: **(1) Simulation/modelling** (path loss, SINR, capacity, traffic); **(2) Configuration automation** (the same setting on thousands of routers/base stations; fewer mistakes); **(3) Data analysis** (KPI, logs, CDR). Popular languages: **Python** (most used), **MATLAB** (simulation), **Bash** (Linux/automation), SQL (data), YAML/JSON (config formats).

Job	Tools/Libraries
Numerical computation, plots	NumPy, SciPy, Matplotlib, pandas
Link/system-level simulation	MATLAB (5G/LTE Toolbox), Python **Sionna**, **ns-3**, **OMNeT++**, Vienna Simulator
Open-source 4G/5G testbed	**Open5GS**, **free5GC** (core); **srsRAN**, **OpenAirInterface** (RAN); **UERANSIM** (UE/gNB simulator)
Network device automation	**Netmiko/Paramiko** (SSH), **NETCONF/YANG** (ncclient), **RESTCONF**, **Ansible**, SNMP
Container/cloud	Docker, Kubernetes (kubectl, Helm)
Packet analysis	Wireshark/tshark, scapy

14.2 Example 1: Python — Erlang B, FSPL, Shannon

```
import math

def erlang_b(E, m):
    """Blocking probability, recursive form."""
    b = 1.0
    for k in range(1, m + 1):
        b = E * b / (k + E * b)
    return b

def channels_needed(E, gos):
    m = 1
    while erlang_b(E, m) > gos:
        m += 1
    return m

def fspl_db(d_km, f_mhz):
    return 32.44 + 20 * math.log10(d_km) + 20 * math.log10(f_mhz)

def shannon_mbps(bw_mhz, snr_db):
    return bw_mhz * math.log2(1 + 10 ** (snr_db / 10))

print("Erlang B  E=10, m=15 :", round(erlang_b(10, 15), 4))
print("Channels for E=20, 2%:", channels_needed(20, 0.02))
print("FSPL 2km, 1800MHz    :", round(fspl_db(2, 1800), 2), "dB")
print("Shannon 20MHz, 15dB  :", round(shannon_mbps(20, 15), 1), "Mbps")
```

Output (from running this code)

```
Erlang B  E=10, m=15 : 0.0365
Channels for E=20, 2%: 28
FSPL 2km, 1800MHz    : 103.57 dB
Shannon 20MHz, 15dB  : 100.6 Mbps
```

Explanation: `erlang_b` is exactly the recursion of Chapter 3 (B = E·B/(k+E·B)). `channels_needed` loops to find the smallest m where blocking ≤ GoS. The result matches hand calculation: E = 10, m = 15 ⇒ 3.65%; for 20 Erlang at 2% GoS, 28 channels (in the table 30 channels carry 21.9 E — so 28 channels ≈ 20 E, consistent).

14.3 Example 2: Monte Carlo — SINR Simulation

In a cluster of 7 sites, we find the SINR of users in the centre cell: serving-cell signal ÷ (6 neighbours' interference + noise).

```
import numpy as np
rng = np.random.default_rng(1)           # fixed seed -> reproducible result
f_mhz, tx_dbm = 1800, 43                 # BS transmit power 43 dBm (20 W)

# 7 sites, ISD = 1 km: serving site at the origin + 6 neighbours
isd = 1.0
sites = np.array([(0, 0)] + [(isd*np.cos(np.radians(60*k)),
                              isd*np.sin(np.radians(60*k))) for k in range(6)])

def pl_db(d_km):                         # 3GPP-style urban macro, ~2 GHz
    return 128.1 + 37.6*np.log10(np.maximum(d_km, 0.035))

N = 20000
pts = rng.uniform(-0.5, 0.5, (N, 2))     # users scattered around the centre cell
d = np.linalg.norm(pts[:, None, :] - sites[None, :, :], axis=2)
rx_mw = 10 ** ((tx_dbm - pl_db(d)) / 10)
sinr = rx_mw[:, 0] / (rx_mw[:, 1:].sum(axis=1) + 10 ** (-100/10))   # noise = -100 dBm
sinr_db = 10*np.log10(sinr)
print("median SINR : %.1f dB" % np.median(sinr_db))
print("5th %%-ile   : %.1f dB" % np.percentile(sinr_db, 5))
print("SINR < 0 dB : %.1f %%" % (100*(sinr_db < 0).mean()))
```

Output (seed = 1)

```
median SINR : 4.6 dB
5th %-ile   : -5.8 dB
SINR < 0 dB : 25.3 %
```

Understand: With frequency reuse-1 (all cells on the same frequency), even in the middle of the cell the median SINR is only ≈ 4.6 dB; for a typical user, one in four has SINR below zero — so LTE/5G needs ICIC, beamforming, scheduling and **fractional frequency reuse**. This simulation leaves out shadow fading and antenna patterns — so real values would vary more. (Experiment by changing a parameter: what happens if ISD is 2 km?)

14.4 Configuration and Automation

(a) Open5GS — PLMN config (YAML)

5G core functions are configured in YAML files. Below is an example of a test PLMN (MCC 001 / MNC 01) and one S-NSSAI (to understand the structure):

```
amf:
  sbi:
    server:
      - address: 127.0.0.5
        port: 7777
  ngap:
    server:
      - address: 127.0.0.5
  guami:
    - plmn_id: { mcc: 001, mnc: 01 }
      amf_id: { region: 2, set: 1 }
  tai:
    - plmn_id: { mcc: 001, mnc: 01 }
      tac: 1
  plmn_support:
    - plmn_id: { mcc: 001, mnc: 01 }
      s_nssai:
        - sst: 1        # eMBB slice
```

Explanation: `sbi` = service-based interface (HTTP/2); `ngap` = N2; `guami` = the AMF's global ID; `tai` / `tac` = tracking area; `plmn_support` = which PLMN and slice to serve. In a real network the PLMN would be like 470/04.

(b) Python — Config on multiple devices over SSH (Netmiko, example — not run)

```
from netmiko import ConnectHandler

devices = ["10.0.0.11", "10.0.0.12", "10.0.0.13"]
cmds = ["interface Gi0/0/1", "description Backhaul-to-Core", "mtu 9000"]

for ip in devices:
    conn = ConnectHandler(device_type="cisco_xr", host=ip,
                          username="netops", password="***")
    print(ip, conn.send_config_set(cmds))
    conn.disconnect()
```

(c) NETCONF/YANG and REST — the modern method

- **YANG** = data-model language for config/state; device configuration over **NETCONF** (SSH/830, XML) or **RESTCONF** (HTTPS, JSON) — transactional (commit if all succeed, otherwise rollback).
- The NFs in the 5G core have a **REST API (OpenAPI)**; they can be called directly with Postman/curl/Python requests. In O-RAN, the O1 interface uses NETCONF/YANG.
- **Infrastructure as Code:** Ansible playbook / Helm chart / Terraform — "write what we want, the tool makes it so" (idempotent).

(d) Bash — KPI from logs

```
# count RRC setup failures per hour
grep "RRC_SETUP_FAIL" /var/log/enb.log | awk '{print substr($1,1,13)}' | sort | uniq -c
```

(e) MATLAB — Okumura-Hata path loss

```
f=900; hb=50; hm=1.5; d=5;                % MHz, m, m, km
a  = (1.1*log10(f)-0.7)*hm - (1.56*log10(f)-0.8);
PL = 69.55 + 26.16*log10(f) - 13.82*log10(hb) - a ...
     + (44.9 - 6.55*log10(hb))*log10(d);
fprintf('Path loss = %.1f dB\n', PL)          % -> 146.9 dB
```

Good Scripting Practices

- Version control (Git), parameters in separate files, dry-run/diff first, a rollback plan, no credentials in code (vault/env), logging, keep the **seed fixed** so simulations are reproducible, and roll out step by step (canary) instead of to all devices at once.

Practice (MCQ)

1. In the Python Erlang B recursion, what is B(E,0)?

(a) 0 (b) 1
(c) E (d) ∞

Answer: (b) — B(E,0)=1; then B(E,m) = E·B/(m+E·B).

2. What should be done to make a simulation reproducible?

(a) Keep the random seed fixed (b) A different seed each time
(c) Run the simulation fewer times (d) Only hand calculation

Answer: (a) — e.g. default_rng(1).

3. Which data-model language does NETCONF usually use?

(a) JSON Schema (b) YANG
(c) SQL (d) HTML

Answer: (b) — YANG.

4. What does sst: 1 mean in Open5GS?

(a) URLLC (b) eMBB
(c) V2X (d) MIoT

Answer: (b) — SST 1 = eMBB.

5. Which one is an open-source 5G core?

(a) Open5GS (b) srsUE
(c) Wireshark (d) Sionna

Answer: (a) — Open5GS / free5GC.

6. What is UERANSIM?

(a) A 5G UE and gNB simulator (b) A firewall
(c) A database (d) A router OS

Answer: (a) — for testing the core.

7. What does an idempotent script mean?

(a) Runs only once
(b) Gives the same final state even if run repeatedly
(c) Slow
(d) Encrypted

Answer: (b) — a feature of Ansible.

8. What happens when more samples are taken in a Monte Carlo simulation?

(a) The result becomes more stable
(b) The result becomes random
(c) No change
(d) Less accurate

Answer: (a) — Law of large numbers.

9. What is the correct definition of SINR?

(a) S/(I+N)
(b) S/N
(c) I/S
(d) (S+I)/N

Answer: (a) — Signal / (Interference + Noise).

10. What is the best way to keep credentials in code/config?

(a) Directly in the script
(b) In a vault/env variable
(c) In a comment
(d) In email

Answer: (b) — they must not be hard-coded.

Chapter 15 — Bangladesh Telecom Industry

Basic Knowledge about Telecom Industry of Bangladesh

> **Warning: data may be outdated**
>
> Figures and events change over time (subscriber numbers, 5G coverage, etc.). Before the exam, check the latest numbers on the websites of BTRC (btrc.gov.bd), AMTOB and Teletalk (teletalk.com.bd). Main sources of the facts below: Wikipedia (Telecommunications in Bangladesh; Teletalk) and The Daily Star (1 September 2025).

15.1 Industry Structure

Layer	Who	Remarks
Policy	Posts and Telecommunications Division (under the ICT/Posts and Telecommunications Ministry)	Teletalk is under this division (the circular also says so: "the only state-owned mobile network operator of the country").
Regulator	**BTRC** — Bangladesh Telecommunication Regulatory Commission	Formed under the **Bangladesh Telecommunication Act 2001** (operating from 2002). Oversees licences, spectrum, tariff, QoS, interconnect and numbering.
Mobile operators (MNO)	Grameenphone, Robi, Banglalink, Teletalk	MCC 470; MNC: GP 01 · Robi 02 · Banglalink 03 · Teletalk 04
International	BSCCL (submarine cable), IGW, IIG, ICX	Gateway / interconnect licences.
Transmission / fibre	NTTN operators (e.g. Fiber@Home, Summit Communications), BTCL, Railway, Power Grid, etc.	Fibre backbone; supply "bandwidth" to ISPs.
Tower	Tower companies (TowerCo) — e.g. edotco, Summit Towers	Passive infrastructure sharing.
ISP / broadband	Hundreds of ISPs (home/office internet)	Nationwide, Divisional, Zonal categories.

15.2 Mobile Operator Profiles

Operator	Short profile	MNC / number prefix
Grameenphone (GP)	Started in 1997; the largest operator; main shareholders Telenor (Norway) and Grameen Telecom.	01 / 017, 013
Robi Axiata	Formerly Aktel; owned by Axiata (Malaysia); merged with Airtel Bangladesh in 2016.	02 / 018, (016 — formerly Airtel)

Banglalink	Part of the Orascom/VEON group; became known after acquiring Sheba Telecom in 2005.	03 / 019, 014
Teletalk	**State-owned**; commercial launch on 26 December 2004 (per Wikipedia); first 3G in 2012; 4G (LTE) launched on 16 December 2018.	04 / 015

Teletalk's market share is comparatively small next to the three big private operators. **Challenges:** brand and network-quality perception, limits on spectrum and investment. **Opportunities:** government services (exam application SMS, digital services), coverage in rural and remote areas, education / free Wi-Fi / government projects. Teletalk's spectrum (per Wikipedia): 2G GSM 900; 3G 2100; for 4G a total of 20 MHz (10 MHz at 1800 MHz and 10 MHz at 2100 MHz).

15.3 Technology and Spectrum Timeline

Year	Event
1993	Citycell — first mobile operator (AMPS, later CDMA); shut down around 2016.
1997	Grameenphone and Aktel (Robi) start GSM service.
2001–02	Telecommunication Act 2001; BTRC formed (operating from 2002).
2004	Teletalk launched (26 December 2004).
2006	SEA-ME-WE 4 submarine cable (Cox's Bazar).
2012	Teletalk 3G launched (October 2012); IGW/ICX/IIG licence round.
2013	3G spectrum auction for private operators.
2017	SEA-ME-WE 5 (Kuakata).
2018	4G auction for private operators; Bangabandhu-1 satellite launched (May 2018); Teletalk 4G (December 2018).
2022	**5G spectrum auction (31 March 2022)** — for all mobile operators, about 190 MHz in total.
2025	**Limited 5G launch — 31 August 2025:** Robi first (in specified areas of Dhaka, Chattogram, Sylhet) and Grameenphone (divisional cities); commercial roll-out gradually (The Daily Star).

Bands in use today (broadly): 900/1800 MHz (2G/4G), 2100 MHz (3G/4G), 2300 MHz TDD (4G), 2600 MHz (4G); mid-bands such as 2600/3500 MHz for 5G (see BTRC documents for the bands sold at auction).

15.4 Market and Numbers

- **Mobile connections:** about **181.4 million (18.14 crore)** in September 2022 (Wikipedia, BTRC data); later roughly 180–190 million. Remember: connections (SIMs) ≠ unique users.
- **Internet:** mobile internet is dominant; fixed broadband is comparatively smaller.
- **MFS (Mobile Financial Services):** bKash, Nagad, Rocket and others — USSD/app-based financial services over mobile networks; a big role in the economy.

- **Government initiatives:** Digital Bangladesh (from 2009) → Smart Bangladesh Vision 2041; National Broadband / Info-Sarker, Union Digital Centre.
- **Policy:** National Telecommunication Policy (1998; updated later), ILDTS Policy 2007. (For the exam: National Telecom Policy 1998, Act 2001, BTRC 2002.)

15.5 Regulatory Concepts (may come in the exam)

Concept	Explanation
Licensing	Separate categories: mobile operator, ISP, IGW/IIG/ICX, NTTN, tower, etc.
Spectrum auction	Allocation of limited radio-wave spectrum by auction; fee + percentage revenue roll-out.
MNP	Mobile Number Portability — change operator without changing the number (introduced in Bangladesh in 2018).
SIM registration	Biometric (fingerprint) verification mandatory (from 2015–16); maximum number of SIMs per NID is limited.
QoS monitoring	BTRC measures call drop, throughput and coverage; fines or warnings.
Infrastructure sharing	Sharing of towers, fibre and power — reduces cost.
Emergency	999 (national emergency), 109 (women and children), 16263 (health line).
Data protection / cyber	Digital / cyber security law and its amendments; if asked about the name or section of the old law, check the current status.

15.6 Likely Teletalk-Related Topics

- Fees for government jobs / exam applications are paid via SMS (e.g. in this circular: `TBL <space> User ID` → 16222); exam fee 200 taka + Teletalk service charge 6 taka = 206 taka (circular items 12 and 14(e)).
- Challenges in 5G implementation: fibre backhaul, power, devices, business case, ecosystem; discuss national roaming / sharing.
- A viva question may be: "What are Teletalk's strengths and weaknesses? How would you improve network quality? How can Open RAN / 5G help?" — use Chapters 7, 8 and 13 for the answer.

> **A Good Answer Structure**
>
> (1) Identify the problem → (2) cause (data/KPI) → (3) technical solution (e.g. cell splitting, carrier aggregation, backhaul upgrade, power backup) → (4) how you will measure the result (CSSR, DCR, throughput).

Practice (MCQ)

1. What is the Mobile Country Code (MCC) of Bangladesh?

(a) 470 (b) 404
(c) 410 (d) 460

Answer: (a) — MCC = 470.

2. What is Teletalk's MNC?

(a) 01 (b) 02
(c) 03 (d) 04

Answer: (d) — 470-04.

3. What is GP's MNC?

(a) 01 (b) 02
(c) 03 (d) 04

Answer: (a) — 01; Robi 02; Banglalink 03.

4. Under which law was BTRC formed?

(a) Telecommunication Act 2001 (b) ICT Act 2006
(c) Digital Security Act 2018 (d) Electricity Act 2003

Answer: (a) — Bangladesh Telecommunication Act 2001.

5. When was the 5G spectrum auctioned in Bangladesh?

(a) 2013 (b) 2018
(c) 31 March 2022 (d) 2025

Answer: (c) — 31 March 2022.

6. Who first launched limited 5G (August 2025)?

(a) Robi and Grameenphone (b) Teletalk only
(c) Banglalink and Teletalk (d) None

Answer: (a) — 31 August 2025.

7. What is the country code (CC) of Bangladesh?

(a) +88 (b) +880
(c) +8801 (d) +91

Answer: (b) — +880.

8. Which submarine cable landed at Kuakata?

(a) SEA-ME-WE 4 (b) SEA-ME-WE 5
(c) SEA-ME-WE 3 (d) I-ME-WE

Answer: (b) — SMW-5 at Kuakata; SMW-4 at Cox's Bazar.

9. When did Teletalk launch 4G (LTE)?

(a) 2012 (b) 16 December 2018

(c) 2022 (d) 2025

Answer: (b) — According to Wikipedia.

10. What is the full form of MNP?

(a) Mobile Number Portability (b) Mobile Network Protocol

(c) Multi Node Packet (d) Main Network Port

Answer: (a) — You do not need to change your number.

Chapter 16 — Communication Skills

16.1 What Is Communication?

Communication = delivering information, ideas or feelings from the sender to the receiver so that the receiver understands exactly the same meaning. Sending alone is not enough; the goal is **understanding**. A big part of a technical manager's job is communication: instructing the team, discussing with vendors, reporting to seniors, and explaining customer problems.

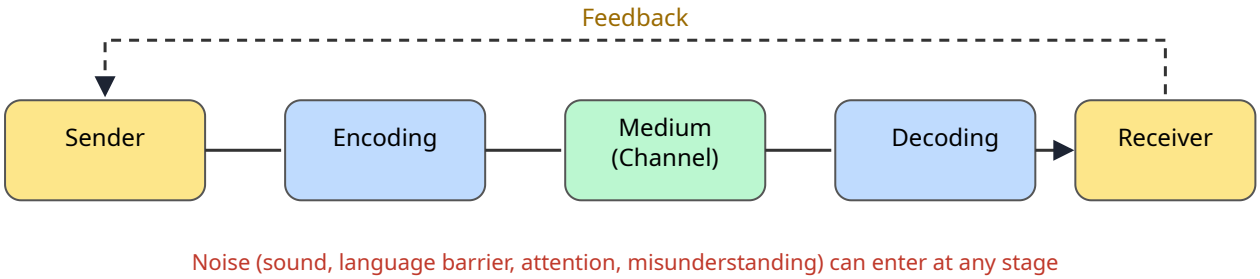


Figure 16.1: The communication process

Types of Communication

Type	Examples	Advantage	Disadvantage
Verbal	Meeting, phone, viva	Fast; instant feedback	No record (unless written down)
Written	Email, report, notice	Record/proof; clarity	Slow; tone is hard to judge
Non-verbal	Body language, eye contact, tone of voice	Shows emotion (50%+ of the message)	Risk of wrong interpretation
Visual	Chart, diagram, slide	Makes complex ideas easy	Takes time to design

By flow: *Downward* (superior → subordinate), *Upward* (subordinate → superior), *Horizontal/Lateral* (same level), *Diagonal* (department to department). **Formal** (organisational channel) and **Informal** (grapevine).

16.2 The 7 Cs of Effective Communication

C	Meaning	Example
Clear	Clear	Say "by 5 pm on Thursday", not "soon"
Concise	Brief	Remove unnecessary words
Concrete	Specific / fact-based	Say "RSRP −110 dBm, 30% drop", not "the signal is bad"
Correct	Error-free (facts and grammar)	Check numbers, names, dates
Coherent	Consistent	Logical flow of ideas

Complete	Complete	Who / what / when / where / why / how
Courteous	Polite	"Please", "thank you"

16.3 Barriers to Communication

- **Language:** jargon / difficult words (a customer does not understand "RRC drop"), unclear language.
- **Physical / environmental:** noise, distance, poor network.
- **Psychological:** bias, emotion (anger), lack of interest, assumptions.
- **Organisational:** too many layers, information filtering, departmental silos.
- **Cultural:** the meaning of body language differs between cultures.

Solutions: simple language, asking for feedback, digital tools (chat/email), active listening, short and specific messages.

16.4 Active Listening

- Give full attention; do not interrupt; eye contact; nod; ask questions to understand; **confirm by summarising in your own words** ("You mean to say ...").

16.5 Written Communication

(a) Structure of a Professional Email

> **Sample**
>
> **Subject:** Request for Approval — BTS Battery Replacement (Dhaka-South Cluster)
>
> Dear Sir,
> Greetings. I am writing to seek your approval for replacing the VRLA battery banks at 12 sites in the Dhaka-South cluster. Test results show that 9 sites provide less than 1.5 hours of backup against the 4-hour design requirement.
> Estimated cost: BDT ... ; Planned completion: 30 days from approval. A detailed list is attached.
> Kindly let me know if you need any additional information.
>
> Best regards,
> Name · Designation · Phone

- **Rules:** clear subject line; salutation; purpose in the first paragraph; data/figures; next step/deadline; polite closing; mention attachments; proofread before sending; be careful with Reply-All.

(b) Official Letter / Notice / Application (Bangla)

- Memo number and date → recipient's designation and address → subject → salutation (Sir / Madam) → main body (background → request) → closing ("Yours faithfully" / "Yours sincerely") → signature, name, designation → copy to (if applicable). (This circular itself is a good example — number, date, subject "Recruitment Notice".)

(c) Writing a Technical Report

Part	What goes in it
Title and summary	Main findings in 1 paragraph (Executive Summary)
Background	Problem / objective
Method	What was measured / tested
Results	Tables, charts, KPIs
Analysis	Causes and impact
Recommendation	Steps, cost, time, risk
Appendix	Data, maps

(d) Good Writing Skills

- Short sentences; active voice ("We have drive-tested", not "Drive test has been done"); numbers and units; **BLUF** (Bottom Line Up Front — conclusion first, explanation later); bullet points; separate levels of detail for different readers.

16.6 Oral Communication and Presentation

- **Presentation structure:** introduction (hook + purpose) → 3 main points → conclusion (summary + action). "Tell them what you'll tell them, tell them, tell them what you told them."
- **Slides:** one idea per slide, little text, large font, diagrams.
- **Voice and body language:** pace and pauses, eye contact, upright posture.
- **Meetings:** agenda first, keep to time, **minutes** and action items at the end (who, what, when).

16.7 Communicating with Customers and the Team

- **Customer complaint:** listen → empathise → apologise/acknowledge → solution or timeline → follow-up (HEAT: Hear, Empathize, Apologize, Take action).
- **Giving bad news:** direct but polite; reason + plan for solution.
- **Conflict resolution:** talk about the problem, not the person; "I" messages ("I feel delivery is delayed" vs "You are late").
- **Feedback:** SBI model — Situation (when/where), Behaviour (what was observed), Impact (the effect).

16.8 Professional Ethics and Teamwork

- Confidentiality (customer data), honesty, punctuality, taking responsibility, admitting mistakes, sharing team success, transparency and accountability in a government organisation.

16.9 Viva Preparation

Question	How to answer (formula)

Tell us about yourself	30–60 seconds: name/degree → technical interest/experience → why Teletalk
Why Teletalk?	National operator, role in the country's digital progress, big potential, chance to learn
Difference between 4G and 5G?	Speed, latency, slicing, SBA core, massive MIMO (Chapters 4, 8)
How will you reduce call drops?	Cause analysis (coverage, interference, handover, backhaul, power), specific action, KPI
How do you handle pressure?	Set priorities, divide duties in the team, communicate, give examples
Weakness?	An honest, real weakness + how you are improving

> **Viva Day**
> The circular asks you to bring to the viva the original certificates, the Applicant Form, the admit card, 1 set of attested photocopies and 2 passport-size photos (circular item 06) — keep your documents organised.

Practice (MCQ)

1. Which element of the communication process verifies that the message was delivered?

(a) Noise (b) Feedback
(c) Channel (d) Encoding

Answer: (b) — Feedback confirms understanding.

2. Which of the 7 Cs means 'brief'?

(a) Concise (b) Concrete
(c) Complete (d) Courteous

Answer: (a) — Concise.

3. Which is non-verbal communication?

(a) Email (b) Body language
(c) Telephone conversation (d) Memo

Answer: (b) — Body language / language of the eyes.

4. What does BLUF mean?

(a) Conclusion first, explanation later (b) Explanation first
(c) Table only (d) Picture first

Answer: (a) — Bottom Line Up Front.

5. What is the grapevine?

(a) Informal communication (b) Formal letter
(c) Report (d) Feedback form

Answer: (a) — Informal communication.

6. Which is NOT part of active listening?

(a) Interrupting others
(b) Confirming by summarising
(c) Eye contact
(d) Asking questions

Answer: (a) — Interrupting is not active listening.

7. Which sentence is the most 'concrete'?

(a) The signal is very bad
(b) Some sites have problems
(c) At Site A, RSRP is −112 dBm and drop rate is 3%
(d) Look into it quickly

Answer: (c) — Numbers and specifics.

8. What should the first paragraph of an email contain?

(a) Purpose
(b) Humour
(c) All the data
(d) Apology

Answer: (a) — Purpose and request come first.

9. Which flow is an instruction from superior to subordinate?

(a) Upward
(b) Downward
(c) Horizontal
(d) Diagonal

Answer: (b) — Downward communication.

10. In the SBI feedback model, what is 'B'?

(a) Benefit
(b) Behaviour
(c) Budget
(d) Boundary

Answer: (b) — Situation–Behaviour–Impact.

Chapter 17 — Aptitude (Maths, Reasoning and Data Interpretation)

Aptitude Related Topic

The aptitude part is the best place to pick up marks in a short time. Below, each topic has formulas, shortcuts and solved examples. Cover each example while practising and solve it yourself.

17.1 Percentage

x% of y = xy/100 | Increase/decrease % = (change / original value) × 100

Example: Successive increase and decrease

Price rises 20%, then falls 20%. Net change? 1.2 × 0.8 = 0.96 ⇒ **4% decrease**. *Shortcut:* +a% and −a% ⇒ net = $-a^2/100$ % = −4%.

Example: Rate of increase

Monthly income rises from 120 to 150: increase = (150−120)/120 × 100 = **25%**.

17.2 Profit, Loss and Discount

Profit % = (SP − CP)/CP × 100 | SP = CP × (1 ± %/100) | Successive discount: $(1-d_1)(1-d_2)$

Example: Profit

CP 800, SP 920 ⇒ profit = 120/800 × 100 = **15%**.

Example: Successive discounts

Price 1000 taka; 20% and 10% off: 1000 × 0.8 × 0.9 = 720 ⇒ single discount = **28%** (20 + 10 − (20×10/100) = 28).

17.3 Ratio and Proportion

Example: Compound ratio

A:B = 2:3 and B:C = 4:5. Make B equal: A:B = 8:12, B:C = 12:15 ⇒ **A:B:C = 8:12:15**.

Example: Division

Divide 3500 taka in the ratio 2:3:5: total parts = 10; one part = 350 ⇒ **700, 1050, 1750**.

17.4 Average

Average = sum of numbers / count

Example: Removing a number

The average of 5 numbers is 20 (sum 100). After removing one number the average becomes 18 (sum of the remaining 4 = 72). Removed number = 100 − 72 = **28**.

17.5 Time and Work, Pipe and Tank

A alone takes a days, B alone takes b days ⇒ together = ab/(a+b) days | daily work = 1/days

Example: Working together

A = 12 days, B = 18 days ⇒ together = (12×18)/(12+18) = 216/30 = **7.2 days**.

Example: Pipe

The inlet fills in 6 hours; the outlet empties in 8 hours. Both open: 1/6 − 1/8 = 1/24 ⇒ **24 hours**.

17.6 Speed, Distance, Time

Speed = distance / time | km/h → m/s: × 5/18 | Average speed over the same distance = 2uv/(u+v)

Example: Average speed

Going 60 km/h, returning 40 km/h (same road) ⇒ average = 2×60×40/(60+40) = **48 km/h** (not 50!).

Example: Train

A 150 m train crosses a pole in 10 seconds ⇒ speed = 15 m/s = 15 × 18/5 = **54 km/h**.

Example: Opposite-direction trains

120 m (36 km/h) and 80 m (54 km/h) moving in opposite directions ⇒ relative speed = 90 km/h = 25 m/s; total length 200 m ⇒ time = 200/25 = **8 seconds**.

17.7 Simple and Compound Interest

SI = P·r·t/100 | $A = P(1 + r/100)^t$ | CI = A − P

Example: Interest

P = 10,000, r = 10%, t = 2 years: SI = **2000**; A = 10000 × 1.1^2 = 12100 ⇒ CI = **2100**. Difference = 100 = $P(r/100)^2$.

17.8 Age and Algebra

Example: Age

Father's age is 3 times the son's; after 12 years it will be 2 times. Son's present age x: 3x + 12 = 2(x + 12) ⇒ **x = 12** (father 36).

Example: Quadratic equation

$x^2 - 5x + 6 = 0 \Rightarrow (x-2)(x-3) = 0 \Rightarrow$ **x = 2, 3**. In general: $ax^2+bx+c=0 \Rightarrow x = (-b \pm \sqrt{(b^2-4ac)}) / 2a$; sum of roots = −b/a, product = c/a.

17.9 Permutation, Combination and Probability

$P(n,r) = n!/(n-r)!$ | $C(n,r) = n!/(r!(n-r)!)$ | Arrangements with repeated letters = $n!/(p!q!r!)$ | Probability = favourable / total

Example: Arrangement of a word

TELETALK has 8 letters; T×2, E×2, L×2 ⇒ 8!/(2!·2!·2!) = 40320/8 = **5040**.

Example: Committee

Choose 3 from 10: C(10,3) = 10×9×8/6 = **120**.

Example: Two dice

Probability that the sum is 7: favourable (1,6), (2,5), (3,4), (4,3), (5,2), (6,1) = 6; total 36 ⇒ **1/6**.

17.10 Geometry and Mensuration

- Pythagoras: $a^2 + b^2 = c^2$ (3-4-5, 5-12-13). Circle: area πr^2, circumference $2\pi r$. Cylinder volume $\pi r^2 h$. Sphere 4/3 πr^3. Triangle ½bh.

Example: Circle

r = 7 cm ⇒ area = (22/7) × 49 = **154 cm^2**; circumference = 2×(22/7)×7 = **88 cm**.

17.11 Number Systems (Special for Engineers)

Decimal	Binary	Hex
10	1010	A

45	101101	2D
255	11111111	FF
100	1100100	64

Conversion: decimal → binary: divide repeatedly by 2, read the remainders from the bottom up. 45 → 45 = 22·2+1; 22 = 11·2+0; 11 = 5·2+1; 5 = 2·2+1; 2 = 1·2+0; 1 = 0·2+1 ⇒ **101101**. Useful in IP subnetting and scripting.

17.12 Series

Series	Rule	Next term
2, 6, 12, 20, 30, ?	n(n+1)	42
3, 6, 12, 24, ?	×2	48
1, 4, 9, 16, 25, ?	Squares	36
2, 3, 5, 7, 11, ?	Primes	13
1, 1, 2, 3, 5, 8, ?	Fibonacci	13

17.13 Data Interpretation

From a table / bar / line chart you must find percentage change, ratio and average. Rules: (1) check the units (thousand/lakh); (2) check the axis start; (3) do approximate calculations first and eliminate options.

Example: Network KPI

Months: Jan 98.2%, Feb 98.6%, Mar 97.8% (CSSR) ⇒ average = (98.2 + 98.6 + 97.8)/3 = 294.6/3 = **98.2%**. Change from Feb to Mar = −0.8 percentage points (relative change ≈ −0.81%) — 'percentage point' and 'percent' are different!

17.14 Logical and Analytical Reasoning

- **Coding-decoding:** CAT → DBU (each letter +1). **Direction:** going 5 km north, 3 km east, 5 km south ⇒ **3 km east** of the start.
- **Rank:** 7th from the top and 18th from the bottom ⇒ total = 7 + 18 − 1 = **24**.
- **Blood relation:** "A is the only sister of B's father" ⇒ A is B's **paternal aunt (Fufu / Pishi)**.
- **Syllogism:** All engineers are intelligent; some intelligent people are honest ⇒ "All engineers are honest" is not certain.
- **Calendar:** 14 October 2026 is a Wednesday ⇒ 16 October 2026 = **Friday**.

> **Time Management**
>
> Spend no more than 45–60 seconds on each aptitude question; if stuck, test the options (back-substitution); if there is negative marking, do not guess — mark only when sure (check the exam instructions for negative marking).

Practice (MCQ)

1. Net change after a 25% price increase followed by a 20% decrease?

(a) 5% increase
(b) 0%
(c) 5% decrease
(d) 4% increase

Answer: (b) — 1.25 × 0.8 = 1.0 ⇒ 0%.

2. Cost price 600, selling price 750 ⇒ profit %?

(a) 20%
(b) 25%
(c) 30%
(d) 15%

Answer: (b) — 150/600 = 25%.

3. Successive discounts of 30% and 20% ⇒ single discount?

(a) 44%
(b) 50%
(c) 40%
(d) 48%

Answer: (a) — 0.7 × 0.8 = 0.56 ⇒ 44%.

4. A:B = 3:4, B:C = 6:7 ⇒ A:B:C?

(a) 9:12:14
(b) 3:4:7
(c) 18:24:28
(d) 9:8:7

Answer: (a) — Take B = 12: A = 9, C = 14.

5. A does a job in 10 days, B in 15 days. In how many days together?

(a) 5
(b) 6
(c) 8
(d) 12.5

Answer: (b) — 150/25 = 6.

6. 20 m/s = how many km/h?

(a) 54
(b) 72
(c) 90
(d) 36

Answer: (b) — 20 × 18/5 = 72.

7. Going at 30 km/h, returning at 60 km/h ⇒ average speed?

(a) 45
(b) 40
(c) 50
(d) 35

Answer: (b) — 2 × 30 × 60/90 = 40.

8. P = 5000, r = 10%, compound interest for 2 years?

(a) 1000 (b) 1050
(c) 1100 (d) 1210

Answer: (b) — 5000 × 1.21 − 5000 = 1050.

9. C(8,2) = ?

(a) 16 (b) 28
(c) 56 (d) 64

Answer: (b) — 8 × 7/2 = 28.

10. In how many ways can the letters of 'LETTER' (L, E, T, T, E, R) be arranged?

(a) 180 (b) 360
(c) 720 (d) 120

Answer: (a) — 6!/(2! · 2!) = 720/4 = 180.

11. 1101_2 (binary) = ? in decimal

(a) 11 (b) 12
(c) 13 (d) 15

Answer: (c) — 8 + 4 + 0 + 1 = 13.

12. Series: 5, 10, 20, 40, ?

(a) 60 (b) 80
(c) 70 (d) 100

Answer: (b) — ×2.

13. 12th from the top, 20th from the bottom ⇒ total students?

(a) 31 (b) 32
(c) 30 (d) 33

Answer: (a) — 12 + 20 − 1 = 31.

14. Roots of $x^2 - 7x + 12 = 0$?

(a) 3, 4 (b) 2, 6
(c) 1, 12 (d) −3, −4

Answer: (a) — (x−3)(x−4) = 0.

Appendix — Formula Summary · Node Comparison · Quick Tables · Model Test

A. All Formulas in One Place

Topic	Formula	Value / Example
dB / dBm	10 log(P2/P1); 10 log(P/1mW)	1 W = 30 dBm; ×2 = +3 dB
Shannon	C = B log2(1+SNR)	20 MHz, 15 dB ⇒ ≈ 100.6 Mbps
Noise floor	−174 + 10 log B + NF (dBm)	20 MHz ⇒ −101 dBm (NF 0)
λ	c / f	1800 MHz ⇒ 16.7 cm
FSPL	32.44 + 20 log d(km) + 20 log f(MHz)	2 km, 1800 MHz ⇒ 103.57 dB
Doppler	f_d = v f / c	100 km/h, 2 GHz ⇒ 185 Hz
PCM	fs = 2 f_max; bit rate = fs × bits	64 kbps; E1 = 2.048 Mbps
Cluster	N = i^2+ij+j^2; D/R = √(3N)	N=7 ⇒ Q=4.58
SIR (6 interferers)	(D/R)^n / 6	N=7, n=4 ⇒ 18.7 dB
Erlang	A = λ h; B(E,m)=E·B(E,m−1)/(m+E·B(E,m−1))	E=10, m=15 ⇒ 3.65%
LTE 20 MHz	1200 SC × 14 × 1000 × bits	64QAM ⇒ 100.8 Mbps/layer
CPRI/antenna	fs·2·15·(16/15)·(10/8)	30.72 MS/s ⇒ 1228.8 Mbps
NR SCS	15·2^μ kHz; slot = 1ms/2^μ	μ=1 ⇒ 30 kHz, 0.5 ms
WCDMA Gp	chip rate / bit rate	3.84M/12.2k ⇒ 25 dB
BDP	BW × RTT	100 Mbps×50 ms ⇒ 625 kB
Availability	Series A1A2; parallel 1−(1−A)^n	2×99.9% ‖ ⇒ 99.9999%
Battery	Ah = I t /(DoD) × K	30 A, 4 h ⇒ 150→188 Ah
VoLTE	payload = rate × 20 ms	12.65 kbps ⇒ 32 B
Fresnel	17.3√(d1d2/(f d))	10 km, 7 GHz ⇒ 10.3 m
Hata (900, 50 m, 5 km)	69.55+26.16 log f −13.82 log hb − a + (44.9−6.55 log hb) log d	≈ 146.9 dB

B. Core Nodes by Generation

Generation	RAN	Control	User plane	Database	Voice
2G	BTS/BSC	MSC/VLR	MSC (CS) / SGSN	HLR/AuC	CS
3G	NodeB/RNC	MSC, SGSN	SGSN/GGSN	HLR	CS

4G	eNB	MME	SGW/PGW	HSS	VoLTE (IMS)
5G	gNB (CU/DU/RU)	AMF/SMF	UPF	UDM/UDR/AUSF	VoNR / EPS-FB

C. Interface Summary (a Favourite for MCQs)

Interface	Connection	Memory trick
S1-MME / S1-U	eNB–MME / eNB–SGW	MME = signalling; U = User data
S11	MME–SGW	—
S5/S8	SGW–PGW	S8 = roaming
S6a	MME–HSS	—
Gx / Rx	PGW–PCRF / P-CSCF–PCRF	Gx = Gateway policy
X2 / Xn	eNB–eNB / gNB–gNB	—
N1/N2/N3	UE–AMF / gNB–AMF / gNB–UPF	N3 = data
N4	SMF–UPF	PFCP
N6	UPF–DN	—
N11	AMF–SMF	—
N12/N13	AMF–AUSF / AUSF–UDM	—
Gm / Mw / ISC / Cx	UE–P-CSCF / CSCF–CSCF / S-CSCF–AS / CSCF–HSS	IMS
F1 / E1 / E2 / A1 / O1 / O2	CU–DU / CU-CP–UP / RIC–CU/DU / Non-RT–Near-RT RIC / SMO–node / SMO–Cloud	O-RAN

D. Abbreviations

Abbr	Full form	Abbr	Full form
AKA	Authentication and Key Agreement	**AMF**	Access & Mobility Mgmt Function
AMR-WB	Adaptive Multi-Rate Wideband	**APN**	Access Point Name
AUSF	Authentication Server Function	**AuC**	Authentication Centre
BBU	Baseband Unit	**BSC**	Base Station Controller
BTS	Base Transceiver Station	**BTRC**	Bangladesh Telecom Regulatory Commission
CDMA	Code Division Multiple Access	**CHF**	Charging Function
CP	Cyclic Prefix	**CPRI**	Common Public Radio Interface
CSCF	Call Session Control Function	**CSFB**	Circuit Switched Fallback
CU/DU/RU	Central/Distributed/Radio Unit	**CUPS**	Control & User Plane Separation
DNN	Data Network Name	**DoD**	Depth of Discharge

eMBB	enhanced Mobile Broadband	**EIR**	Equipment Identity Register
EPC	Evolved Packet Core	**EPS**	Evolved Packet System
FDD/TDD	Frequency/Time Division Duplex	**GGSN**	Gateway GPRS Support Node
GoS	Grade of Service	**GPRS**	General Packet Radio Service
GSM	Global System for Mobile	**GTP**	GPRS Tunnelling Protocol
HLR	Home Location Register	**HSS**	Home Subscriber Server
IMEI	Intl. Mobile Equipment Identity	**IMS**	IP Multimedia Subsystem
IMSI	Intl. Mobile Subscriber Identity	**KPI**	Key Performance Indicator
LTE	Long Term Evolution	**LVD**	Low Voltage Disconnect
MANO	Management & Orchestration	**MGW**	Media Gateway
MIMO	Multiple Input Multiple Output	**MME**	Mobility Management Entity
mMTC	massive Machine Type Comm.	**MSC**	Mobile Switching Centre
MSISDN	Mobile Subscriber ISDN Number	**NAS**	Non-Access Stratum
NFV	Network Function Virtualization	**NGAP**	NG Application Protocol
NR	New Radio	**NRF**	NF Repository Function
NSSAI	Network Slice Selection Assistance Info	**NSSF**	Network Slice Selection Function
OFDMA	Orthogonal Freq. Division Multiple Access	**O-RAN**	Open Radio Access Network
PCRF/PCF	Policy & Charging Rules / Policy Control Function	**PDN**	Packet Data Network
PGW	PDN Gateway	**PLMN**	Public Land Mobile Network
PTP	Precision Time Protocol	**QCI/5QI**	QoS Class Identifier
RAN	Radio Access Network	**RIC**	RAN Intelligent Controller
RRC	Radio Resource Control	**RSRP**	Reference Signal Received Power
SBA	Service-Based Architecture	**SDN**	Software Defined Networking
SGSN	Serving GPRS Support Node	**SGW**	Serving Gateway
SIP	Session Initiation Protocol	**SMF**	Session Management Function
SMO	Service Mgmt & Orchestration	**SRVCC**	Single Radio Voice Call Continuity
SUPI/SUCI	Subscription Permanent/Concealed Identifier	**TAU**	Tracking Area Update
TDMA	Time Division Multiple Access	**TEID**	Tunnel Endpoint Identifier
UDM	Unified Data Management	**UPF**	User Plane Function
URLLC	Ultra-Reliable Low-Latency Comm.	**VLR**	Visitor Location Register
VNF	Virtual Network Function	**VoLTE**	Voice over LTE

VRLA	Valve Regulated Lead Acid	**WCDMA**	Wideband CDMA

E. Last 24 Hours Checklist

- ☐ I can draw the 4G EPC and 5GC diagrams by hand, with interface names
- ☐ I can state the Attach / Registration / VoLTE call steps in order
- ☐ I can explain AKA (RAND, AUTN, RES/XRES, K_{ASME})
- ☐ I can solve dB, FSPL, Shannon, Erlang, SIR and battery Ah problems by plugging into formulas
- ☐ I can explain NFV (MANO), C-RAN vs O-RAN, and slicing (S-NSSAI)
- ☐ Bangladesh: I remember BTRC, operators, MCC/MNC, and the 5G auction/launch year
- ☐ NID original copy, admit card, pen/pencil, calculator (if allowed) are ready; I know the exam centre in advance

Model Test

30 MCQs — attempt in 45 minutes, then check the answers.

> **Rules**
>
> Set a timer (30 questions → 45 minutes). Cover the answers (the answer is given under every question — hide it with paper). 70%+ means good preparation.

Practice (MCQ)

1. Which node usually gives the user an IP address in LTE?

(a) MME (b) SGW
(c) PGW (d) eNB

Answer: (c) — PGW (in 5G: SMF/UPF).

2. Which node is responsible for mobility management in the 5G core?

(a) SMF (b) AMF
(c) UPF (d) NRF

Answer: (b) — AMF.

3. Which interface connects SMF and UPF?

(a) N2 (b) N3
(c) N4 (d) N6

Answer: (c) — N4 (PFCP).

4. Which node triggers services in IMS?

(a) P-CSCF (b) I-CSCF
(c) S-CSCF (d) MGCF

Answer: (c) — S-CSCF (iFC → AS).

5. What is the QCI of the VoLTE voice bearer?

(a) 1 (b) 5
(c) 8 (d) 9

Answer: (a) — QCI 1.

6. What is the maximum number of digits in an IMSI?

(a) 10 (b) 12
(c) 15 (d) 16

Answer: (c) — 15.

7. What is Teletalk's MCC-MNC?

(a) 470-01 (b) 470-02
(c) 470-03 (d) 470-04

Answer: (d) — 470-04.

8. How many dBm is 1 W?

(a) 10 (b) 20
(c) 30 (d) 33

Answer: (c) — 30 dBm.

9. If N = 7, what is D/R?

(a) 3.0 (b) 4.58
(c) 5.2 (d) 7.0

Answer: (b) — $\sqrt{21}$.

10. For E = 10 Erlang and m = 15 channels, the Erlang B blocking is about?

(a) 0.4% (b) 3.65%
(c) 10% (d) 25%

Answer: (b) — by recursion: 0.0365.

11. How many RBs are there in LTE 20 MHz?

(a) 50 (b) 75
(c) 100 (d) 200

Answer: (c) — 100 RB.

12. What is the slot duration for 5G NR with 30 kHz SCS?

(a) 1 ms (b) 0.5 ms
(c) 0.25 ms (d) 0.125 ms

Answer: (b) — $\mu=1$.

13. What is the CPRI rate for LTE with 1 antenna, 20 MHz?

(a) 614.4 Mbps (b) 1228.8 Mbps
(c) 2457.6 Mbps (d) 9.8 Gbps

Answer: (b) — $30.72M\times2\times15\times16/15\times10/8$.

14. What is the loop time of the Near-RT RIC in O-RAN?

(a) <1 ms (b) 10 ms–1 s
(c) One minute (d) An hour

Answer: (b) — xApps.

15. Which technology separates functions from hardware?

(a) SDN (b) NFV
(c) CDMA (d) SDH

Answer: (b) — NFV.

16. Which element manages the VNF lifecycle in NFV?

(a) NFVO
(b) VNFM
(c) VIM
(d) NFVI

Answer: (b) — VNFM.

17. In S-NSSAI, what is SST = 2?

(a) eMBB
(b) URLLC
(c) MIoT
(d) V2X

Answer: (b) — URLLC.

18. What is the target density of mMTC?

(a) $10^3/km^2$
(b) $10^4/km^2$
(c) $10^6/km^2$
(d) $10^8/km^2$

Answer: (c) — 1 million.

19. Which message changes the path at the end of an LTE X2 handover?

(a) Path Switch Request
(b) Paging
(c) Attach
(d) RACH Msg1

Answer: (a) — eNB → MME.

20. In GSM MTC, who allocates the MSRN?

(a) HLR
(b) VLR
(c) BSC
(d) GMSC

Answer: (b) — VLR.

21. In authentication, what does the MME compare RES with?

(a) RAND
(b) XRES
(c) AUTN
(d) KASME

Answer: (b) — XRES.

22. In 5G, what is sent over the air instead of SUPI?

(a) SUCI
(b) GUTI
(c) IMEI
(d) MSRN

Answer: (a) — SUCI.

23. What is the current for a 1.5 kW load on a −48 V bus?

(a) 15 A
(b) 31.25 A
(c) 48 A
(d) 72 A

Answer: (b) — 1500/48.

24. What is the float voltage of a 24-cell VRLA battery (approx.)?

(a) 48 V
(b) 52 V
(c) 54 V
(d) 58 V

Answer: (c) — 24×2.25 = 54 V.

25. What is '180' in SIP?

(a) Trying
(b) Ringing
(c) OK
(d) Busy Here

Answer: (b) — Ringing.

26. Under which law is BTRC established?

(a) Telecommunication Act 2001
(b) ICT Act 2006
(c) Electricity Act
(d) Companies Act 1994

Answer: (a) — 2001.

27. When was 5G auctioned in Bangladesh?

(a) 2018
(b) 31 March 2022
(c) 2025
(d) Not yet

Answer: (b) — 2022.

28. What is the net result of a 20% increase and a 20% decrease?

(a) 0%
(b) 4% decrease
(c) 4% increase
(d) 20% decrease

Answer: (b) — 1.2×0.8 = 0.96.

29. A can do a job in 12 days and B in 18 days. How long working together?

(a) 6
(b) 7.2
(c) 8
(d) 10

Answer: (b) — 216/30.

30. In how many ways can the letters of TELETALK be arranged?

(a) 5040
(b) 40320
(c) 2520
(d) 10080

Answer: (a) — 8!/(2!2!2!) = 5040.