Basics of Wireless Networking

Energy and Power

Energy

The ability to do work

Energy can be kinetic (movement) or potential (stored)

Power

Energy transfer per second

Transfer can be kinetic (motion) or potential (moving stored energy)

Units

Power is measured in Watts

Energy is measured in Joules = Watts × seconds

1 kW-hour = 1000 Watts × 3600 seconds/hour
= 3.6×10^6 Joules

Electricity and Magnetism

A charged object may create

Electric field $\mathbf{E}$

Magnetic field $\mathbf{B}$

Radiation (transfer of power) from a charged object

Power $\propto \mathbf{E} \times \mathbf{B}$

Motionless charge does not radiate

$\mathbf{E} = -\dfrac{\text{charge}}{R^2}$, at distance R

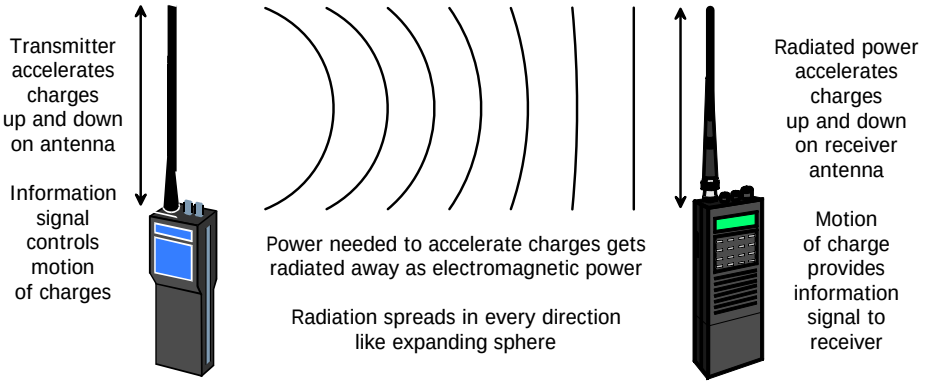
$\mathbf{B} = 0$

Antenna accelerates charges = electric current

Accelerated charges induce fields $\mathbf{E} \neq 0$ and $\mathbf{B} \neq 0$

Antenna radiates power as electromagnetic waves

Radio Communication



Moving electric charge is called electric current

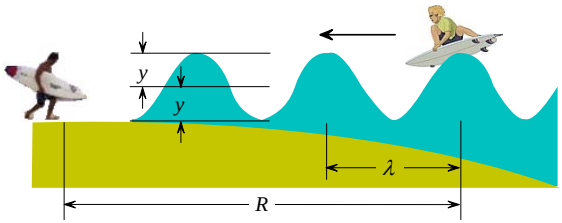
Current depends on time ⇒ charges must accelerate

Electromagnetic radiation satisfies wave equation

Radiated power depends on time t and distance R from antenna

Wave Motion

Ocean waves rolling onto a beach



Wave height has peaks and troughs

y = height of peak above center = depth of trough below center

At fixed distance from shore, wave rises and falls over time

T = time between two wave peaks (period)

$f = 1/T$ = number of wave peaks per second (frequency)

At fixed time, multiple wave peaks at various distances

λ = distance between two wave peaks (wavelength)

Surfer rides peak of wave

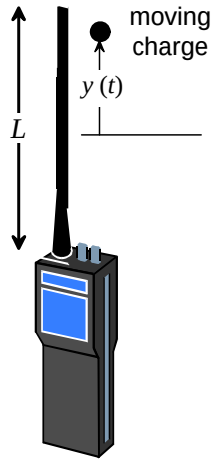
Peak depends on distance and time $\Rightarrow$ peak moves over time

Speed of moving peak = $f \times \lambda$

Charge Moving on Antenna

Charge on antenna accelerated up and down

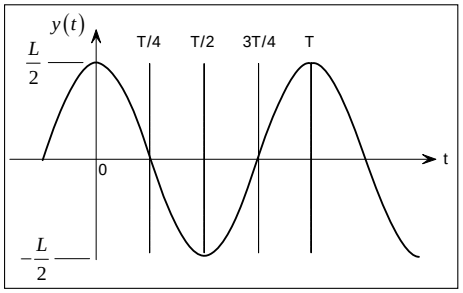
Oscillates top to bottom (distance L) every T seconds



Frequency $f = 1/T$ oscillation cycles per second

$y(t)$ = position of charge on antenna at time t

$$y(t) = \frac{L}{2}\cos\left(2\pi\frac{t}{T}\right) = \frac{L}{2}\cos(2\pi ft)$$



Field is Solution to Maxwell Equations

Radiation fields

$$\mathbf{E}(R,t) = \frac{\mathbf{E}_0\cos\left[2\pi f\left(R/c - t\right)\right]}{R} \qquad \mathbf{B}(R,t) = \frac{\mathbf{B}_0\cos\left[2\pi f\left(R/c - t\right)\right]}{R}$$

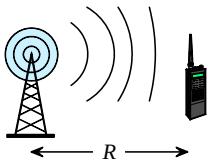
R = distance from antenna to point of measurement

t = time (measured on some clock)

f = frequency = $1/T$

$\mathbf{E}_0, \mathbf{B}_0$ are physical constants

c = speed of light

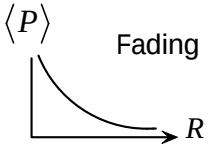


Radiated power

$$\mathbf{P} = \mathbf{E}\times\mathbf{B} = \frac{\mathbf{E}_0\times\mathbf{B}_0}{R^2}\cos^2\left[2\pi f\left(R/c - t\right)\right]$$

Average power

$$\langle P\rangle = \frac{1}{T}\int_0^T |P(t)|\,dt = \frac{|\mathbf{E}_0\times\mathbf{B}_0|}{2}\frac{1}{R^2}$$



Wavelength

Define electromagnetic wavelength

$$\lambda = cT = c/f \qquad \Rightarrow \qquad \lambda f = c$$

Radiation field

$$\mathbf{E}(R,t) = \frac{\mathbf{E}_0\cos\left[2\pi f\left(R/c - t\right)\right]}{R} = \frac{\mathbf{E}_0\cos\left[2\pi\left(\frac{fR}{c} - ft\right)\right]}{R} = \frac{\mathbf{E}_0\cos\left[2\pi\left(\frac{R}{\lambda} - \frac{t}{T}\right)\right]}{R}$$

Wave peaks

$$\cos\left[2\pi\left(\frac{R}{\lambda} - \frac{t}{T}\right)\right] = 1 \Rightarrow \left(\frac{R}{\lambda} - \frac{t}{T}\right) = 0,1,2,\ldots$$

$$\left(\frac{R}{\lambda} - \frac{t}{T}\right) = 0 \rightarrow \left(\frac{R+\Delta R}{\lambda} - \frac{t+\Delta t}{T}\right) = 0 \Rightarrow \left(\frac{\Delta R}{\lambda} - \frac{\Delta t}{T}\right) = 0$$

Speed

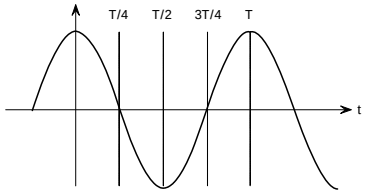
$$v = \frac{\Delta R}{\Delta t} = \frac{\lambda}{T} = \lambda f = c$$

Wave peaks travel at speed of light

Spherical Waves in Space and Time

At fixed distance wave rises and falls over time

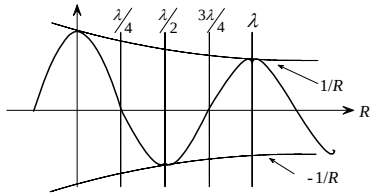
$$\mathbf{E}(R_{const},t)=\frac{\mathbf{E}_0}{R_{const}}\cos\left[2\pi\left(\frac{R_{const}}{\lambda}-\frac{t}{T}\right)\right]$$
$$=C_1\times\cos(2\pi ft-C_2)$$



At fixed time, multiple wave peaks at various distances

Wave peaks decrease at larger distances from source

$$\mathbf{E}(R,t_{const})=\frac{\mathbf{E}_0}{R}\cos\left[2\pi\left(\frac{R}{\lambda}-\frac{t_{const}}{T}\right)\right]$$
$$=\frac{C_1}{R}\cos\left[2\pi\left(\frac{R}{\lambda}-C_2\right)\right]$$



Electromagnetic Spectrum

Radio antennas are effective in the frequency range

from ~ 30 kHz (λ = 10 km)
to ~ 300 GHz (λ = 1 mm)

Chemical reactions generate higher frequencies:

Infra-Red (IR)
Visible Light
Ultra-Violet (UV)
X-rays (Roentgen)

Nuclear reactions generate gamma rays (γ)

Electromagnetic Spectrum

Wavelength (m)	10^4	10^2	10^0	10^{-2}	10^{-4}	10^{-6}	10^{-8}	10^{-10}	10^{-12}	10^{-14}	10^{-16}
Frequency (Hz)	10^4	10^6	10^8	10^{10}	10^{12}	10^{14}	10^{16}	10^{18}	10^{20}	10^{22}	10^{24}
	radio		microwave		IR	visible	UV	X-ray		gamma	

$\lambda f = c = 3\times10^{10}$ cm/s

1 MHz ~ 300 m
100 MHz ~ 3 m
10 GHz ~ 3 cm

VLF	< 30 kHz
LF	30 - 300 kHz
MF	300 kHz - 3 MHz
HF	3 - 30 MHz
VHF	30 - 300 MHz
UHF	300 MHz - 3 GHz
SHF	3 - 30 GHz
EHF	> 30 GHz

Example

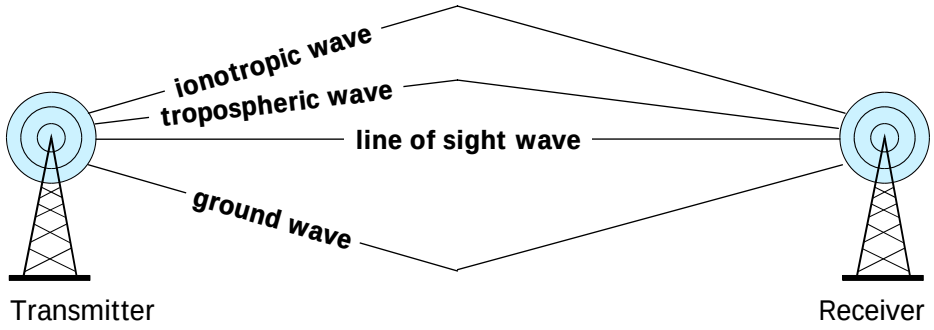
Line antenna most efficient when L = λ / 2
GSM cellphones operate at f ~ 1 GHz
λ = (3×10¹⁰ cm/sec)/(10⁹ Hz) = 30 cm ⇒ L ~ 15 cm = phone size

Radio Wave Propagation

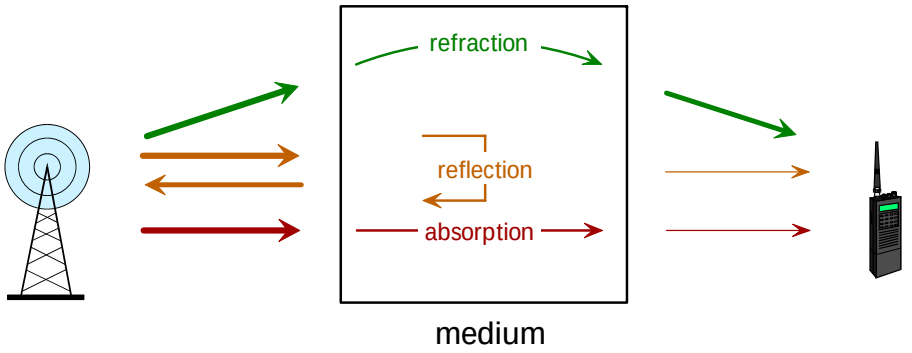
Transmitter generates radio waves

Waves propagate (spread out) through space

Part of radiated power may be obstructed
Part of radiated power is detected by receiver



Interference with Radio Signals



Multipath Fading

Obstacles reflect radio waves

Receiver gets signals from multiple paths

Time-to-arrive depends on path taken by signal

Receiver gets signals transmitted at different times

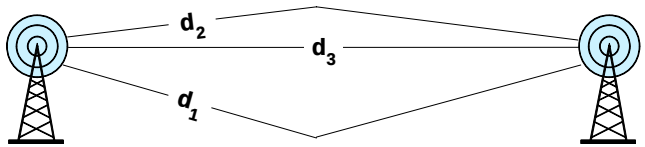
Example

Three signals sent at times $t_1 < t_2 < t_3$

Antenna receives all three signals at time t

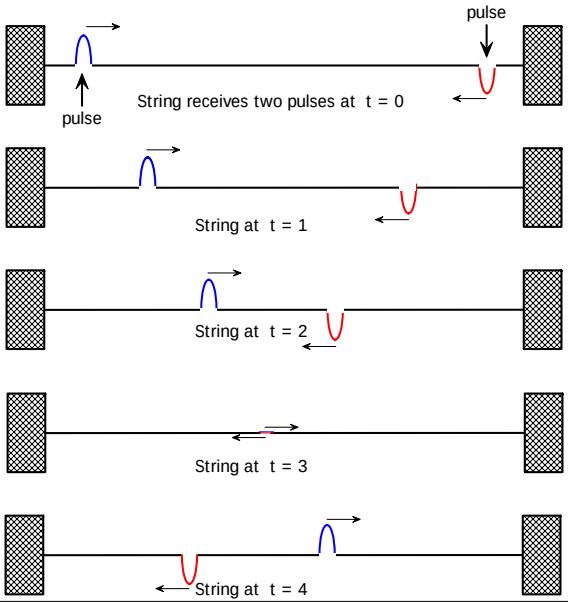
- Signal 1 — sent first and followed longest path d_1
- Signal 2 — sent second and followed second longest path $d_2 < d_1$
- Signal 3 — sent last and followed shortest path $d_3 < d_2$

Sum of waves can cancel out signals



Cancellation of Signals in Wave Motion

Wave amplitudes combine by adding



Wave Interference

Two waves arrive at antenna by slightly different paths

$$\mathbf{E} = \mathbf{E}(R,t) + \mathbf{E}(R+\Delta R, t+\Delta t)$$

where $\Delta R << R$ and $\Delta t << t$

$$\mathbf{E} = \frac{\mathbf{E}_0}{R}\cos\left[2\pi\left(\frac{R}{\lambda} - ft\right)\right] + \frac{\mathbf{E}_0}{R+\Delta R}\cos\left[2\pi\left(\frac{R+\Delta R}{\lambda} - f(t+\Delta t)\right)\right]$$

$$\mathbf{E} = \frac{\mathbf{E}_0}{R}\cos\left[2\pi\left(\frac{R}{\lambda} - ft\right)\right] + \frac{\mathbf{E}_0}{R\left(1+\frac{\Delta R}{R}\right)}\cos\left[2\pi\left(\frac{R}{\lambda} + \frac{\Delta R}{\lambda} - ft - f\Delta t\right)\right]$$

Ignoring $\frac{\Delta R}{R} << 1$

$$\mathbf{E} \approx \frac{\mathbf{E}_0}{R}\left\{\cos\left[2\pi\left(\frac{R}{\lambda} - ft\right)\right] + \cos\left[2\pi\left(\frac{R}{\lambda} - ft\right) + 2\pi\left(\frac{\Delta R}{\lambda} - f\Delta t\right)\right]\right\}$$

Wave Interference

$$\mathbf{E} \approx \frac{\mathbf{E}_0}{R}\left\{\cos\left[2\pi\left(\frac{R}{\lambda} - ft\right)\right] + \cos\left[2\pi\left(\frac{R}{\lambda} - ft\right) + 2\pi\left(\frac{\Delta R}{\lambda} - f\Delta t\right)\right]\right\}$$

Using identity $\cos(A) + \cos(B) = 2\cos\frac{1}{2}(A+B) \times \cos\frac{1}{2}(A-B)$

$$\mathbf{E} = \frac{\mathbf{E}_0}{R}\left\{2\cos\left[2\pi\left(\frac{R}{\lambda} - ft\right)\right] \times \cos\left[\pi\left(\frac{\Delta R}{\lambda} - f\Delta t\right)\right]\right\}$$

Transparent medium

$$\Delta R = c\Delta t \quad \Rightarrow \quad \frac{\Delta R}{\lambda} - f\Delta t = \Delta t\left(\frac{c}{\lambda} - f\right) = \frac{\Delta t}{\lambda}(c - \lambda f) = 0$$

$$\cos\left[\pi\left(\frac{\Delta R}{\lambda} - f\Delta t\right)\right] = 1$$

Total cancellation

$$\frac{\Delta R}{\lambda} - f\Delta t = \frac{1}{2} \quad \Rightarrow \quad \cos\left[\pi\left(\frac{\Delta R}{\lambda} - f\Delta t\right)\right] = \cos\left(\frac{\pi}{2}\right) = 0$$

Wireless Local Area Networks

IEEE 802.11 Protocol Layers

Physical Layer Convergence Sublayer

- Specifies header for PHY Dependent Sublayer
  - Direct Sequence Spread Spectrum (DSSS)
  - Frequency Hopping Spread Spectrum (FHSS)
- Transmission type
- Modulation scheme
- Data transmission rates

MAC layer

- Medium access
- Addressing
- Procedures

Wi-Fi
Trademark of Wi-Fi Alliance trade association

Data Link Layer	LLC	802.2	LLC frame for SEQ/ACK/Control
	Bridging		Exchange of 802.2 PDUs
	MAC	802.11	CSMA/CA, MACA, CFP
Physical Layer	Convergence		PHY-Dependent Convergence Sublayer
	PHY		FHSS, DSSS, IR, Data rates

WiFi Ad Hoc Mode

Independent Basic Service Set (IBSS)

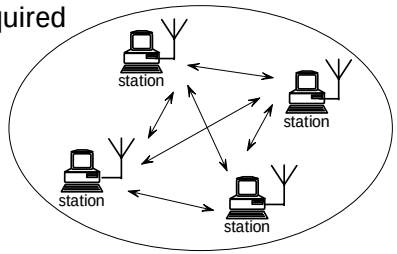
- Any set of 802.11 STAs (wireless stations)
- All STAs transmit / receive on same frequency
- Peer-to-peer service
- No connection to a wired network

Simple unmediated communication

- STAs communicate directly with one another
- Useful for quick set up
- Authentication or Registration not required

Multiple IBSSs are independent

- No bridging
- No hand-off



Independent Basic Service Set

WiFi Infrastructure Mode

Basic Service Set (BSS)

A set of wireless end stations (STA)

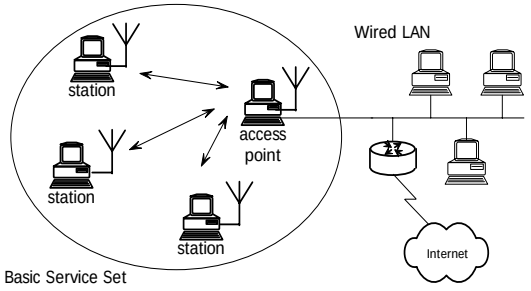
An Access Point (AP)

- Connected to the wired network infrastructure
- Acts as base station for the wireless network
- All traffic flows through AP by Contention or Polling (CFP)

Stations must Associate with AP

Authentication

Registration



WiFi Extended Infrastructure Mode

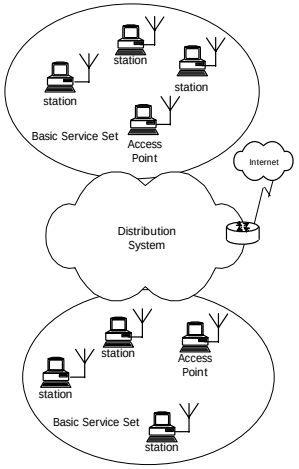
Extended Service Set (ESS)

Two or more BSSs

- Form single subnetwork (broadcast domain)
- Looks like one large BSS to LLC layer
- One Access Point (AP) in each BSS

BSSs connected via Distribution System (DS)

- DS is backbone network
- DS performs MAC-level transport of MAC SDUs
- DS implementation not specified in 802.11



Portal

Software gateway function in AP

Bridges BSS to any non-802.11 DS protocol

DS services permit handoff

Station moving from one BSS to another

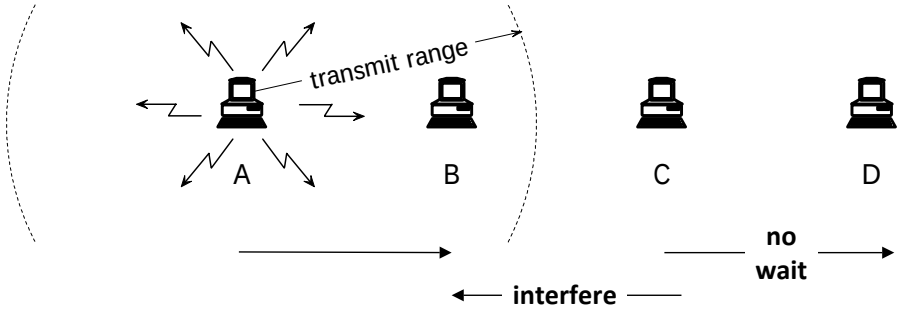
Requires coordination between APs

Hidden Node Problem

A transmits to B

C cannot receive from A — out of range

C transmits — corrupts transmission from A to B

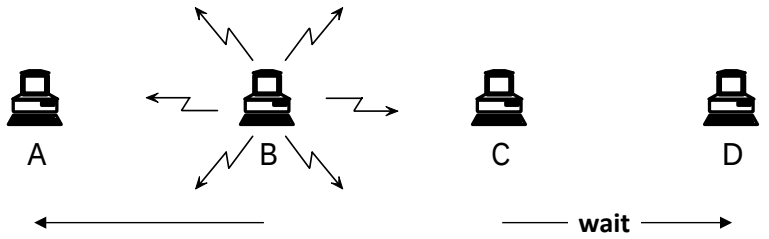


Exposed Node Problem

B transmits to A

C receives transmission from B — delays transmission to D

Inefficient — C transmission to D will not interfere with B to A



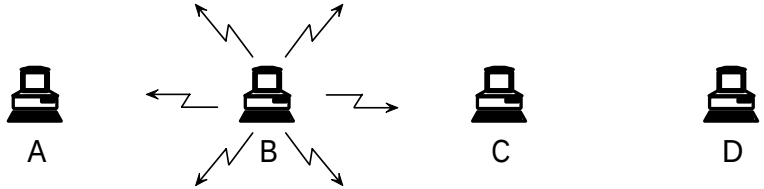
CSMA with Collision Avoidance (CSMA/CA)

Carrier Sense Multiple Access (CSMA)

- Stations listen for transmissions
- Do not transmit if carrier is detected
- Collision detection not possible
  - Hidden node problem
  - Antenna cannot receive while transmitter active

Collision Avoidance (CA)

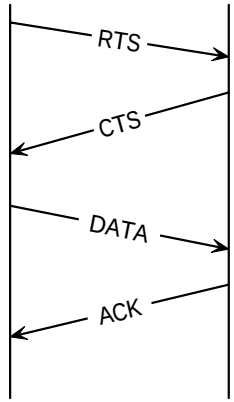
- Non-persistent access
- Random backoff



Multiple Access with Collision Avoidance (MACA)

Channel set-up before data transmission

- RTS — Request To Send
- CTS — Clear To Send
- ACK — Acknowledge error-free transmission



Net Allocation Vector (NAV)

- Transmitted in RTS
- Echoed in CTS
- Predicted data transmission time

Trade-off

- Adds overhead
- Better throughput in hidden and exposed Nodes

Multiple Access with Collision Avoidance (MACA)

C sends 30-byte RTS to D

- Includes NAV for data transmission
- B and D hear RTS

D responds with CTS to C

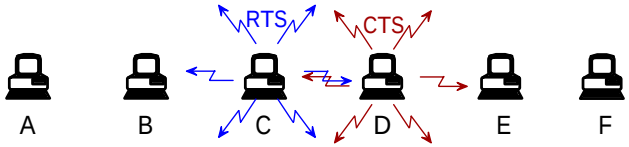
- Echoes NAV
- C and E hear CTS

B hears RTS but not CTS

- B can transmit to A — no interference with C to D

E hears CTS but not RTS

- E waits data transmit time before transmission to F



MAC Sublayer Frame Structure

Frame Control	Control flags
Duration/ID	Timing control
Addresses	Various MAC entities
Sequence Control	Sequence/Fragment number for error/flow control
Frame Body	0 or more data bytes (SDU)

Frame Control	Duration/ ID	Address 1	Address 2	Address 3	Sequence Control	Address 4	Frame Body	FCS
2 bytes	2 bytes	6 bytes	6 bytes	6 bytes	2 bytes	6 bytes	0-2312 bytes	4 bytes

Frame Control

Type and Subtype	Data, Control, Management with subtypes	
To DS/From DS	Access Point (AP) is destination/source	
More Fragments	Part of fragmented LLC packet	
Retry	Indicates re-transmission of bad packet	
Power Management	STA alerts AP of its mode	
	Value of 1	STA will be in power-save mode
	Value of 0	STA will be in active mode
More Data	AP alerts STA (in power-save mode) of buffered frames	
WEP	Indicates WEP encrypted data	
Order	Indicates Strictly Ordered service class	

Protocol Version	Type	Subtype	To DS	From DS	More Fragments	Retry	Power Management	More data	WEP	Order
2 bits	2 bits	4 bits	1 bit	1 bit	1 bit	1 bit	1 bit	1 bit	1 bit	1 bit

MAC Layer Address Fields

4 Address Fields

5 possible MAC entities:

BSS Identification Number (BSSID)

Source Address (SA)

Station that initiated the message

Destination Address (DA)

Final destination for the message

Transmitting Station Address (TA)

Source station for the message on this hop

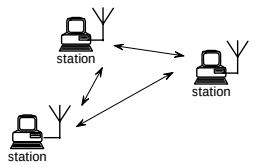
Receiving Station Address (RA)

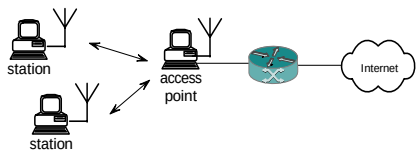
Destination station for the message on this hop

Address Field Definitions

To DS	From DS	Address 1	Address 2	Address 3	Address 4
0	0	DA	SA	BSSID	—
0	1	DA	BSSID	SA	—
1	0	BSSID	SA	DA	—
1	1	RA	TA	DA	SA

Address 1	Immediate destination address
Address 2	Immediate source address
Address 3	Final destination or source when DS performs distribution
Address 4	Source address for DS to DS messages (802.11 is also DS)





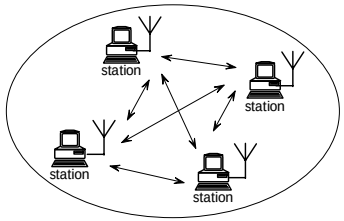
Addressing in an IBSS

To DS	From DS	Address 1	Address 2	Address 3
0	0	DA	SA	BSSID

Independent Basic Service Set (IBSS)

No Access Point (AP) and no DS

Fields To DS and From DS are 0



Independent Basic Service Set

Address 1	Immediate destination address (DA)
Address 2	Immediate source address (SA)
Address 3	BSSID Identifies Ad Hoc network Prevents message from reaching outside IBSS

Data Addressing in a BSS

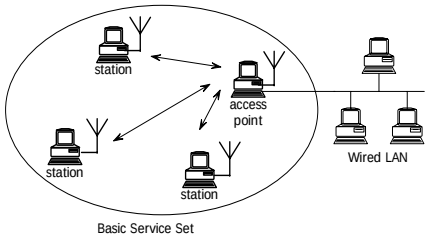
To DS	From DS	Address 1	Address 2	Address 3
0	1	DA	BSSID	SA
1	0	BSSID	SA	DA

Basic Service Set (BSS)

All transmissions are sent To/From Access Point

To/From DS actually means To/From AP

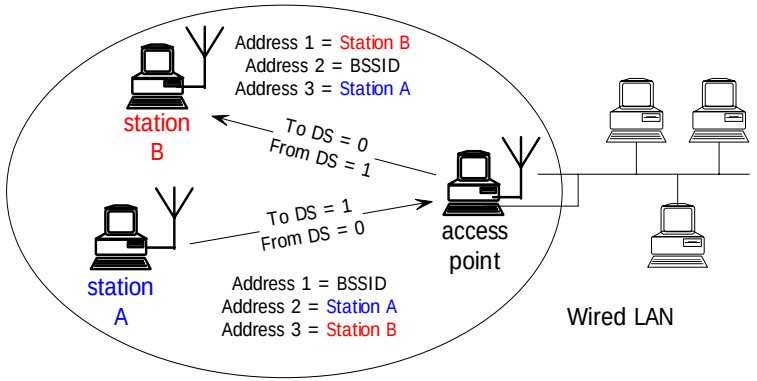
Address 1	Immediate destination address (DA)
Address 2	Immediate source address (SA)
Address 3	Final Destination or Source



BSS Addressing Example

To DS	From DS	Address 1	Address 2	Address 3
0	1	DA	BSSID	SA
1	0	BSSID	SA	DA

Station A sends message to Station B via AP (BSSID)



Control and Management Addressing in a BSS

To DS	From DS	Address 1	Address 2	Address 3
0	0	DA	SA	BSSID

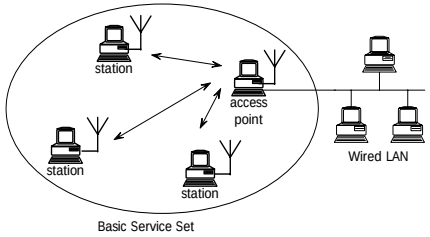
Control and Management messages in a BSS:

Only involve stations in the BSS and the AP

Are sent with To DS = From DS = 0

Either the Source or the Destination will be the AP (BSSID)

Address 3 in included as an error check



Addressing in an ESS

To DS	From DS	Address 1	Address 2	Address 3
0	1	DA	BSSID	SA
1	0	BSSID	SA	DA

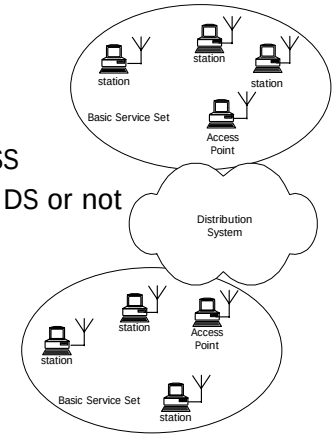
Extended Service Set (ESS)

All transmissions are sent via an AP

To the stations, entire ESS looks like one BSS

Stations do not know if message passes via DS or not

Address 1	Immediate destination address (DA)
Address 2	Immediate source address (SA)
Address 3	Final Destination or Source



ESS Addressing Example

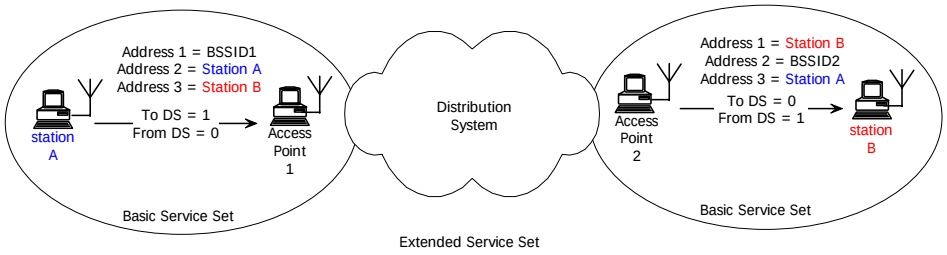
To DS	From DS	Address 1	Address 2	Address 3
0	1	DA	BSSID	SA
1	0	BSSID	SA	DA

Station A sends message to Station B via

AP1 (BSSID1) → DS → AP2 (BSSID2)

DS must forward Data, Sequence, SA, and DA

By some legal means



Mobility Management in Wireless Systems

Registration

Performed when mobile station (MS) activated in Service Area

Authentication

WiFi — managed by access point (AP)

2G / 3G Cellular

- Home Location Register (HLR)
  - Maintains account + location information for home customers
- Visitor Location Register (VLR)
  - Cache of HLR data on active roamers in each Service Area

4G / 5G — integrated mobility management replaces HLR/VLR

Call Establishment

Performed when user initiates or receives call

Security

Protects from fraud and eavesdropping

Handoff (handover)

Performed when MS changes attachment point to network

Handoff (Handover)

User moves between cells

Hard Handoff

Old cell transfers control to new cell

Break-Before-Make sequence

- Transceiver in old cell stops transmitting to user
- Transceiver in new cell begins transmitting to user

New BS assigns user frequency pair from its frequency group

Soft Handoff

Central transceiver coordinates with nearest cells

Determines which transmitter is receiving strongest signal from user

Make-Before-Break sequence

- Transceiver in old cell transmitting to user
- Transceiver in new cell begins transmitting to user
- Transceiver in old cell stops transmitting to user

Cellular Networks

First Mobile Telephone

AT&T Mobile Phone System (MPS)

1970

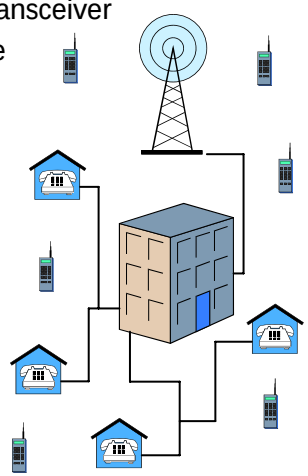
0G

One central transceiver (transmitter/receiver)

Mobile telephones communicate via central transceiver

Transmit at high power for maximum distance

System covers 65 to 80 km



Modulation is standard analog FM

Supports 12 simultaneous mobile phone calls

If 12 channels busy, other calls are blocked

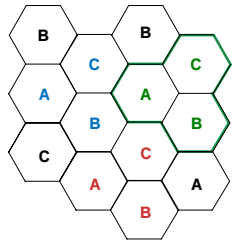
Requires 24 carrier frequencies

2 frequencies per phone:

- Dedicated transmit frequency
- Dedicated receive frequency

Cellular Concept

Divide coverage area into cells



In each cell

Central cell transceiver serves all clients in cell

Mobile Stations communicate via cell transceiver

Each active device allocated frequency pair

- Receive — downstream from base station
- Transmit — upstream to base station

Transmit at low power (just enough to cover a cell)

Use same frequencies in many cells

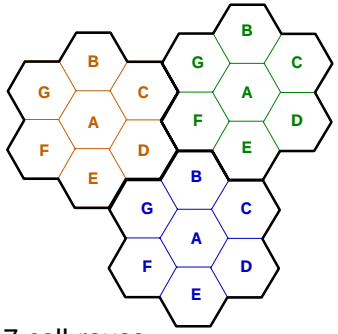
No interference between cells

Handoff

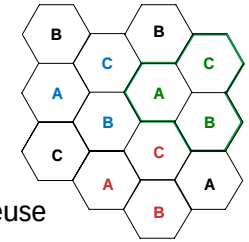
Telephone can move from cell to cell during a call

Requires cell-to-cell infrastructure and coordination

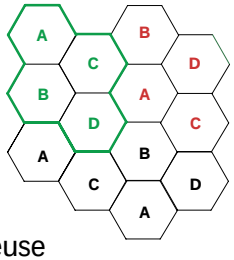
Frequency (Channel) Reuse Patterns



7 cell reuse



3 cell reuse



4 cell reuse

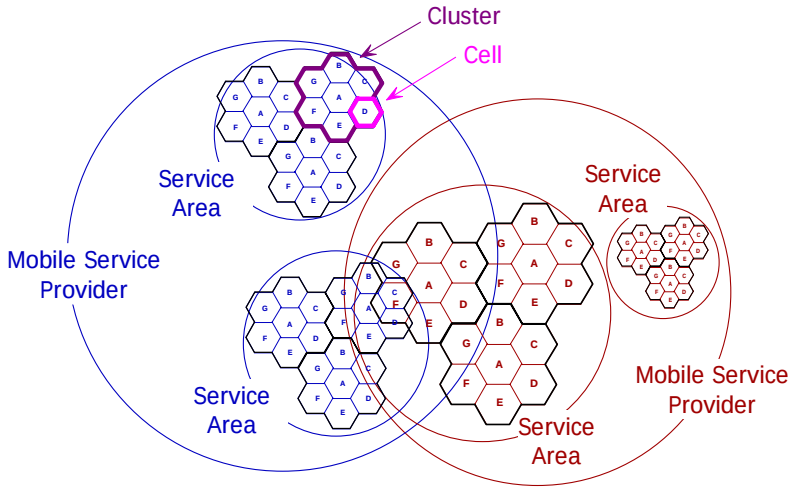
Mobile Network Switching Hierarchy

Mobile Service Provider

Service Areas or Registration Areas

Clusters

Cells

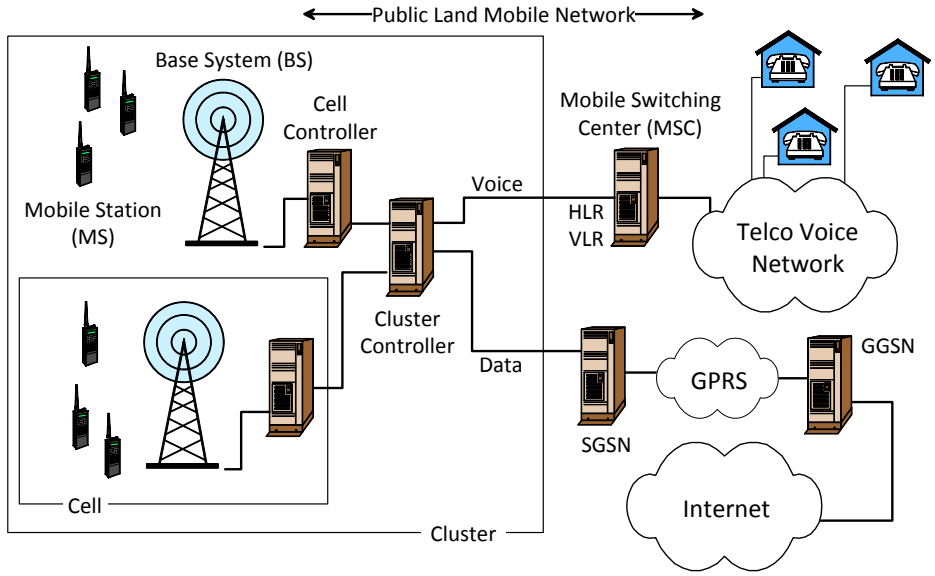


Generations in Cellular Networks

1G	Analog radio end-to-end Separate proprietary systems with no interoperability
2G	US — Separate proprietary systems with no interoperability Analog and digital radio Very limited data service EU — Public standards for European-wide interoperability GSM (Global System for Mobile telephones) digital voice channel CDMA (Code Division Multiples Access) digital voice channel GPRS (General Packet Radio Service) IP-based data network
3G	UMTS (Universal Mobile Telecommunications System) based on GSM WCDMA (Wideband CDMA) based on CDMA Adopted as international standards by ITU Higher data rates Improved mobility management
4G	ITU standard for enhanced performance (mostly still not satisfied) Eliminates voice network — voice calls carried as Voice over IP (VoIP)
5G	ITU standard for enhanced performance More complete integration of network functions

Cellular Network in 2G

Wireless to base station — uses Telco network for voice service



Registration Process in GSM

Mobile subscriber (MS) enters Service Area

Establishes low bit-rate control channel with service provider

MS requests service

Base Transmitter System (BTS) allocates a frequency pair

BTS requests access from Base Controller System (BSC)

BSC reports to Mobile Switching Center (MSC)

Location, Status, and Identity

- Dedicated hardware ID code in phone
- Subscriber Identity Module (SIM) card identifies customer in GSM
- Mobile Station generates access code to network

Transmits code by public key encryption (PKE) algorithm

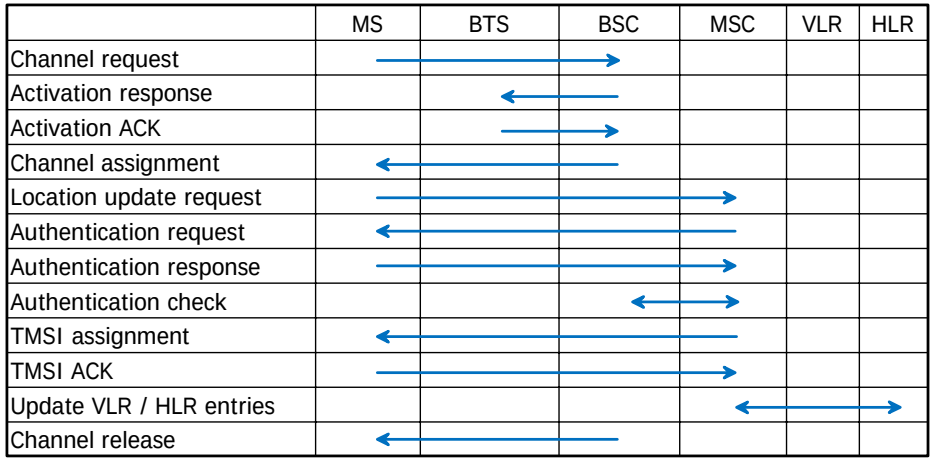
Mobile Switching Center (MSC)

Authenticates customer identity with HLR

For roaming subscriber, creates VLR entry

Updates Home Location Register (HLR) and billing database

GSM Registration



GSM Call Establishment

MS Initiated

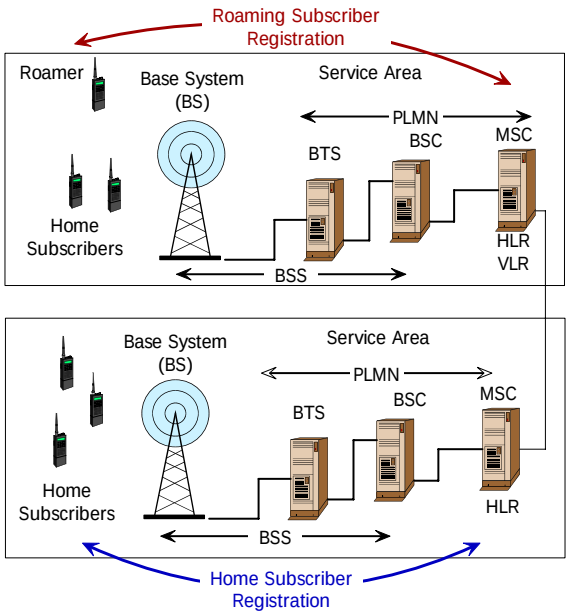
	MS	BTS	BSC	MSC
Request control channel	→	→		
Assign control channel	←	←		
Call establishment request	→	→	→	
Authentication request	←	←	←	
Authentication response	→	→	→	
Encryption key	←	←	←	
Encryption response	→	→	→	
Destination address	→	→	→	
Routing response	←	←	←	
Traffic channel request	→	→		
Assign traffic channel	←	←		
Available or busy	←			
Call accepted	←	←	←	
Connection established				
Data exchange	→	→	→	

GSM Call Establishment

Mobile Terminated

	MS	BTS	BSC	MSC	VLR	HLR	GMSC	PSTN	Caller
Standard call set-up								←	
Request to Gateway MSC							←		
HLR user request						↔	↔		
Assign roaming number					↔	↔			
Request to MSC (user location)						←			
Update user status				↔	↔				
Page MS	↔	↔	↔	↔					
Authentication				↔	↔				
Call connection	↔	↔	↔	↔					

Mobility Management in GSM

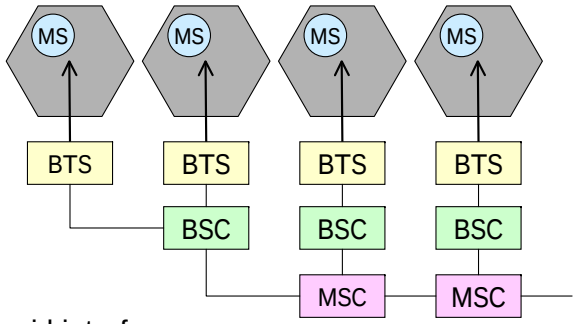


PLMN — public land mobile network, the portion of the cellular network that operates over cables.

BSS — Base Station Subsystem
GSM Access Network
Handles one cell

MSC — Mobile Switching Center
Handles multiple BSSs

Handover Types in GSM



Intra-cell

Change frequencies to avoid interference

Inter-cell — Intra-BSC

MS moves between cells within control of one BSC

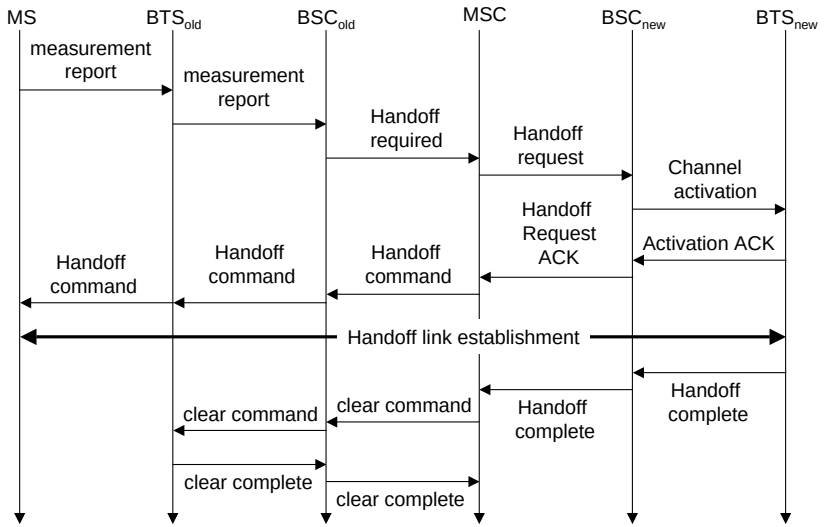
Inter-BSC — Intra-MSC

MS moves between cells controlled by different BSCs
MSC controls handover

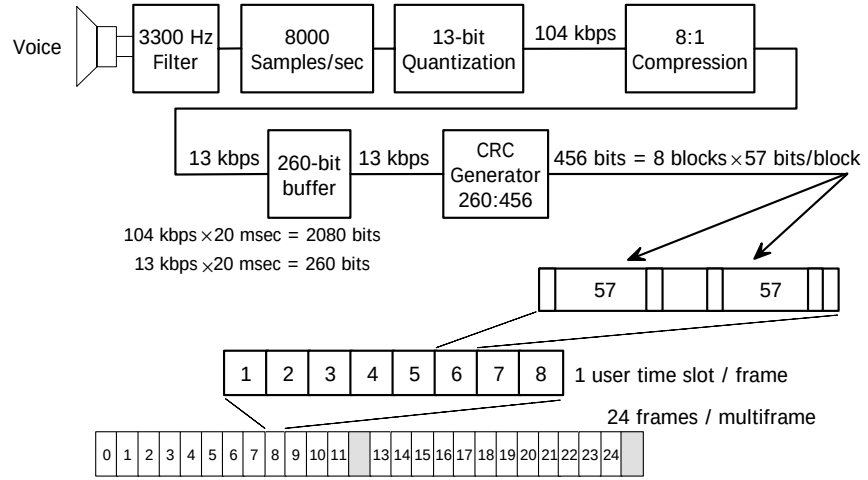
Inter MSC

MS moves between cells controlled by different MSCs

GSM Inter-BSC Handover Procedure



GSM Voice Transmission Summary

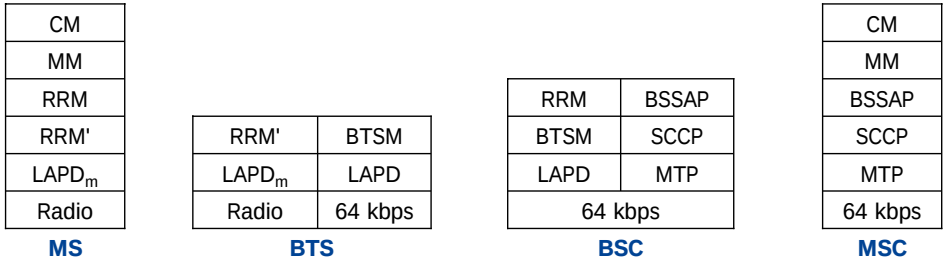


57 user bits per field × 2 fields per frame × 24 frames per multiframe = 2736 user bits per multiframe

2736 bits per multiframe / 120 ms per multiframe = 22.8 kbps

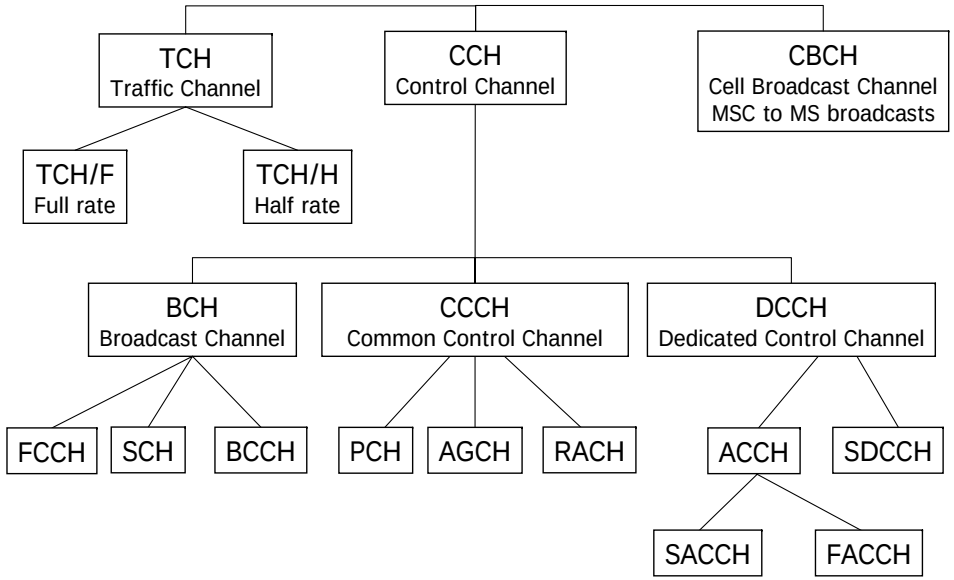
22.8 kbps / (456/260) = 13 kbps

GSM Protocol Stack



CM	Connection Management
MM	Mobility Management
RRM RRM'	Radio Resource Management — allocates physical parameters for radio system Separate protocol instances at MS/BTS layer and MS/BSC layer
LAPD	Link Access Protocol D — ISDN layer 2 protocol (Q.920/921) for LLC services
BTSM	Base Transceiver Station Management (BTS to BSC management messages)
BSSAP	BSS Application Part (call setup + management)
SCCP	Signaling Connection Control Part (SCCP) — one SCCP connection per MS
MTP	Message Transfer Part — standard PSTN signaling and management

GSM Logical Channel Structure



General Packet Radio Service (GPRS)

Provides packet mode data access for GSM

- IP-based architecture
- Began as 2.5G enhancement

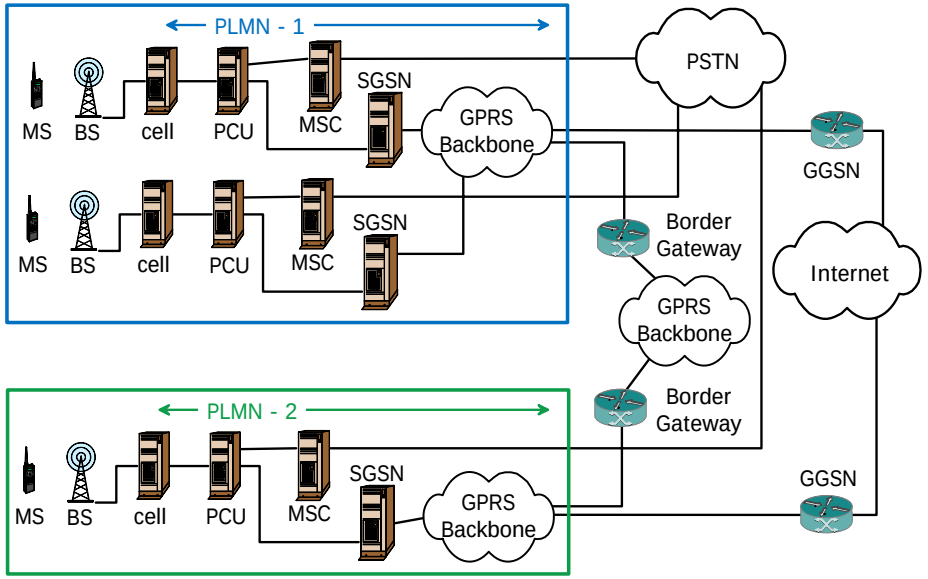
IP datagrams separated from circuit mode traffic at cluster

- Packet Control Unit (PCU)
  - Packet mode function in BSC to handle IP datagrams
- Circuit mode voice/data routed to MSC
  - Forwarded to other MSC or PSTN
- Packet mode data is routed to Serving GPRS Support Node (SGSN)
  - Forwarded to Internet
  - PCU to SGSN runs IP over Frame Relay

Mobility management

- Circuit mode traffic uses PSTN / PLMN routing
- Packet mode traffic uses IP routing

GPRS System Architecture



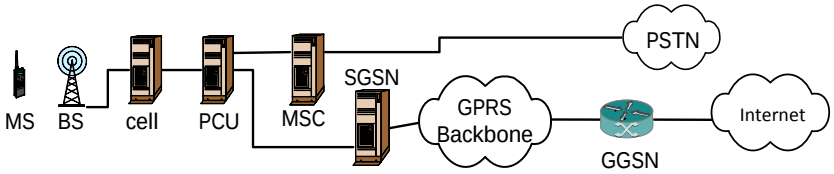
GPRS Support Nodes

Serving GPRS Support Node (SGSN)

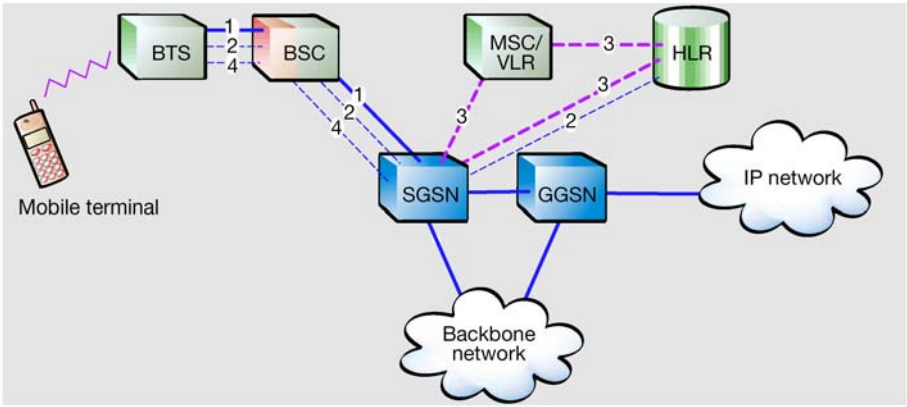
- Packet-switched version of MSC
- Handles packets to / from Mobile Stations (MS)
- Handles MS mobility management

Gateway GPRS Support Node (GGSN)

- Interfaces SGSNs to external IP networks
- Maintains routing information
  - Exterior gateway for GPRS network
  - DHCP — assigns IP addresses to MS
  - Routes incoming IP datagrams to appropriate PCU



GPRS Connection Process



GPRS Connection Process

MS switches on and sends GPRS attach request

User Registration — 1

- Associate PLMN address with Packet Data Protocol (PDP) address
  - PDP address — Static or dynamic IP
  - PLMN address — International Mobile Subscriber ID (IMSI)

Authentication

- BSC queries Home Location Registers (HLR) — 2
- HLR updates Visitor Location Registers (VLR) — 3

Call Admission Control (CAC) — 4

- Determines required network resources
- Grants resources if available

Routing — hop-by-hop IP datagram delivery

- Routing tables in GSN (GGSN or SGSN)
  - Address conversion / VC mapping
- GSN handles compression and encryption

High Speed Circuit Switched Data (HSCSD)

Circuit Switched Data (CSD)

- 14.4 kbps circuit mode data connection in 2G GSM
- User data replaces digitized voice in 1 time slot

High Speed Circuit Switched Data (HSCSD)

- 2.5G enhancement
- Up to 8 slots (full user frame) allocated to one data channel
- Up to 115.2 kbps

Transparent data transmission

- User data stream can contain signaling to network
  - Allows dynamic reconfiguration of data connection (data rate, QoS)
- HSCSD data frames carry data sub-stream numbers
  - Maintains order of transmission over GSM

Non-transparent data transmission

- Only user data in data stream
  - No signaling or reconfiguration
- LLC functions performed by GSM protocols

High Speed Downlink Packet Access (HSDPA)

Higher data rates for packet data

- Downlink speeds of 1.8, 3.6, 7.2, 14.0, 337 Mbps

HS-DSCH simplified for fast packet data

- Power control and variable chip rate eliminated

Hybrid automatic repeat-request (HARQ)

- LLC layer added between PHY and MAC (not in RLC)
- Incremental redundancy
  - Corrupted packets not discarded
  - Retransmitted packets combined until error-free packet assembled
  - Faster than waiting for uncorrupted retransmitted packet

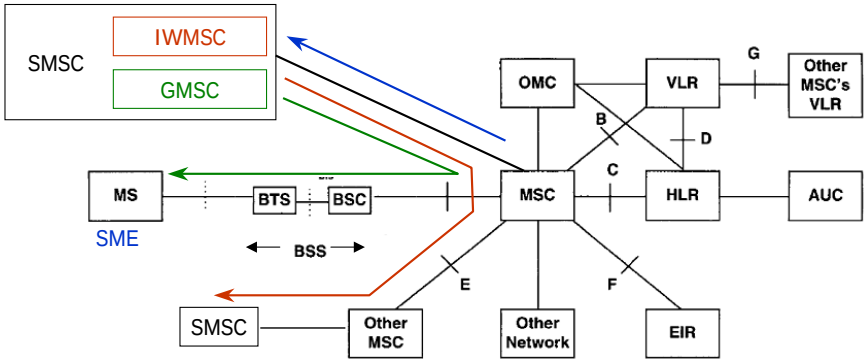
Fast packet scheduling

- 2 ms scheduling granularity (instead of 10 ms)
- Transmission scheduled to UEs reporting highest power levels

Adaptive Modulation and Coding (AMC)

- Modulation scheme and code rate depend on channel quality

SMS in GSM Architecture



SME: Short Messaging Entity

SMSC: Short Message Service Center

GMSC: Gateway Message Service Center

IWMSC: Interworking Message Service Center

SMS Nodes

Short Messaging Entity (SME)

Any entity that can receive or send short messages

- Fixed network element
- Mobile Station
- Another service center

Short Message Service Center (SMSC)

Store and forwarding of SMS between SME and MS

Gateway Message Service Center (GMSC)

Receives SMS in SMSC

Interrogates HLR for routing information

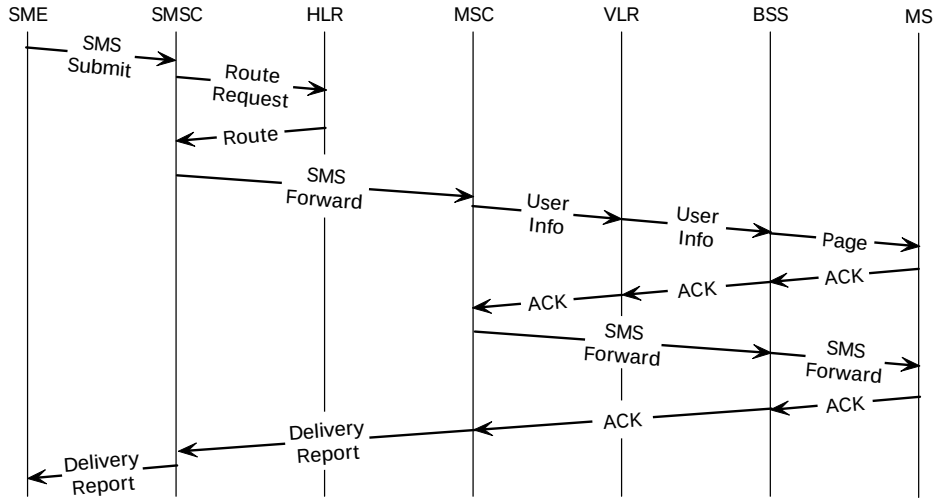
Delivers SMS to MSC for destination SME

Interworking Message Service Center (IWMSC)

Receives SMS from MSC

Delivers SMS to appropriate SMSC for forwarding

SMS Delivery to MS



CDMA

Code Division Multiple Access

Commercial system developed by Qualcomm

Operates on AMPS frequencies

Channelization

25 MHz radio band per direction

Divide band into 1.25 MHz RF channels

25 MHz per cluster / 1.25 MHz per channel = 20 channels per cluster

DSSS digital transmission

Transmit 1.2288 Mcps in 1.25 MHz radio channel

Voice and control modulation — QPSK

Code division

Users transmit simultaneously using independent chip sequences

- Orthogonal (Walsh) Codes / Pseudorandom noise (PN) codes

Receiver separates channels by decoding chip sequences

Standards

IS-95 — now called CDMAone

Orthogonal CDMA Codes

m-dimensional vector space with inner product

$$\mathbf{U} \cdot \mathbf{V} = \frac{1}{m} \sum_{i=1}^{m} U_i \times V_i$$

m orthonormal basis vectors

$S_i, i = 1, \ldots, m$

$\mathbf{T} = \sum_{i=1}^{m} t_i \times S_i$, with coefficient t_i for any vector $\mathbf{T}$

$$S_i \cdot S_j = m \times \delta_{ij} = \begin{cases} 0, i \neq j \\ m, i = j \end{cases}$$

$$t_i = S_i \cdot \mathbf{T} = S_i \cdot \frac{1}{m} \sum_{j=1}^{m} t_j \times S_j = \frac{1}{m} \sum_{j=1}^{m} t_j \times \left(S_i \cdot S_j \right) = \frac{1}{m} \sum_{j=1}^{m} t_j \times m\delta_{ij} = t_i$$

Code scheme

Basis vector S_i is code assigned to station i

Station i transmits $t_i \times S_i$ with coefficient

Total transmission from all stations

$$t_i = \begin{cases} -1, \text{data 0} \\ 0, \text{no transmission} \\ +1, \text{data 1} \end{cases}$$

$$\mathbf{T} = \sum_{i=1}^{m} t_i \times S_i$$

Example — 4-Chip CDMA

Code vectors for m = 4 stations

$$S_1 = \begin{bmatrix} -1 \\ -1 \\ -1 \\ -1 \end{bmatrix} \quad S_2 = \begin{bmatrix} -1 \\ +1 \\ +1 \\ -1 \end{bmatrix} \quad S_3 = \begin{bmatrix} -1 \\ -1 \\ +1 \\ +1 \end{bmatrix} \quad S_4 = \begin{bmatrix} -1 \\ +1 \\ -1 \\ +1 \end{bmatrix}$$

4-bit transmission levels (chips)

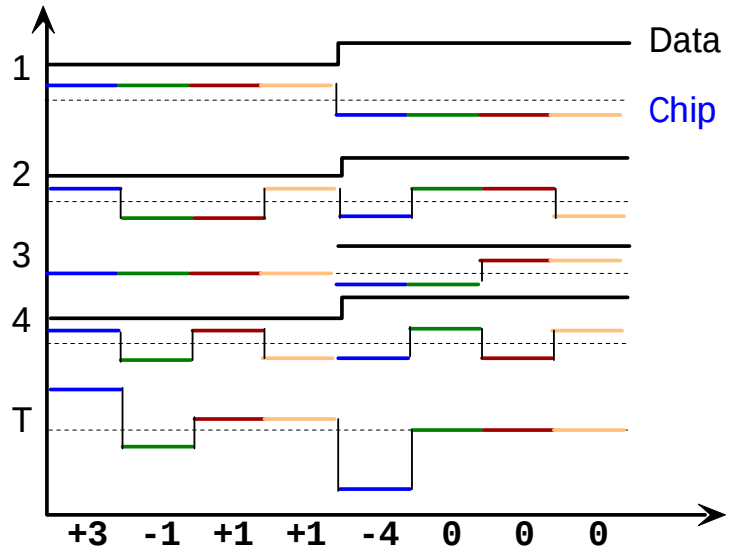
	Binary 1	Binary 0
Station 1	−1 −1 −1 −1	+1 +1 +1 +1
Station 2	−1 +1 +1 −1	+1 −1 −1 +1
Station 3	−1 −1 +1 +1	+1 +1 −1 −1
Station 4	−1 +1 −1 +1	+1 −1 +1 −1

Radio signal amplitudes added together

Example — 2-bit Transmission

Station 1	Data	0	1
	Signal	+1 +1 +1 +1	−1 −1 −1 −1
Station 2	Data	0	1
	Signal	+1 −1 −1 +1	−1 +1 +1 −1
Station 3	Data	no data	1
	Signal	0 0 0 0	−1 −1 +1 +1
Station 4	Data	0	1
	Signal	+1 −1 +1 −1	−1 +1 −1 +1
Total Transmission	Signal	+3 −1 +1 +1	−4 0 0 0

Example — 2-bit Transmission



Example — Decoding

Inner Product

$$\mathbf{U} \cdot \mathbf{V} = \frac{1}{4} \sum_{i=1}^{4} U_i V_i \qquad t_j = \mathrm{T} \cdot \mathrm{S}_j$$

First bit **T** = (+3, -1,+1,+1)	$t_1 = \frac{1}{4}(3,-1,+1,+1)\cdot(-1,-1,-1,-1) = \frac{1}{4}[-3+1-1-1] = -1 \Rightarrow 0$ $t_2 = \frac{1}{4}(3,-1,+1,+1)\cdot(-1,+1,+1,-1) = \frac{1}{4}[-3-1+1-1] = -1 \Rightarrow 0$ $t_3 = \frac{1}{4}(3,-1,+1,+1)\cdot(-1,-1,+1,+1) = \frac{1}{4}[-3+1+1+1] = 0 \Rightarrow$ no data $t_4 = \frac{1}{4}(3,-1,+1,+1)\cdot(-1,+1,-1,+1) = \frac{1}{4}[-3-1-1+1] = -1 \Rightarrow 0$
Second bit **T** = (-4,0,0,0)	$t_1 = \frac{1}{4}(-4,0,0,0)\cdot(-1,-1,-1,-1) = \frac{1}{4}[4] = +1 \Rightarrow 1$ $t_2 = \frac{1}{4}(-4,0,0,0)\cdot(-1,+1,+1,-1) = \frac{1}{4}[4] = +1 \Rightarrow 1$ $t_3 = \frac{1}{4}(-4,0,0,0)\cdot(-1,-1,+1,+1) = \frac{1}{4}[4] = +1 \Rightarrow 1$ $t_4 = \frac{1}{4}(-4,0,0,0)\cdot(-1,+1,-1,+1) = \frac{1}{4}[4] = +1 \Rightarrow 1$

Orthogonal Walsh Codes

Walsh 0

$W_0 = \boxed{1}$ $\quad W_0' = \boxed{-1}$

Walsh 1

$$W_1 = \begin{array}{|c|c|}\hline W_0 & W_0 \\ \hline W_0 & W_0' \\ \hline \end{array} = \begin{array}{|c|c|}\hline 1 & 1 \\ \hline 1 & -1 \\ \hline \end{array}$$

Walsh 2

$$W_2 = \begin{array}{|c|c|}\hline W_1 & W_1 \\ \hline W_1 & W_1' \\ \hline \end{array} = \begin{array}{|c|c|c|c|}\hline 1 & 1 & 1 & 1 \\ \hline 1 & -1 & 1 & -1 \\ \hline 1 & 1 & -1 & -1 \\ \hline 1 & -1 & -1 & 1 \\ \hline \end{array} = \begin{array}{|c|}\hline S_1 \\ \hline S_4 \\ \hline S_3 \\ \hline S_2 \\ \hline \end{array}$$

Walsh 3

$$W_3 = \begin{array}{|c|c|}\hline W_2 & W_2 \\ \hline W_2 & W_2' \\ \hline \end{array}$$

Walsh N

$$W_N = \begin{array}{|c|c|}\hline W_{N-1} & W_{N-1} \\ \hline W_{N-1} & W_{N-1}' \\ \hline \end{array}$$

Walsh N is $2^N \times 2^N$ matrix

Pseudo-Noise (PN) Coding

Pseudorandom Bernoulli sequence of 1 or –1

Equivalent to sequence of m coin tosses

Nearly equal number of 1 and –1 in each code

By central limit theorem

$$P_{-1} = P(-1) = \frac{1}{2} + \delta \qquad P_{+1} = P(+1) = \frac{1}{2} - \delta \qquad |\delta| < \frac{1}{\sqrt{m}}$$

Codes are "nearly orthogonal"

For codes A and B with chip patterns $C_i^{(A)}$ and $C_i^{(B)}$

$$A = B \Rightarrow \frac{1}{m}\sum_{i=1}^{m} C_i^{(A)} \times C_i^{(B)} = \frac{1}{m}\sum_{i=1}^{m} [\pm 1]^2 = 1$$

$$A \neq B \Rightarrow \frac{1}{m}\sum_{i=1}^{m} C_i^{(A)} \times C_i^{(B)}$$

$$= \frac{1}{m}\sum_{i=1}^{m} \left[P_{+1} \times P_{+1} - P_{+1} \times P_{-1} - P_{-1} \times P_{+1} + P_{-1} \times P_{-1}\right] = 4\delta^2 < \frac{4}{m}$$

Channel Coding

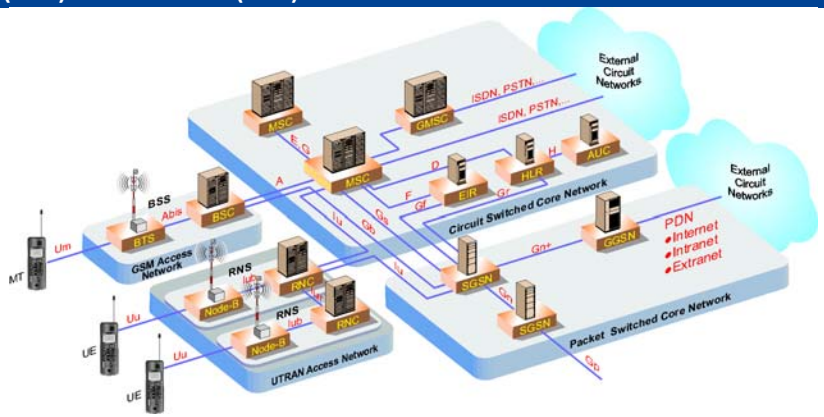
Forward channels

- 64 orthogonal Walsh codes to 64 users
  - Theoretically perfect separation between users
- All signals in same cell scrambled using PN sequence
  - Reduces interference between same Walsh code in neighboring cells
  - Short PN sequence uses cell ID as seed
  - Paging and traffic scrambled with long PN sequence before Walsh

Reverse channels

- Orthogonal codes not applicable in uplink
  - Orthogonality requires time synchronization
  - MSs transmit asynchronously
- Long PN sequence
- Stream is scrambled using short PN sequence
- Carries cell ID

GSM (2G) → UMTS (3G)



GSM Name	UMTS Name
Base Transmitter System (BTS)	Node-B
Base Controller System (BSC)	Radio Network Controller (RNC)
Base Station Subsystem (BSS)	Radio Network System (RNS)

UMTS Terrestrial Radio Access Network (UTRAN) new in 3G

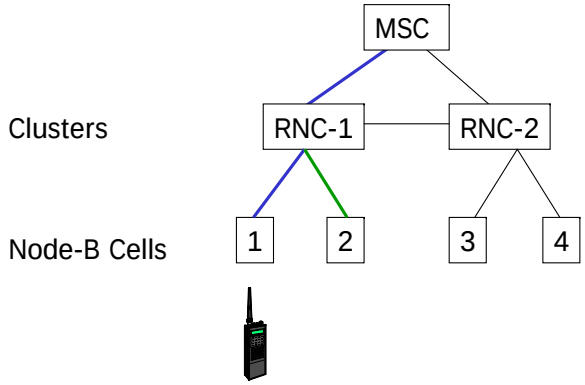
Handles mobility between related RNSs instead of MSC

3G Relocation

Serving RNC (SRNC) — RNC-1

Primary Node-B — 1

Monitoring Node-B — 2

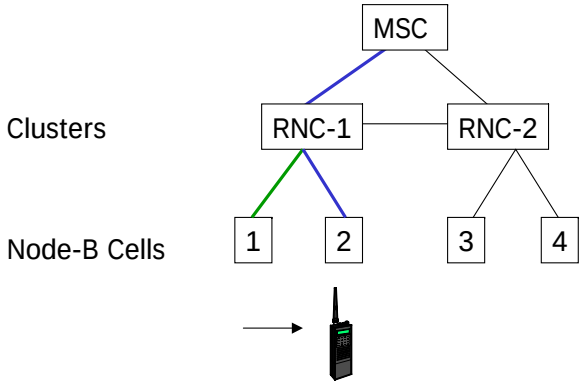


3G Relocation

Serving RNC (SRNC) — RNC-1

UE relocates to primary Node-B — 2

Monitoring Node-B — 1



3G Relocation

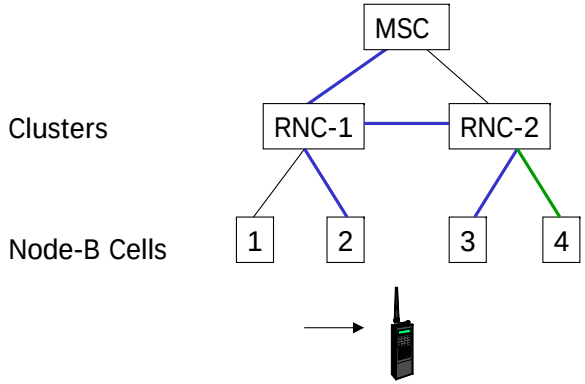
Serving RNC (SRNC) — RNC-1

Active Node-B — 2

Relaying RNC (RRNC) — RNC-2

Primary Node-B — 3

Monitoring Node-B — 4



SRNC (RNC-1) combines data from 2 and 3

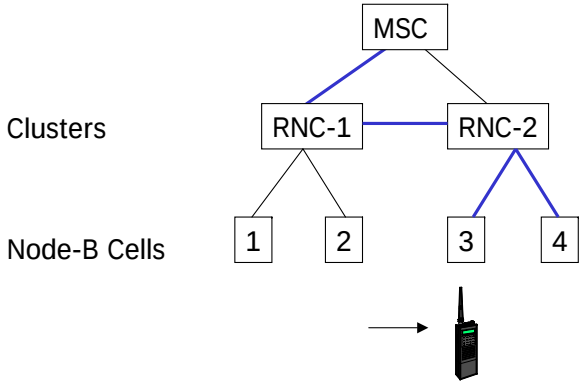
3G Relocation

Serving RNC (SRNC) — RNC-1

No active Node-B

Relaying RNC (RRNC) — RNC-2

Primary Node-Bs — 3 + 4



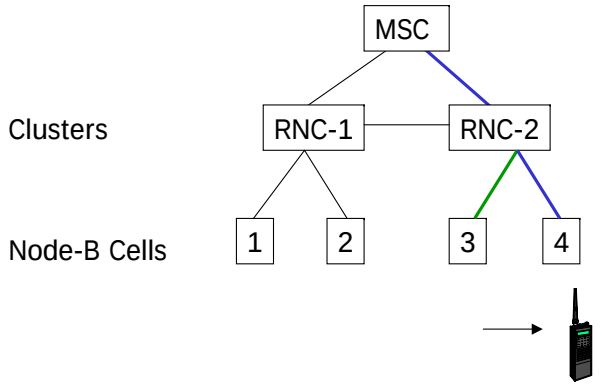
RNC-2 combines data from 3 and 4

SRNC (RNC-1) receives combined data from RNC-2

3G Relocation

Serving RNC (RRNC) — RNC-2

- Monitoring Node-B — 3
- Primary Node-B — 4



3G → 4G

Initial planning for 4G

- International Mobile Telecommunications Advanced (IMT-Advanced)
- Conceived as general network supporting mobility
  - Data + Voice over IP
- Convergence with Next Generation Networks (NGN)

4G objectives

- Higher network capacity than 3G
- Spectral efficiency (high bps / Hz and bps / Hz /site)
- 100 Mbps for moving client and 1 Gbps for stationary client
- 100 Mbps between any two points in world
- Smooth handoff across heterogeneous networks
- Global roaming across multiple networks
- QoS for multimedia support — audio, HDTV, etc
- Interoperability with existing wireless standards
- All IPv6 packet switched network — eliminate circuit mode entirely

Long Term Evolution (LTE)

Extension ("evolution") of GSM / UMTS

- Marketed as 4G — does not meet all IMT/NGN standards
- Attaches "e" (evolved) to UMTS terminology

Improved radio interface + data rates

- 299.6 Mbps downstream
- 75.4 Mbps upstream

Improved mobility

- Supports MS moving at 500 km/h

Voice over LTE (VoLTE)

- Packet switched voice over IP
- Replacement for circuit switched voice network
- Enhanced voice encoding as VBR stream

Circuit-switched fallback (CSFB)

- Intermediate migration path
- Data over LTE + circuit switched voice

System Architecture Evolution (SAE)

LTE core network architecture

- All IP network
- Replaces GPRS packet network of GSM/UMTS

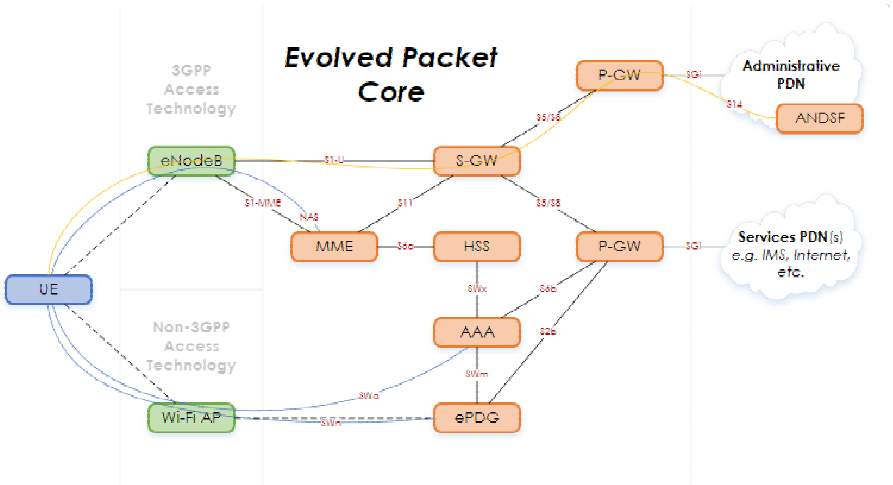
Evolved UTRAN (e-UTRAN)

- Replaces UTRAN in 3G networks
- eNodeB — replaces UMTS NodeB in e-UTRAN

Evolved Packet Core (EPC)

- Mobility Management Entity (MME) — replaces GSM VLR
- Home Subscriber Server (HSS) — replaces GSM HLR
- Serving Gateway (SGW)
  - Routes and forwards user data packets within cellular network
  - Replaces hierarchical network of MSC / SGSN / nodes in GSM/UMTS
- Packet Data Network Gateway (PGW)
  - Routes and forwards user data packets to Internet
  - Replaces GGSN in GSM/UMTS

Evolved Packet Core (EPC) Interfaces



Ref: https://en.wikipedia.org/wiki/System_Architecture_Evolution

4G → 5G

Non-Standalone mode (NSA)

- Supports Mobile Broadband (eMBB)
- Enhanced 4G as a 5G use case
- Provides 5G New Radio (NR) add-on to 4G LTE radio
- Higher data rates + lower latency
  - Up to 10 Gbps

5G Next Generation Core (NGC)

- New abstract networking model
  - Service Based Architecture (SBA)
  - Network functions defined as services — not hardware
- Extensive implementation of
  - Software Defined Network (SDN)
  - Network Function Virtualization (NFV)
- Network designed by standards of software engineering
- Support for Internet of Things (IoT)