18-452/18-750
Wireless Networks and Applications
Lecture 14:
Cellular: 2G

Peter Steenkiste

Spring Semester 2024

http://www.cs.cmu.edu/~prs/wirelessS24

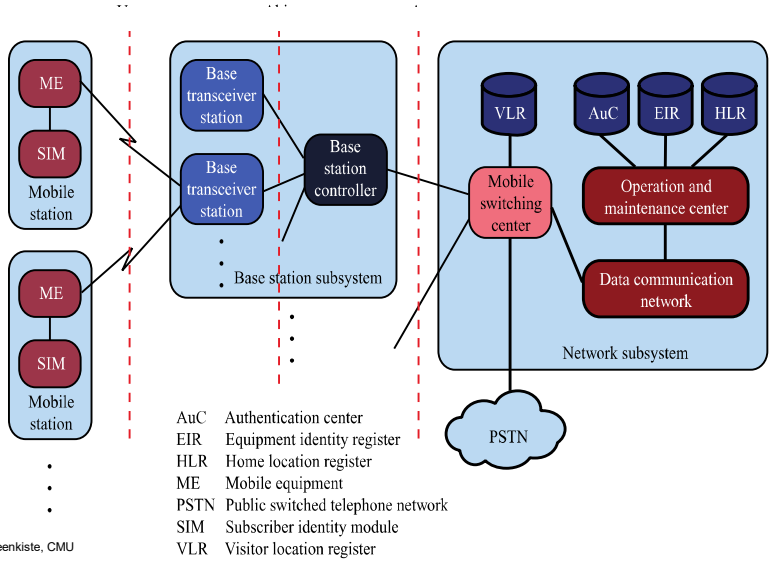
GSM Features

- Hybrid FDMA/TDMA approach
- Mobile station communicates across the air interface with base station in the same cell as mobile unit
- Mobile equipment (ME) – physical terminal, e.g., a telephone or "personal communication system"
  - » ME includes radio transceiver, digital signal processors and subscriber identity module (SIM)
- GSM subscriber units are generic until a SIM is inserted
  - » SIMs roam since they are based on single standard
  - » Not necessarily the case for subscriber devices – may use different versions of the protocol

GSM SIM

- Users have a Subscriber Identity Module (SIM) – a smart card
- The user identity is associated with a mobile device through the SIM card
- The SIM is portable and transferable
- All cryptographic algorithms (for authentication and data encryption) can be realized in the SIM
- May also store short messages, charging info, ..
- SIM implications:
  - » Equipment mobility and user mobility are not the same
  - » International roaming independent of the equipment and network technology

Global GSM System



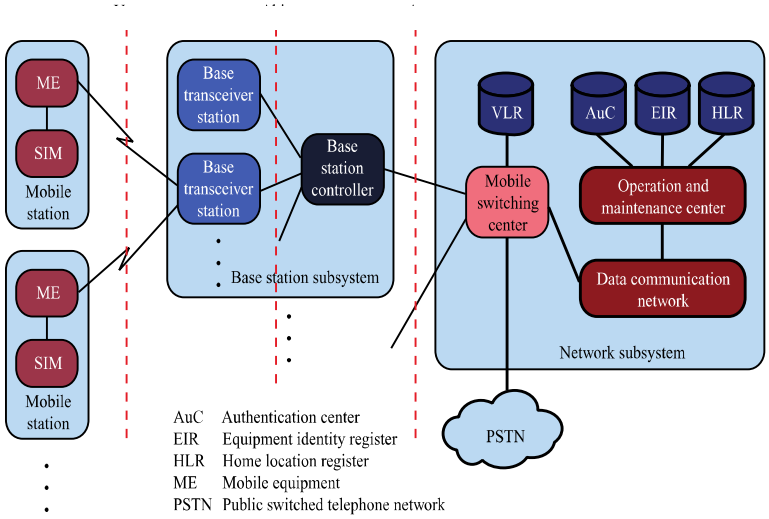
Base Transceiver Station or "Basestation"

- Radio transmission/reception management
  - Modulation/demodulation, equalisation, interleaving ...
- Each BTS defines a single cell
  - » Includes radio antenna, radio transceiver and a link to a base station controller (BSC)
- Physical layer management
  - TDMA transmission, slow frequency hopping, coding, ...
- Link layer management
- Received signal quality and power measurement
- Defines a single "cell"

Base Station Controller

- Interface between the basestations and the mobile switching center
  - Forwarding of traffic
  - Reserves radio frequencies and controls paging
- Manages handoff of mobile unit from one cell to another within the Basestation Subsystem
- Radio resource management for the Base Station Subsystem
  - Channel allocation
  - Basestation measures processing
  - Basestation and mobile device power control
  - ..

Global GSM System



Network Subsystem (NS)

- NS provides link between cellular network and public switched telecommunications networks (PSTN)
  - » GSM was originally voice-only
  - » Controls handoffs between cells in different Base Station Subsystems
  - » Authenticates users and validates accounts
  - » Enables worldwide roaming of mobile users
- Central element of NS is the Mobile Switching Center (MSC)

Mobile Switching Center

- Management of the communication between mobile devices and the fixed telephone network
  - The Gateway Mobile Switching Controller forms the gateway for calls to and from external networks
- MSC is also responsible for mobility management
  - Handover between Base Station Subsystems
  - Roaming across networks

Handover

- Executed by BSC (channels) and by MSC (routing)
- Initiated by base station:
  - » BS monitors the signal coming from the mobile device
  - » Low signal => Need to do handover
- Mobile-terminal aided:
  - » BS transmit beacon
  - » Mobile device, when hearing better beacon, requests join
    - – Sends the identity of the old BS to the new BS
  - » BS accepts the mobile device - calls are then forwarded
- Inter-system system handover is managed MSC
  - » With extra connections to the HLR/VLR

Mobile Switching Center (MSC) Databases

- Home location register (HLR) database – stores information about each subscriber that belongs to this MSC
- Visitor location register (VLR) database – maintains information about subscribers currently physically in the region
- Authentication center database (AuC) – used for authentication activities, holds encryption keys
- Equipment identity register database (EIR) – keeps track of the type of equipment that exists at the mobile station

Home Location Register

- One per local network
  - » Local network covers a geographic area, e.g., Pittsburgh
  - » Controlled by a Network Subsystem
- HLR stores information for every local subscriber
  - » Phone number corresponds to Pittsburgh area code
  - » Identify, billing information, mobile plan information, ..
- This includes temporary information
  - » E.g., the mobile device is currently connected to a remote network subsystem
- All administrative activities of the subscriber happen here!

Visitor Location Register

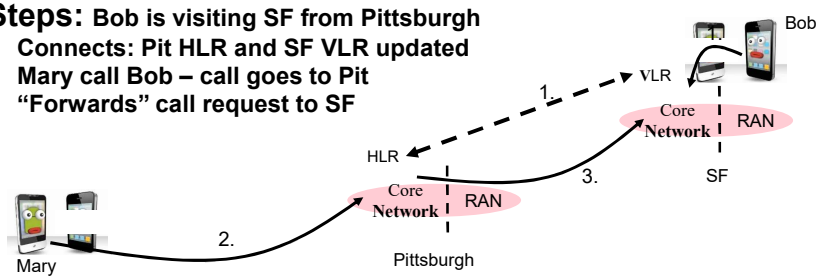
- The VLR stores data on "visiting" mobile stations that are roaming in the localnetwork subsystem
  - » Their home network is somewhere else, e.g., LA
  - » Typically one per network, but 1 VLR could be responsible for several networks
- MS registers upon entering a LA. The MSC passes the identity of the MS and LAI to VLR
  - » See next slide

Roaming In Cellular

- Subscribers are associated with a particular network subsystem, e.g, Pittsburgh region
  - » Historically, phone number is associated with this system
- How can you receive a phone call if you are not in your network?
- Roaming falls into two categories
  - » Roaming between systems but in the network of the same provider
  - » Roaming across providers, e.g., when traveling abroad
  - » Roaming mechanisms are similar but business aspects and some details are different

How about Mobility?

- Subscribers of one network (e.g., Pittsburgh) can get cellular service in other networks (e.g., SF) of same provider
- High level solution (2G terminology)
  - » Home Location Registry: local subscriber information
  - » Visitor Location Registry: visiting subscribers
- **Steps:** Bob is visiting SF from Pittsburgh
  1. Connects: Pit HLR and SF VLR updated
  2. Mary call Bob – call goes to Pit
  3. "Forwards" call request to SF

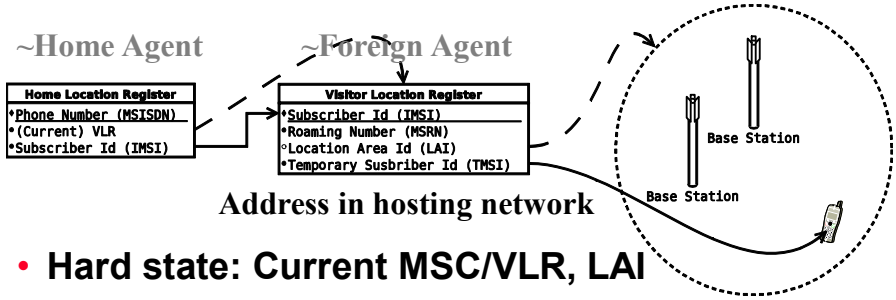


GSM Addressing Hierarchy

- Device
  - » IMEI (International Mobile Equipment Identifier)
- User
  - » IMSI (International Mobile Subscriber Identifier)
  - » MSISDN (Mobile Subscriber IDSN Number)
    - – "Real phone number"
  - » MSRN (Mobile Station Roaming Number)
  - » TMSI (Temporary Mobile Subscriber Identity)
  - » LMSI (Local Mobile Subscriber Identity)
- Other
  - » LAI (Location Area Identity)
  - » CI (Cell Identity)

No need to memorize this list!

GSM Address Lookup ("registers")



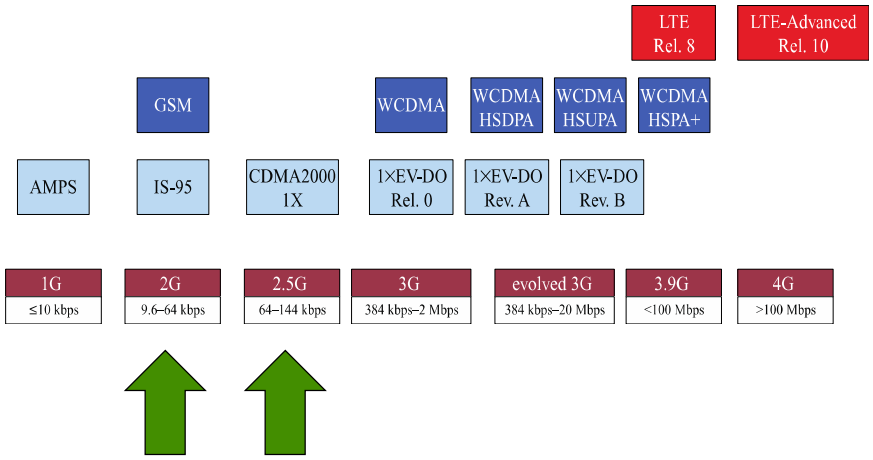
- Hard state: Current MSC/VLR, LAI
  - » (Necessary to page phone, updated whenever mobile moves)
- Soft-ish state:
  - » MSRN, cell ID, TMSI

Note: Grossly simplified for your safety and sanity!

Roaming Discussion

- Roaming introduces some challenges for the phone, similar to those for Wifi
- When you open your phone, how do you know whether the cellular channels are?
  - » There is a lot of variability across regions and countries
- When you are outside of the coverage area of your provider, how do you know which providers you can use?
- Your phone needs to have this information in its memory (at least enough to get started)
  - » This information is updated by your provider as part of regular updates

Evolution of Cellular Wireless Systems



GSM Multiple Access Example

- Combination of FDMA and TDMA
  - » More on this later
- 890-915 MHz for uplink
- 935-960 MHz for downlink
- Each of those 25 MHz bands is sub divided into 124 single carrier channel of 200 KHz
  - » Each with a data rate of 270.833 kbps
  - » Subcarriers are not orthogonal – not OFDM!
- In each uplink/downlink band there is a 200 KHz guard band
- Each 200 KHz channel carries 8 TDMA channels

Additional GSM Features

- GSM uses GMSK modulation
  - » Gaussian Minimum Shift Keying
  - » Optimized version of Frequency Shift Keying (FM)
- Slow frequency hopping: successive TDMA frames are sent over a different frequency
  - » Switches every 4.615 msec
  - » Spreads out effect of multipath fading (fast fading)
  - » Also helps with co-channel interference
- Delay equalization
  - » Mobile stations sharing a frame can be at different distances from the base station
  - » Tail bits and guard bits provide margin to avoid overlap

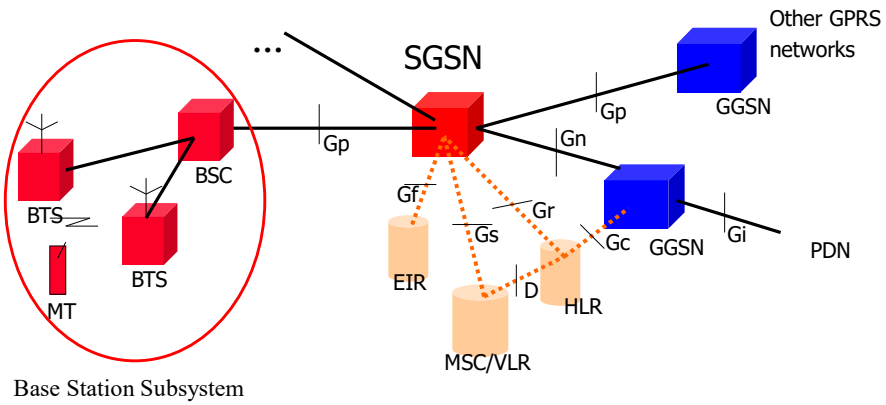
Generalized Packet Radio Service (GPRS)

- Packet-oriented data transport service
  - » Bursty, non-periodic traffic typical for Internet access
- Uses a new architecture for data traffic
  - » Allows users to open a persistent data connection
  - » Sending data traffic over a voice connection would add too much setup and teardown overhead
- Uses the same frame structure as voice
  - » 21.4 kbps from a 22.8 kbps gross data rate
  - » Can combine up to 8 GSM connections
    - – Overall throughputs up to 171.2 kbps
  - » Enhanced Data Rates for GSM Evolution (EDGE) increases rates using more aggressive PHY – GSM 2.5

GPRS Architecture

- **Network Subsystem includes several new entities:**
  - **Serving GPRS Support Node (SGSN): data transfer between Base Station and Network Subsystem**
  - **Gateway GPRS Support Node: connects to other GPRS networks and the packet data network (Internet)**
  - **New interfaces between the various entities**
- **Transmission plane**
  - **Data packets are transmitted by a tunnel mechanisms**
- **Control plane**
  - **Protocol for tunnel management: create, remove, …**
  - **GPRS Tunnel Protocol**
- **Radio interface**
  - **Changes the logical channels and how they are managed**

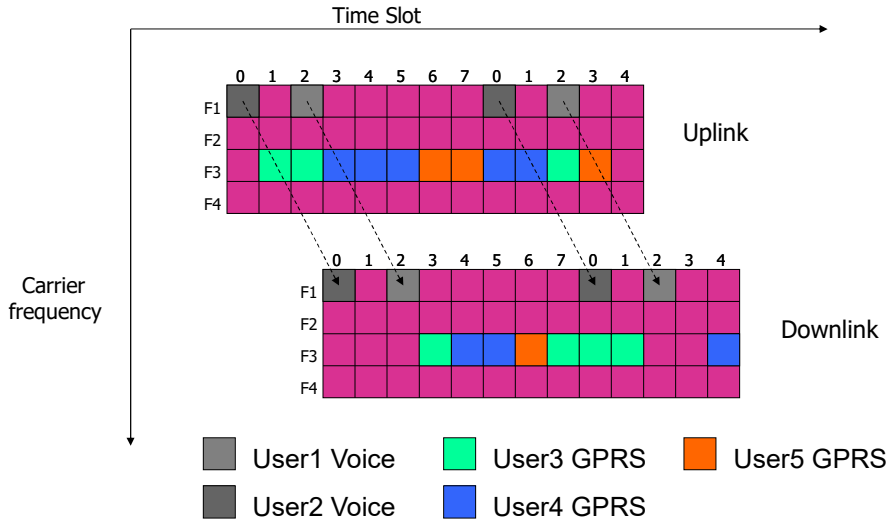
GPRS Architecture



Base Station Subsystem

SGSN – Serving GPRS Support Node
GGSN – Gateway GPRS Support Node

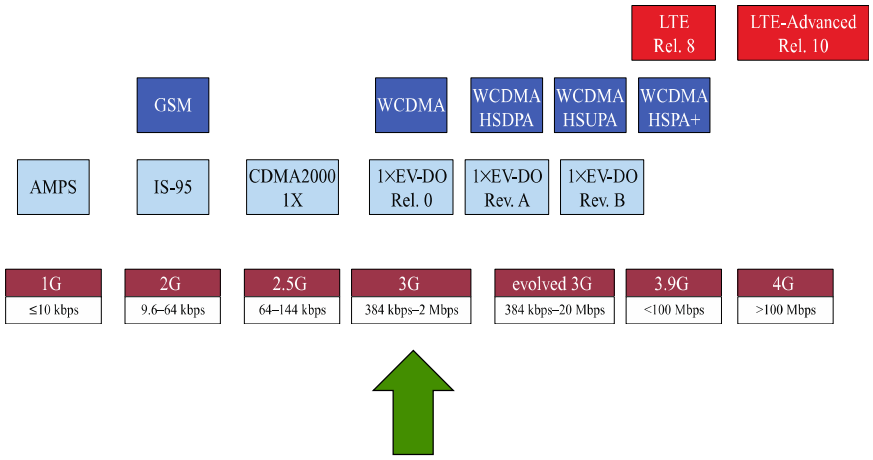
GPRS Radio Interface



Bandwidth Allocation for Devices

- The allocation of transmit resources to devices is controlled by the basestation
- Control channels are used for coordination
  - » Effectively slots in the resource grid (previous slide)
- Downstream: basestation can send data to devices at will
  - » Uses the control channel to identify target devices
- Upstream: devices must request slots to transmit data when they have packet pending
  - » Again uses the control channel for request & response
  - » Adds delay – traditionally quite high in cellular!

Evolution of Cellular Wireless Systems



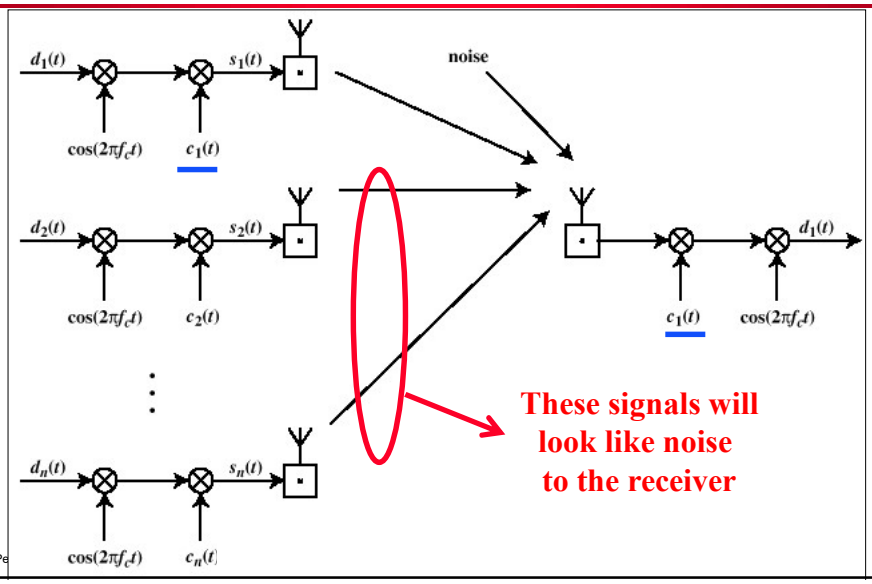
Who is Who

- **International Telecommunications Union (ITU) - agency of the United Nations responsible for:**
  - **Assisting in the development and coordination of world-wide standards**
  - **Coordinate shared use of the global spectrum**
  - **Defined the International Mobile Telecommunications 2000 (IMT-2000) project for 3G telecommunications**
- **Third Generation Partnership Project (3GPP)**
  - **A group of telecommunications associations that represent large markets world-wide**
  - **Defined a group of 3G standards as part of the IMT-2000 framework in 1999**
  - **Originally defined GSM, EDGE, and GPRS**
  - **Later defined follow-on releases and also LTE (4G)**

UMTS and WCDMA

- Part of a group of 3G standards defined as part of the IMT-2000 framework by 3GPP
- Universal Mobile Telecommunications System (UMTS)
  - » Successor of GSM
- W-CDMA is the air interface for UMTS
  - » Wide-band CDMA
  - » Originally 144 kbps to 2 Mbps, depending on mobility
- Basically same architecture as GSM
  - » Many GSM functions were carried over WCDMA
  - » But they changed all the names!

Reminder: CDMA - Direct Sequence Spread Spectrum



Later Releases Improved Performance

- High Speed Downlink Packet Access (HSDPA): 1.8 to 14.4 Mbps downlink
  - » Adaptive modulation and coding, hybrid ARQ, and fast scheduling
- High Speed Uplink Packet Access (HSUPA): Uplink rates up to 5.76 Mbps
- High Speed Packet Access Plus (HSPA+): Maximum data rates increased from 21 Mbps up to 336 Mbps
  - » 64 QAM, 2×2 and 4×4 MIMO, and dual or multi-carrier combinations
- Eventually led to the definition of LTE

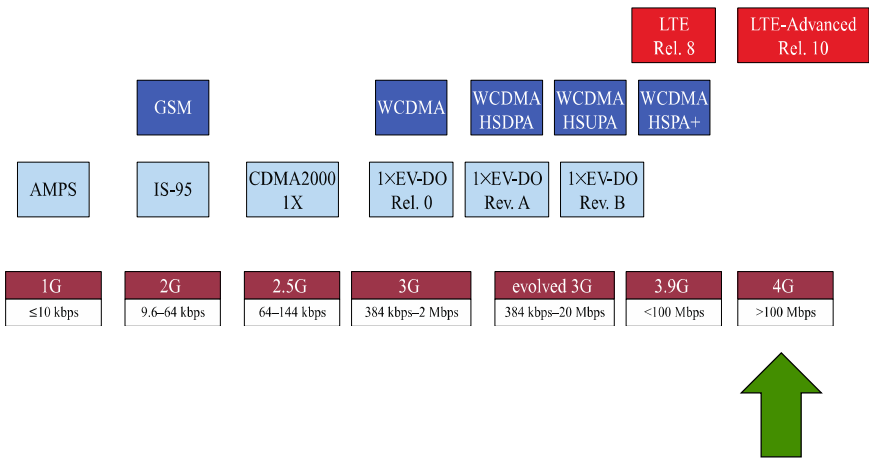
Advantages of CDMA for Cellular systems

- Frequency diversity – frequency-dependent transmission impairments have less effect on signal
- Multipath resistance – chipping codes used for CDMA exhibit low cross correlation and low autocorrelation
- Privacy – privacy is inherent since spread spectrum is obtained by use of noise-like signals
- Graceful degradation – system only gradually degrades as more users access the system

Mobile Wireless CDMA Soft Hand-off

- Soft Handoff – mobile station temporarily connected to more than one base station simultaneously
- Requires that the mobile acquire a new cell before it relinquishes the old
- More complex than hard handoff used in FDMA and TDMA schemes

Evolution of Cellular Wireless Systems



Overview LTE

- Motivation
- Architecture
- Resource management
- LTE protocols
- Radio access network
  - » OFDM refresher
- LTE advanced

Some slides based on material from
"Wireless Communication Networks and Systems"

Purpose, motivation, and approach to 4G

- Defined by ITU directives for International Mobile Telecommunications Advanced (IMT-Advanced)
- All-IP packet switched network.
- Ultra-mobile broadband access
- Peak data rates
  - » Up to 100 Mbps for high-mobility mobile access
  - » Up to 1 Gbps for low-mobility access
- Dynamically share and use network resources
- Smooth handovers across heterogeneous networks
  - » 2G and 3G networks, small cells such as picocells, femtocells, and relays, and WLANs
- High quality of service for multimedia applications

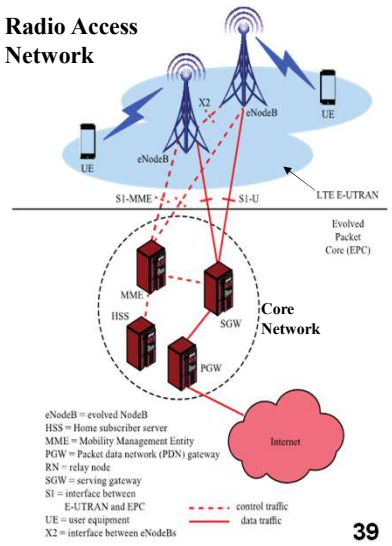
High Level Features

- **No support for circuit-switched voice**
  - **Instead providing Voice over LTE (VoLTE)**
- **Replace spread spectrum/CDMA with OFDM**

Technology	1G	2G	2.5G	3G	4G
Design began	1970	1980	1985	1990	2000
Implementation	1984	1991	1999	2002	2012
Services	Analog voice	Digital voice	Higher capacity packetized data	Higher capacity, broadband	Completely IP based
Data rate	1.9. kbps	14.4 kbps	384 kbps	2 Mbps	200 Mbps
Multiplexing	FDMA	TDMA, CDMA	TDMA, CDMA	CDMA	OFDMA, SC-FDMA
Core network	PSTN	PSTN	PSTN, packet network	Packet network	IP backbone

LTE Architecture

- **evolved NodeB (eNodeB)**
  - **Most devices connect into the network through the eNodeB**
- **Evolution of the previous 3GPP NodeB (~2G BTS)**
  - **Uses OFDM instead of CDMA**
- **Has its own control functionality**
  - **Dropped the Radio Network Controller (RNC - ~2G BSC)**
  - **eNodeB supports radio resource control, admission control, and mobility management (handover)**
  - **Was originally the responsibility of the RNC**



Evolved Packet System

- Overall architecture is called the Evolved Packet System (EPS)
- 3GPP standards divide the network into
- Radio access network (RAN): cell towers and connections to mobile devices
- Core network (CN): management and connectivity to other networks
- Each can evolve independently
  - » Driven by different technologies: optimizing spectrum use versus management and control or traffic

Evolved Packet System Components

- Long Term Evolution (LTE) is the RAN
  - » RAN: Radio Area Network
  - » Called Evolved UMTS Terrestrial Radio Access (E-UTRA)
  - » Enhancement of 3GPP's 3G RAN
  - » eNodeB is the only logical node in the E-UTRAN
  - » No Radio Network Controller (RNC)
- Evolved Packet Core (EPC)
  - » Operator or carrier core network –core of the system
- Traditionally circuit switched but now entirely packet switched
  - » Based on IP - Voice supported using voice over IP (VoIP)

Design Principles of the EPS

- Packet-switched transport for traffic belonging to all QoS classes
  - » Voice, streaming, real-time, non-real-time, background
- Comprehensive radio resource management
  - » End-to-end QoS, transport for higher layers
  - » Load sharing/balancing
  - » Policy management across different radio access technologies
- Integration with existing 3GPP 2G and 3G networks
- Scalable bandwidth from 1.4 MHz to 20 MHz
- Carrier aggregation for overall bandwidths up to 100 MHz

Evolved Packet Core Components

- Mobility Management Entity (MME)
  - » Supports user equipment context, identity, authentication, and authorization
- Serving Gateway (SGW)
  - » Receives and sends packets between the eNodeB and the core network
- Packet Data Network Gateway (PGW)
  - » Connects the EPC with external networks
- Home Subscriber Server (HSS)
  - » Database of user-related and subscriber-related information
- Interfaces
  - » S1 interface between the E-UTRAN and the EPC
    - – For both control purposes and for user plane data traffic
  - » X2 interface for eNodeBs to interact with each other
    - – Again for both control purposes and for user plane data traffic