COMP327
Mobile Computing
Session: 2012-2013

Lecture Set 5 - Wireless Communication

In this Lecture Set

- Review of the Evolution from 2G to 3G
- 2G Communications
  - History, Multiplexing and Handoff
  - GPS / GPRS
  - Circuit Switching vs Packet Switching for Data
- 3G technologies
  - EDGE
  - WCDMA/UMTS
  - HSPA and future technologies
- Emerging 4G Technologies
  - WiMAX
  - LTE

Evolution from 2G to 3G

- Fixed and Wireless Telecoms, and the Internet have evolved greatly since the mid 90ies
  - This has shaped both device capabilities, and demands on mobile computing
- Evolution of Mobile voice and data communication can be reviewed over the following periods:
  - First Half of the 90ies: *Voice-centric Communication*
  - Between 1995 and 2000: *The Rise of Mobility and the Internet*
  - Between 2000 and 2005: *Dot Com Burst, Web 2.0, Mobile Internet*
  - From 2005 to today: *Global Coverage, VoIP and Mobile Broadband*

First Half of the 90ies: Voice-centric Communication

- In the early 90ies, Internet Access was limited!
  - Mainly universities or IT companies
  - Connection was typically through dial-up at 9.6kbit/s...
  - ...but not widespread!
- Telecommunications were mainly voice-centric
  - Expensive to use; mobile devices were bulky and business oriented
  - Few Fixed-Line telecom companies - mainly monopolies
  - Wireless roaming was difficult, due to propriety systems
  - GSM (Global Systems for Mobile Communications) was launched in 1992, but few people noticed!!!

Between 1995 and 2000:
The Rise of Mobility and the Internet

- In 1998, many European telecom monopolies came to an end
- "Faster" Fixed-Line analog modems emerged (up to 56kbit/s)
  - Early consumer adoption of home internet (though still mainly business and students)
  - Web Browsers evolved and became more commonplace
  - Content was mainly top-down from Big News and Company to consumer (Web 1.0)
- Due to GSM (in Europe), mobiles moved from a business luxury to an indispensable consumer good.
  - Mobile Phone tariffs reduced sufficiently to stimulate mass market adoption
  - SMS text messaging became available, initially through GSM
- GSM data rates of 9.6kbit/s and 14.4kbit/s over circuit-switched connections
  - Early PDAs provided limited (but costly) Internet access - typically via Infrared connections to users' mobile phones

Between 2000 and 2005: Dot Com Burst, Web 2.0, Mobile Internet

- Several Important Developments:
  - DSL (Digital Subscriber Lines) and TV Cable Modems
    - Offered 1Mbit/s speeds, replacing older dial-up connections
    - Graphical content could be downloaded easier, and thus was more prevalent
    - Blogs and Wikis appeared, changing the balance from users as content consumers, to users as content providers (Web 2.0)
  - Internet telephony and VoIP
    - Faster fixed-line networks supported Skype and cheap international calls
    - Emergence of *Analog-Phone-to-IP* converters which used SIP (Session Initialisation Protocol) to make calls over the internet
    - Gateways supported connections to more traditional phone networks
  - GPRS (General Packet Radio Service) and early 3G appeared...

Between 2000 and 2005: Dot Com Burst, Web 2.0, Mobile Internet

- GPRS (General Packet Radio Service) was introduced in 2001 over GSM networks
  - Given that, prior to this...
    - Internet access was through circuit-switched data calls
    - Not really suitable for most Internet applications
    - Most devices had small, monochrome displays
  - ... early wireless internet services were WAP 1.0 based.
  - However, by 2005...
    - High resolution colour displays matured with image capture capability
    - WAP 2.0 browsers and easy-to-use email clients became available
    - GPRS enabled a packet-switched transport layer
  - ... leading to mass market demand and consumption of internet services

Between 2000 and 2005: Dot Com Burst, Web 2.0, Mobile Internet

- 3G networks came online in 2004/2005
  - GPRS provided similar speeds as fixed-line Dial-Up (analog modem) connections
    - Although slow, charging was now based on data, not time
  - 3G UMTS (Universal Mobile Telecommunications System) provided faster speeds...
    - ... and hence a similar experience to fixed-line DSL (broadband) connections
      - Faster data access - up to 384kbits/s
  - However, high prices prevented large-scale adoption for several years

From 2005 to today: Global Coverage, VoIP and Mobile Broadband

- Use (and speed) of broadband DSL has continued to rise
  - Download Speeds can approach 15Mbit/s for users near central exchanges
- Increase in the use of VoIP via broadband
  - Circumvents traditional analogue telephone networks, leading to a decline in fixed-line telephony customers
- High adoption of mobile devices (3 billion users as of 2009)
  - Mainly due to rollout of GSM/GPRS networks in emerging markets
  - Lead to economies of scale and competition between network vendors
    - Cheaper phones and cheaper tariffs...!

From 2005 to today: Global Coverage, VoIP and Mobile Broadband

- 3G Networks have also evolved in Industrialised Countries
  - First upgrades to UMTS in 2006 to HSDPA (High Speed Data Packet Access), with speeds of 1-3 Mbits/s
  - Takeup of 3G devices improved after 2007
    - Mainly due to falling tariffs, with increasing monthly transfer volumes
    - Packages supporting occasional Internet access for Laptop/Desktops through 3G dongles started to appear
      - As of 2007, mobile data revenues accounted for more than 30% of total operator revenue in countries such as Italy and the UK!
    - Wireless Data Roaming is still prohibitively expensive (up to £6/MB)
      - However, pre-paid SIMs for wireless Internet access are available (150 MB per week for 3 Euros in Italy, for example)

For more info on pre-paid data sims, check out:
http://prepaid-wireless-internet-access.wetpaint.com/

Challenges beyond 3G

- Several trends will necessitate increased bandwidth beyond 3G networks
    - Rising usage due to falling prices
    - Ubiquity of multimedia content (both upstream and downstream)
    - Uptake of Mobile Social Networks such as Facebook and Twitter
    - Voice over IP; adoption is slow, but mirroring Fixed-Line adoption
    - Replacement of Fixed-Line Internet (DSL, Cable, etc)
    - The "personal internet bubble" is leaving traditional locations (WiFi enabled homes, cafes, offices etc), and becoming ubiquitous
        - Creating new demands on applications, and hence data access

What is so special about Mobile Communication?

- Many challenges not found in Fixed-Line Networks:
  - Unpredictable medium
    - Intermittent or noisy connections, and high error rates
  - Low Bandwidth
  - Shared Medium and Limited Spectrum
    - Users have to share the same "airwaves"
  - Security Challenges
    - Early Analog systems were easy to eavesdrop
  - Mobility Challenges
    - As users move from one area to another, networks need to ensure continuity of service (often between one standard to another)
- Devices themselves are resource poor (battery, processor, etc)
  - Different activities have differing QoS requirements (e.g. voice vs email)

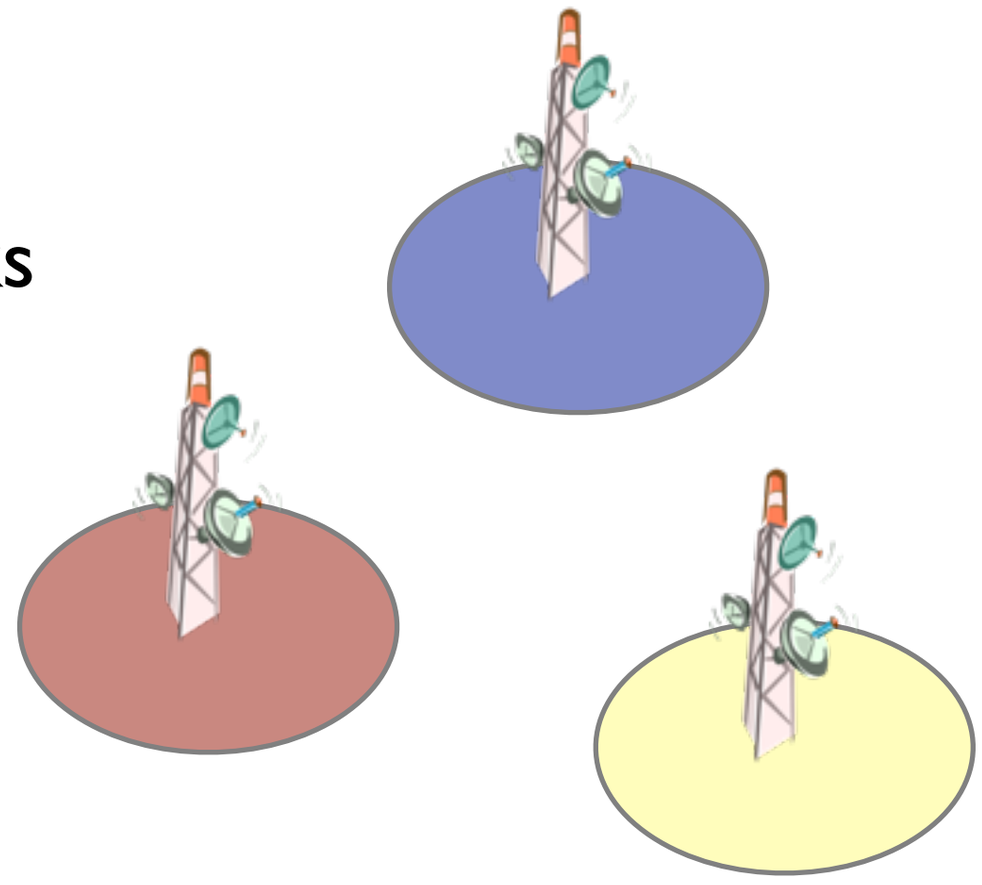
Basic Multiplexing Schemes

- Communication between the phone and the base station in a given area or *Cell* exists for a given time over some frequency band using some encoding

- One of the main distinguishing features of different networks is how they separate users:
  - Space Division Multiplexing (SDM)
  - Frequency Division Multiplexing (FDM)
  - Time Division Multiplexing (TDM)
  - Code Division Multiplexing (CDM)

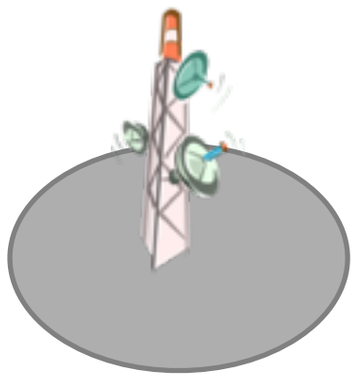
Space Division Multiplexing (SDM)

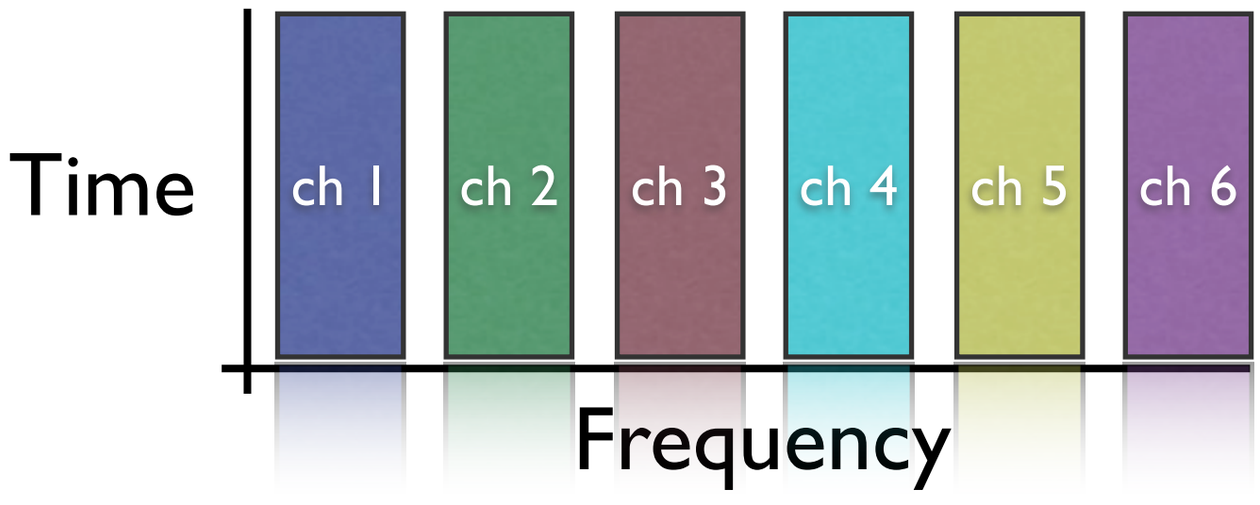
- Involves separating users based on their location
  - Simple approach which works with non-adjacent cells
  - Relies on the power of the signal being too weak to reach next cell, to avoid interference



Frequency Division Multiplexing (FDM)

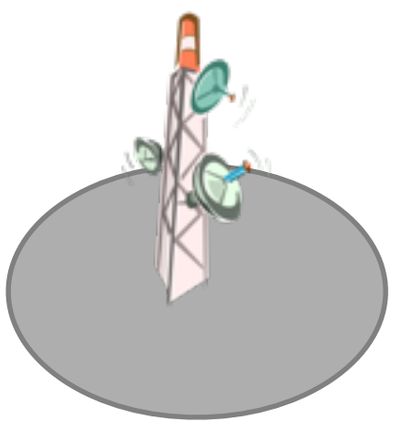
- Involves partitioning the available spectrum into frequency bands
  - Analogous to analog radio stations
  - Each user is allocated a different frequency
    - Users typically only need short periods of airtime
    - Hence, highly inefficient when used in isolation
- Disadvantage:
  - Crosstalk can cause interference on other frequencies and may disrupt the transmission

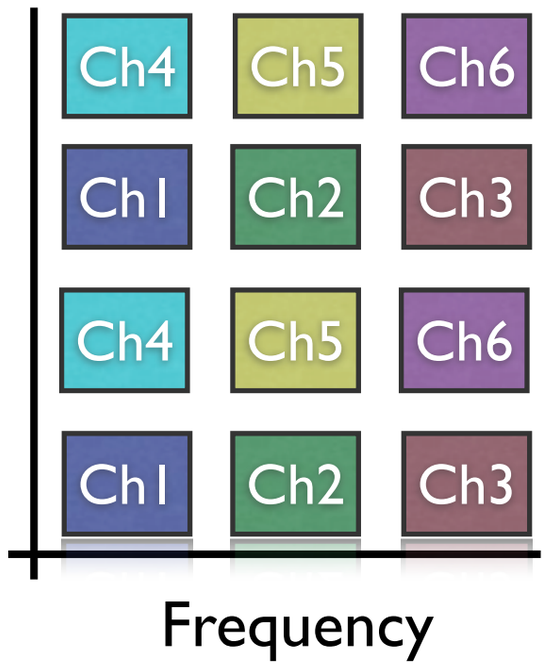




Time Division Multiplexing (TDM)

- Allows users to share a given frequency band, as long as this is used at different times
  - The time domain is divided into several recurrent time slots of a fixed length
    - One for each time channel
  - Requires coordination between mobile stations (via the base station)
  - Is typically combined with FDM (and SDM), where each user gets a short time slot for their allocated frequency
    - Thus, the same frequency can be shared by different users
  - More advanced combinations are used in GSM





Code Division Multiplexing (CDM)

- Allows users to use different coding schemes to different channels
  - Also known as Synchronous CDMA
  - Codes designed to minimise interference with other users
    - The two ends of a given communication channel share the same code
  - Allows many users to simultaneously share frequencies at the same time
    - Coding scheme includes inherent security
  - However, this approach is more complex

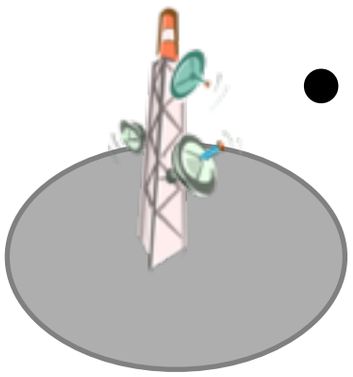
Analogy - Crowds of chatting people

- Imagine having a number of people, who want to talk to each other in a crowd!
  - Space Division Multiplexing (SDM)
    - Equivalent to spreading out each group of people out so they can't hear their neighbours
  - Frequency Division Multiplexing (FDM)
    - Equivalent to different groups talking at different pitches in the same room
  - Time Division Multiplexing (TDM)
    - Equivalent to different groups each taking turns to talk
  - Code Division Multiplexing (CDM)
    - Equivalent to speaking in different languages, where each group only understands one language

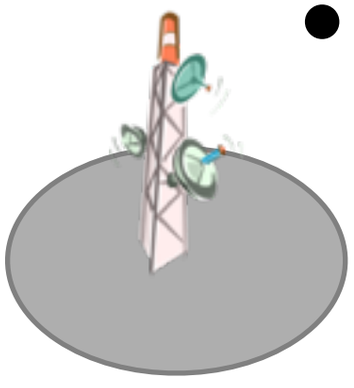
Uplink vs Downlink Traffic

- In addition to separating channels between users
  - Need to separate uplink (phone to base station) and downlink traffic (base station to phone)
- Two general approaches
  - Time Division Duplex (TDD)
    - Different time slots are given to uplink and downlink whilst using the same frequency band
      - Used in Bluetooth communication.
  - Frequency Division Duplex (FDD)
    - Different frequencies are allocated to the downlink and uplink streams
      - Used in GSM

Handover or Handoff



- This refers to the process of transferring a call or data session from one channel to another
  - A phone is moving from one cell to another
  - The capacity of current cell is exhausted, and the phone is in an overlapping cell with excess capacity
  - Interference between channels occurs
  - Change of user behaviour
    - e.g. from fast travelling (served by a larger "umbrella" cell) to stationary (served by a "macro" or "micro" cell)



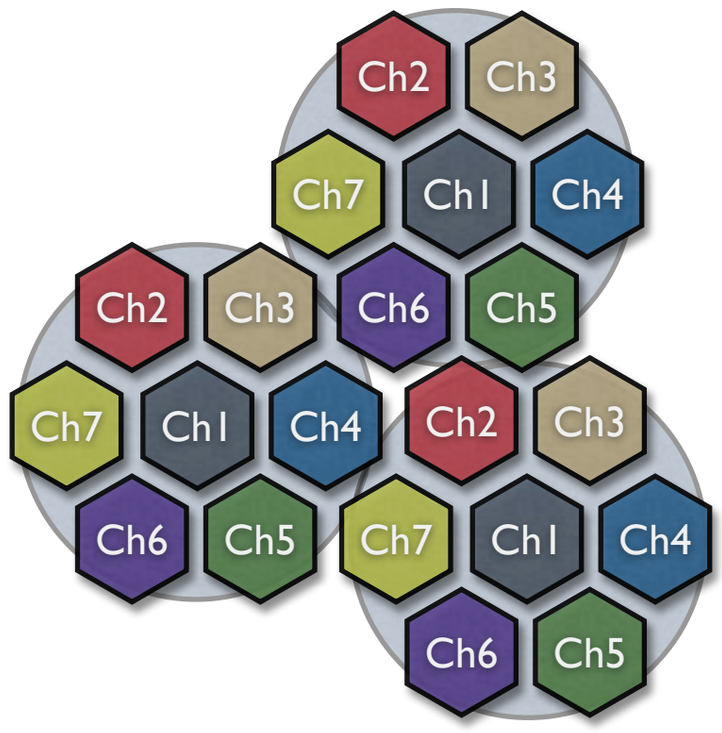
- Both Phone and old/new cells monitor parameters of the signal in the channel to determine if/when to handoff

Handover or Handoff

- Two methods of handoff exist
  - Hard Handoff (*break-before-make*)
    - The channel in the source cell is released before the channel in the target cell is engaged.
    - Typically instantaneous, but will fail if the new channel fails
    - Used by GSM
  - Soft Handoff (*make-before-break*)
    - A new channel is engaged and the old channel is only released when the new connection is considered reliable.
    - Both channels may be held for some time
      - The best signal from any used channels will be used at any moment
    - Requires more sophisticated and expensive technology
    - Reduces cell capacity whilst multiple channels are used
    - Used by UMTS

Pre 2G Networks: AMPS and the first mobile phones

- AMPS (Advanced Mobile Phone System) was introduced in the USA in 1983
  - Geography was divided into "cells" (aprox 10-20km across), using different frequencies
    - Smaller cells mean lower power usage
    - Frequencies could be reused in non-adjacent cells
      - "Back End" call setup would select frequencies based on location, supporting a larger number of phones
      - Initially, each carrier had 333 channels, which grew to 416 by 1989 to increase capacity for a growing user base
- Communication was analogue, thus prone to eavesdropping, static and noise
  - Also prone to cloning using a scanner!!!



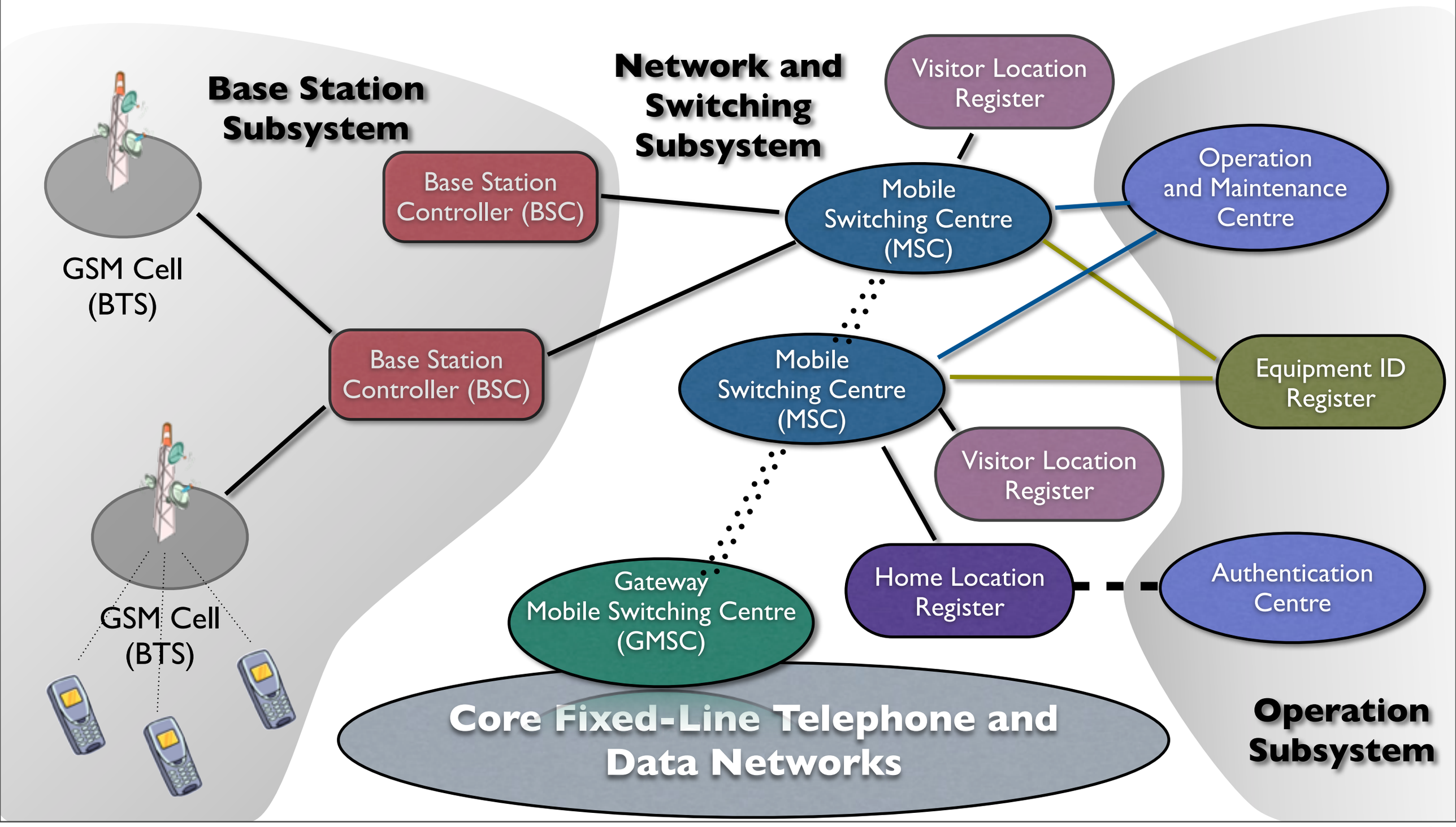
From Analog (1G) to Digital (2G)

- There were many advantages in moving from Analog to Digital Networks...
  - Digitised voice could be compressed
  - Voice transmission could be included with other media (fax, data etc)
  - Control signals and digitised voice / data could be encrypted
  - Error correction could be used to improve transmission quality
- In the USA, early 2G network designs were made backwardly compatible
  - Could use 1G networks where no 2G coverage was available
  - A digital form of AMPS (now referred to as TDMA) was developed to exploit the existing AMPS infrastructure
  - cdmaOne exploited CDM and appeared in the USA, Korea, Japan and other countries
- In Europe, most countries differed in the 1G technology, so backward compatibility was untenable
  - To facilitate Roaming, a joint standard (GSM) was developed, to complement the existing Fixed-Line ISDN (Integrated Services Digital Network)

GSM
Global System for Mobile communications

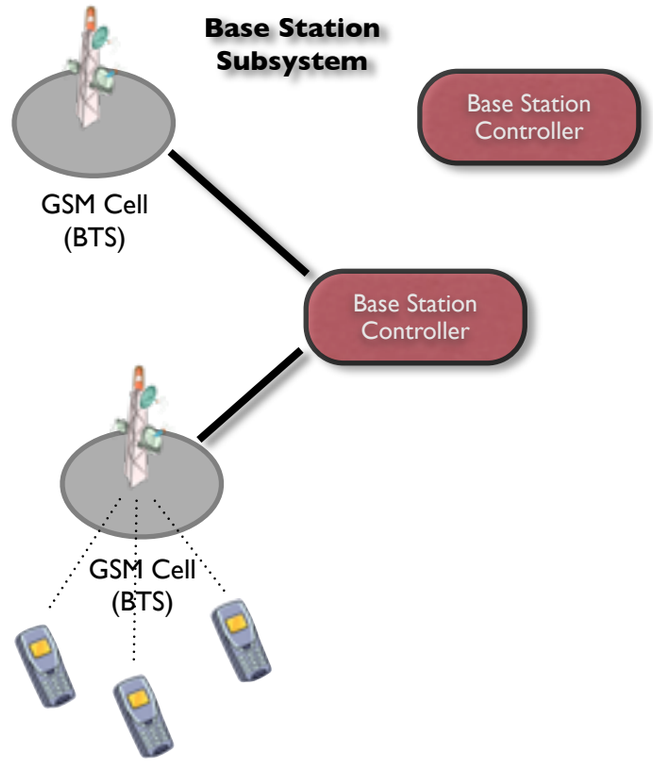
- Currently the most popular standard for mobile phones
  - Over 80% of the global market (July 2009), making roaming easy
- Several key features and innovations
  - Signalling and Speech channels are digital
  - Circuit-switched data services (upto 14.4kBit/s)
  - Authentication Infrastructure based on SIM cards
  - Encryption on the wireless link to prevent eavesdropping
  - Efficient integration with ISDN, through Mobile Switching Centres (MSC)
  - Voice Mail, Call Waiting and other telephony services available
  - SMS (Short Messaging Service) and CB (Cell Broadcast)
  - Single Worldwide Emergency Telephone Number (112)
- GSM EDGE is considered a 3G variant of the GSM protocol

GSM System Architecture



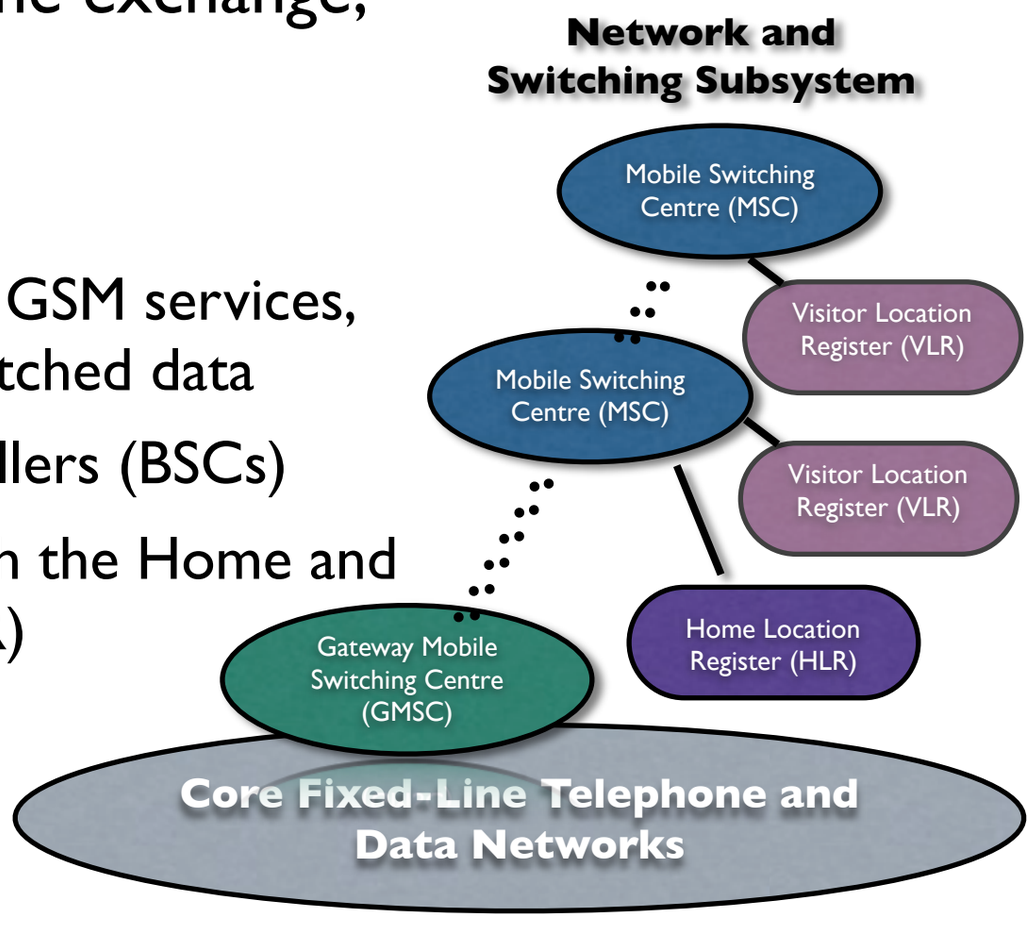
GSM Base Station Subsystem

- Includes all elements responsible for the air interface
  - GSM Cell, or Base Transceiver Station (BTS) responsible for encrypting and decrypting communications with mobile devices
  - Base Station Controller (BSC) manages many BTSs, including:
    - allocation of frequencies
    - handover from BTS to BTS
    - managing DBs of carrier frequencies, frequency hopping lists, power reduction levels, and receiving levels for cell border calculation



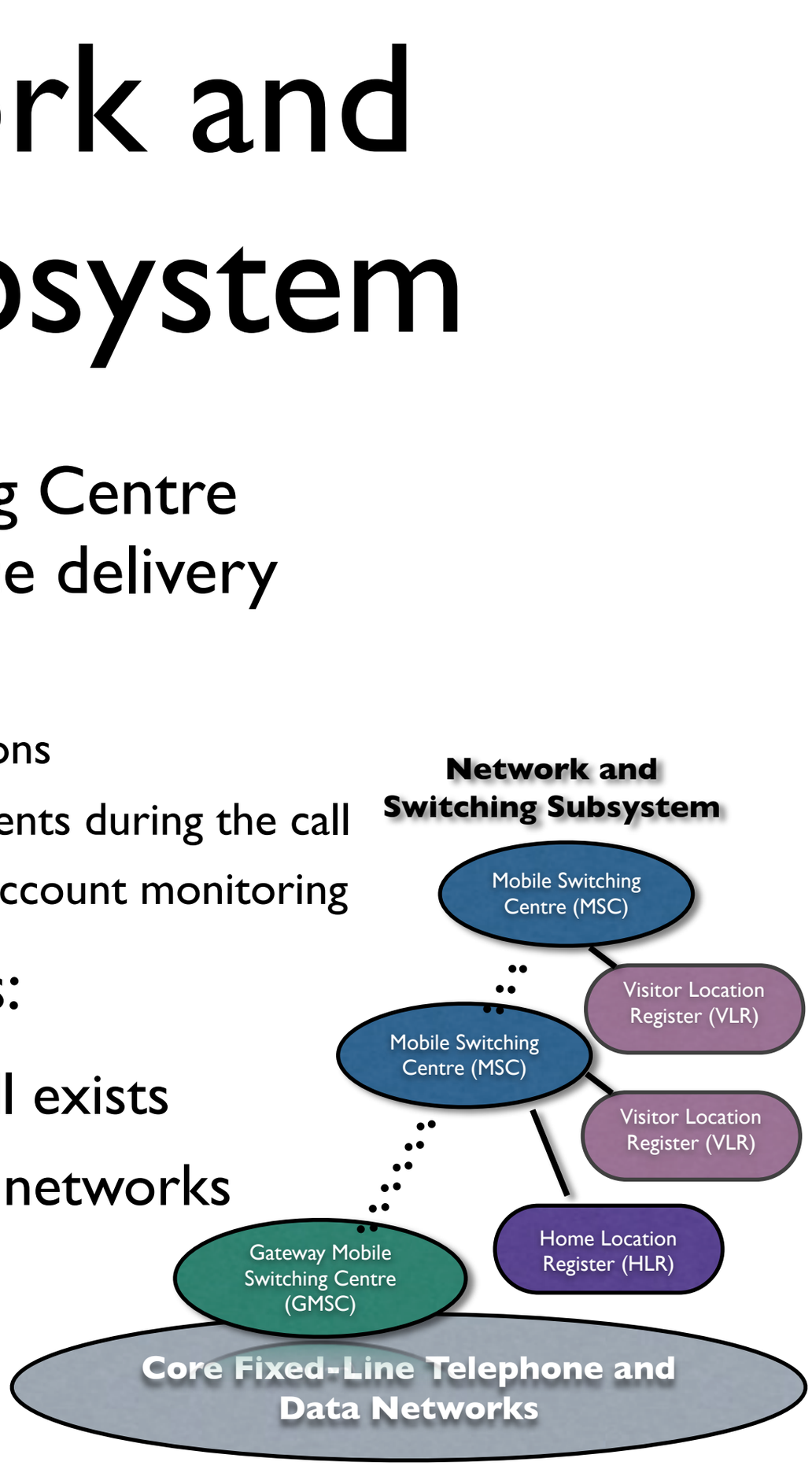
GSM Network and Switching Subsystem

- Carries out switching functions and manages communications between mobile phones and core telephone and data networks
  - e.g. PSTN, ISDN, X.25 etc
- Closely resembles Fixed-Line telephone exchange, with mobility management support
- Responsible for:
  - Circuit-switched core network used for GSM services, including voice calls, SMS, and circuit-switched data
  - Handover between Base Station Controllers (BSCs)
  - Management of user information through the Home and Visitor Location Registers (HLR and VLR)



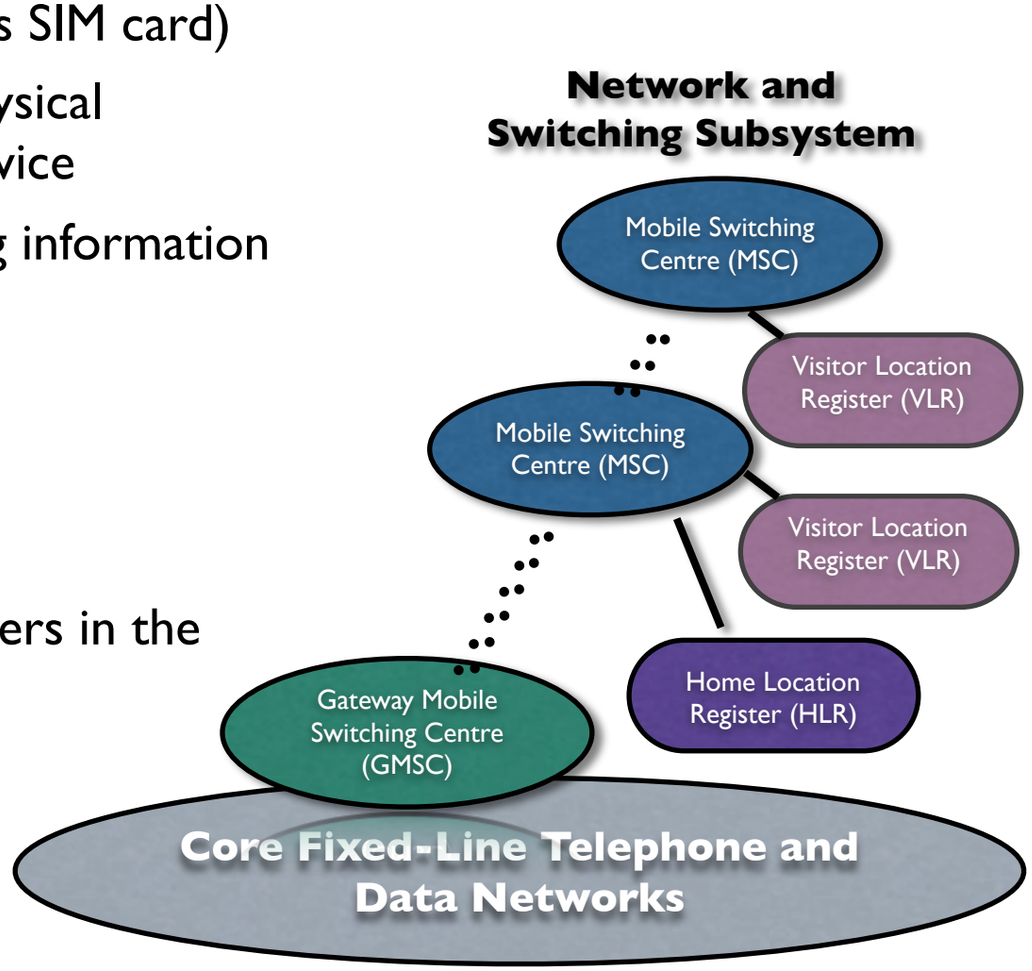
GSM Network and Switching Subsystem

- Each Mobile Services Switching Centre (MSC) acts as a primary service delivery node
  - Sets up and releases end-to-end connections
  - Handles mobility and hand-over requirements during the call
  - Manages charging and real-time pre-paid account monitoring
- The Gateway MSC determines:
  - in which MSC a recipient of a call exists
  - how to route calls to Fixed-Line networks



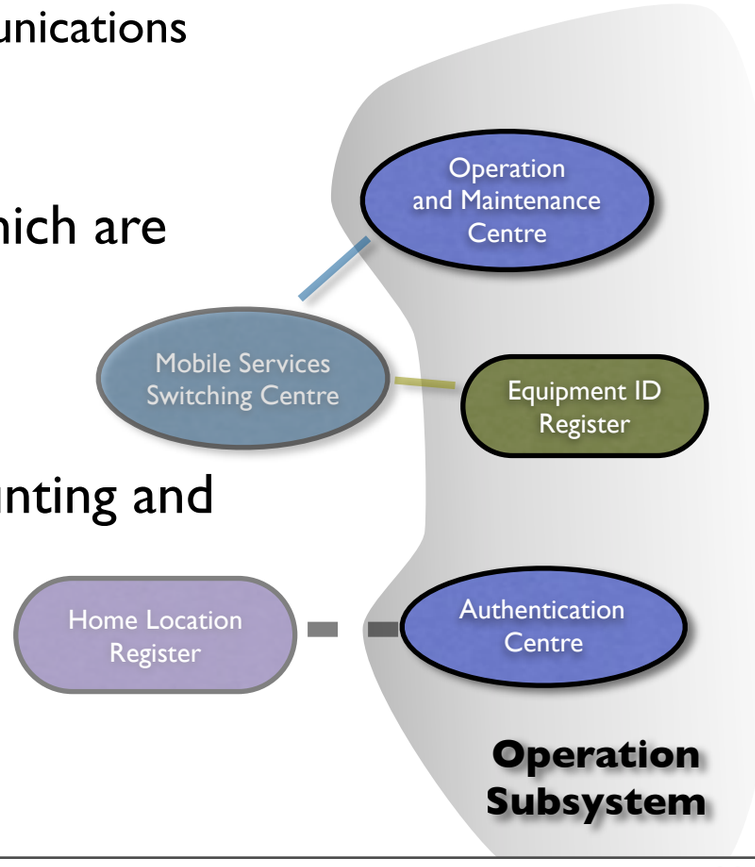
GSM Network and Switching Subsystem

- Home Location Register (HLR)
  - Network-specific repository of all network's user information
    - User's static information, including telephone number & authentication key (also found on the user's SIM card)
    - User's dynamic information, such as the physical location (and relevant cell) of the user's device
    - Also used to support billing and accounting information such as roaming
- Visitor Location Register (VLR)
  - Each MSC is connected to a VLR
    - Stores a copy of user information for all users in the area associated with an MSC



GSM Operation Subsystem

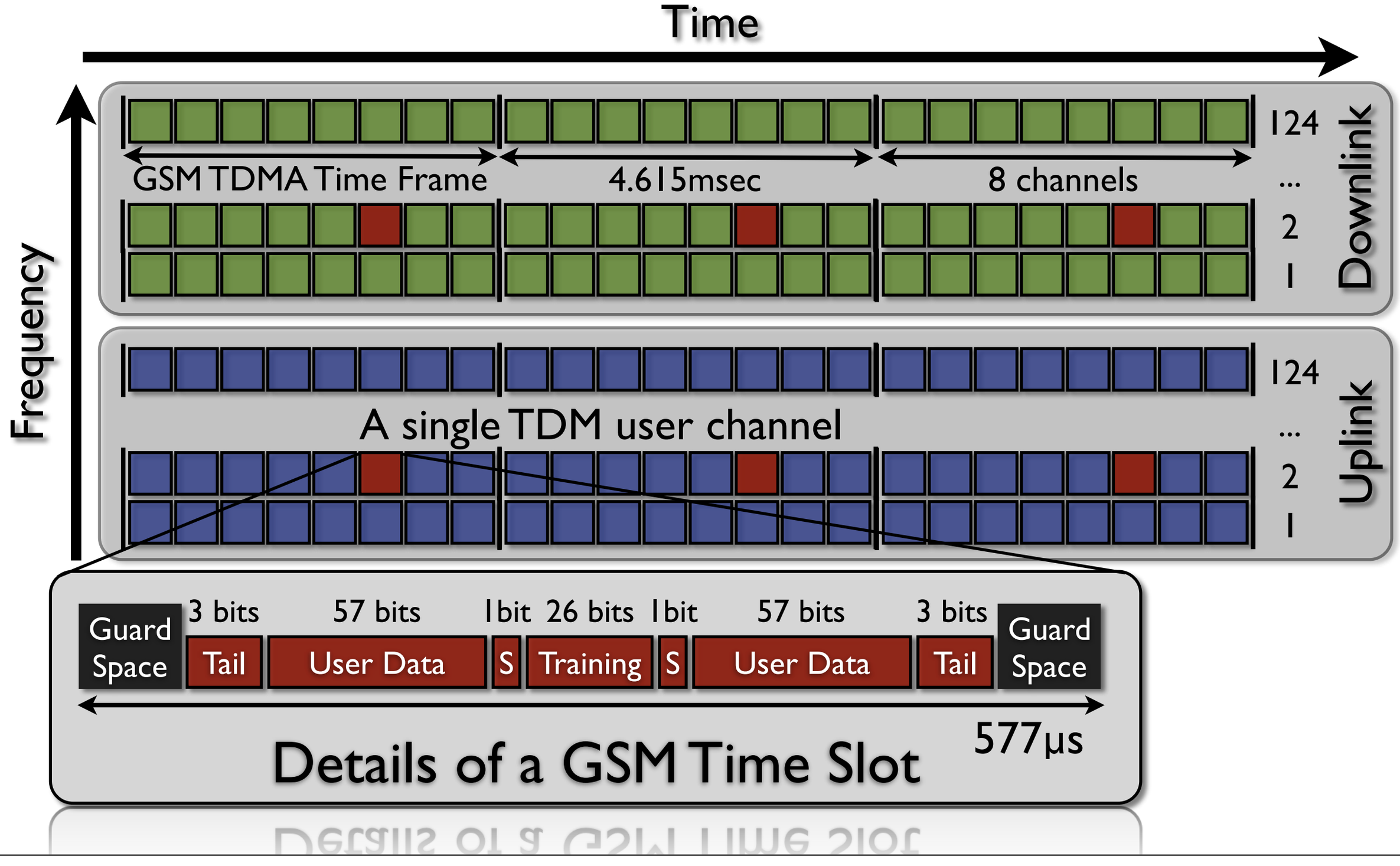
- Responsible for network operation and maintenance activities:
  - Authentication Centre (AC)
    - Authenticates SIM cards that connect to the network
    - Once successful, the HLR manages the user's SIM information
    - Also generates an encryption key for all wireless communications
  - Equipment Identity Register (EIR)
    - Maintains a list of phones identified by their IMEI which are banned or to be monitored
  - Operations and Management Centre
    - Manages traffic monitoring, status monitoring, accounting and billing



GSM Multiplexing

- GSM uses a combination of TDM and FDM
  - Time Frames consist of 8 slots
    - Typically, 2 slots are used for signalling
  - Frequency divided into 248 bands
    - 124 each for uplink and downlink
- Each slot consists of:
  - Guard Spaces to separate each slot
  - Tail bits to further separate each data packet
  - Training bits to adjust parameters at receiver to improve communication
  - Two 57 bit data segments

GSM Multiplexing

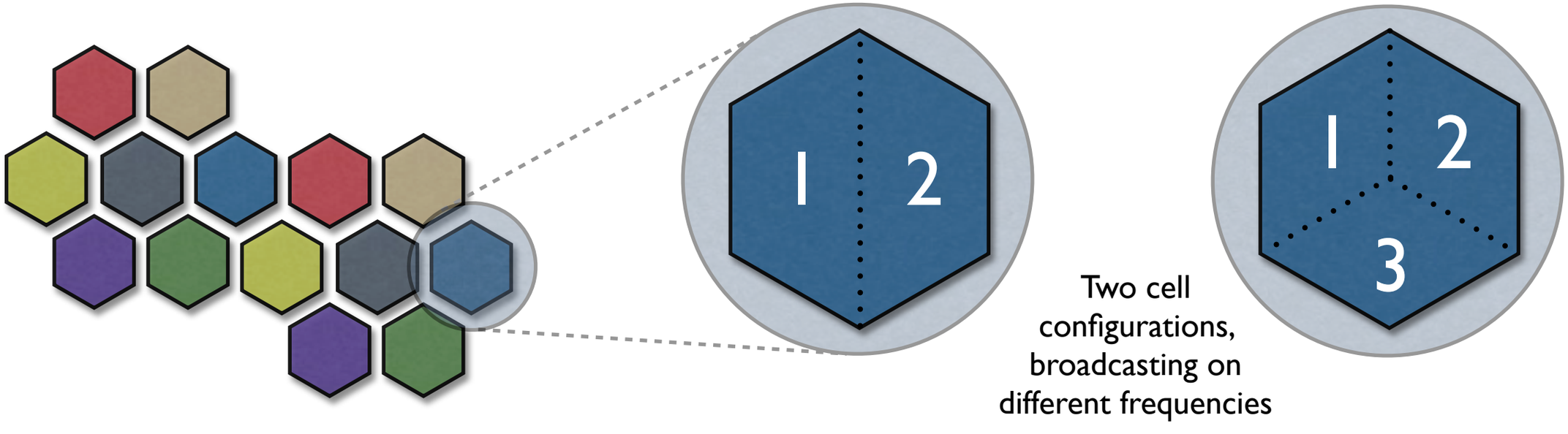


GSM BTS Cells

- The GSM Base Transceiver Stations are the most numerous components of a network
  - e.g. in the UK, each operator has well over 10,000 base stations
- In theory, it can cover an area of up to 35km (known as a cell)
  - However, it can only cover a limited number of users
  - Therefore cell size is normally determined by user density
    - Radius of 3-4 km in residential and business areas, down to 100m in shopping areas and city centres
  - Transmission power is also dependent on cell size, and can be a limiting factor
    - Even in rural areas, transmission power of 1-2 watts can limit cells to 15km
    - However, in city centres, this can be significantly lower due to small cell size

GSM BTS Cells

- A form of space division multiplexing is used to avoid interference
  - Each cell typically only operates on a limited number of frequencies, to avoid interference with its neighbours
  - To increase capacity, the coverage area is usually split into two or three sectors, covered using different frequencies by a dedicated transmitter
    - Improves reuse of frequencies in 2D space, compared to a single frequency per cell.



Cell Capacity

- It is possible to calculate the cell capacity, and hence estimate subscriber provision
- Example scenario
  - Assume a BTS cell is split into 3 sectors, with each sector covered by 2 transmitters and 2 receivers.
  - Also assume that each transmitter/receiver pair uses 1 time slot for signalling, and 2 time slots for GPRS data
- Each GSM channel consists of 8 time slots, with uplink data going to the receiver, and downlink data coming from the transmitter
  - Therefore each transmitter/receiver pair has 5 time slots for voice calls
  - Given that there are two transmitter/receiver pairs in each sector, with three sectors in the cell, **the cell capacity is (5x2x3 =) 30 simultaneous subscribers.**
- Not all subscribers communicate at the same time.
  - Mobile providers use a "*theoretical call profile model*" to determine the number of minutes on average a subscriber uses per hour.
  - If this profile states that for an hour, the average use is 1 min, then a cell can support 60 times the number of active subscribers.
  - **Hence, the subscriber provision per cell is (30x60 =) 1800 subscribers.**

Case Study

Vodafone Germany had a subscriber base of aprox 25 million in 2005. By dividing this number by the subscriber provision per cell, the number of BTSs needed can be calculated.

Given the figures opposite, this would be aprox 14,000, which is in line with the number of actual BTs used by Vodafone Germany!!!

SIM
(Subscriber Identity Modules)

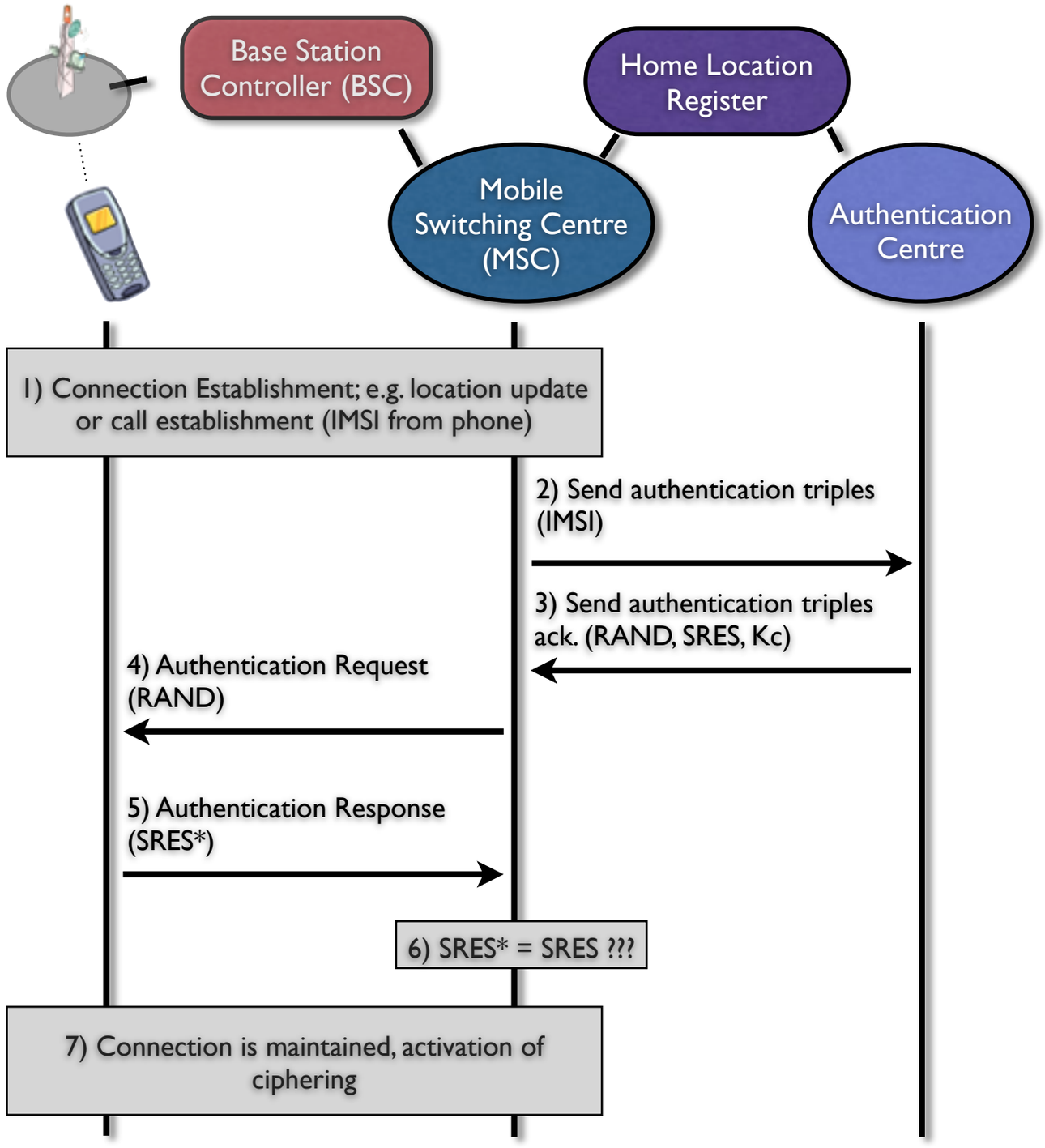
- Smart cards that are inserted into the GSM phone to identify the user
  - Stores the service subscriber key (IMSI)
    - Used to obtain details of the mobile from the Home Location Register (HLR)
    - Not the same as the IMEI (International Mobile Equipment Identity)
  - Stores security authentication and ciphering information
    - 128-bit authentication key which is used to sign carrier data by the SIM itself
  - Stores temporary information related to the local network
  - Stores two passwords
    - PIN for usual use (to prevent unauthorised use)
    - PUK for unlocking lost PIN codes
  - Can also store SMS messages and phone book pairs (name-number tuples)

SIM (Subscriber Identity Modules)

- SIMs can be used by any GSM or UMTS phone
  - However, some phones have a "SIM lock", so that the phone only works with a single SIM or a single operator's SIM
    - Introduced to prevent subsidised phones being used with other networks
- More than just a simple memory card
  - A complete micro-controller system exists to provide additional functionality
    - Not all information is directly accessible from the phone, but must be requested from the SIM's CPU
    - Authentication is done by the SIM
      - the individual key per subscriber (Ki) is stored on the SIM, but is never revealed to the phone.
      - It is sent to the Authentication Centre with the user's IMSI, to generate and verify a signed response
      - This helps to prevent cloning of SIMS by eavesdropping on calls during call initiation
    - Can also be used to execute programs and provide additional services to the phone, and delivering operator specific functions in the phone's menu

GSM Authentication

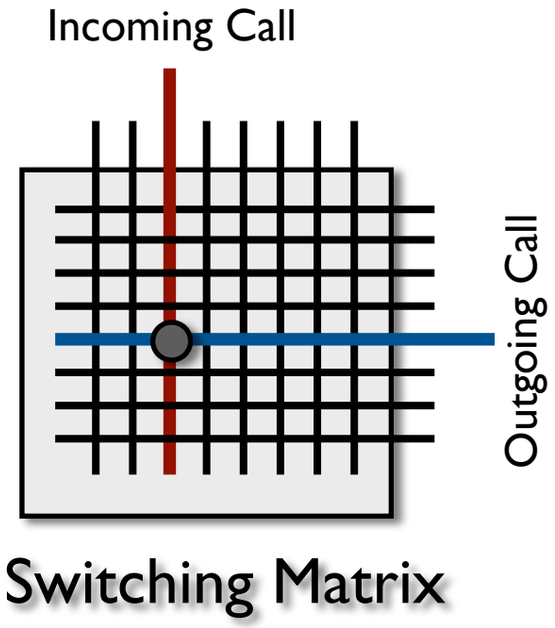
- The IMSI (International Mobile Subscriber Identity) and Ki (individual key per subscriber) are stored on the SIM and the AC.
  - 1) Authentication is initiated when a device establishes a signalling connection
  - 2, 3) The MSC requests an authentication triplet (RAND, SRES, Kc) from the HLR/AC.
    - The signed response (SRES) is generated from the Ki and a random number (RAND) using the A3 authentication algorithm
    - The cyphering key (Kc) is also generated from Ki and RAND.
  - 4, 5) The MSC sends RAND to the device, which uses its own Ki and A3 alg. to generate a second SRES*
  - 6, 7) The MSC verifies the two signed responses are equivalent, before establishing connection
- As the secret key (Ki) is not transmitted, it cannot be eavesdropped. Fresh RANDs are generated for each authentication.



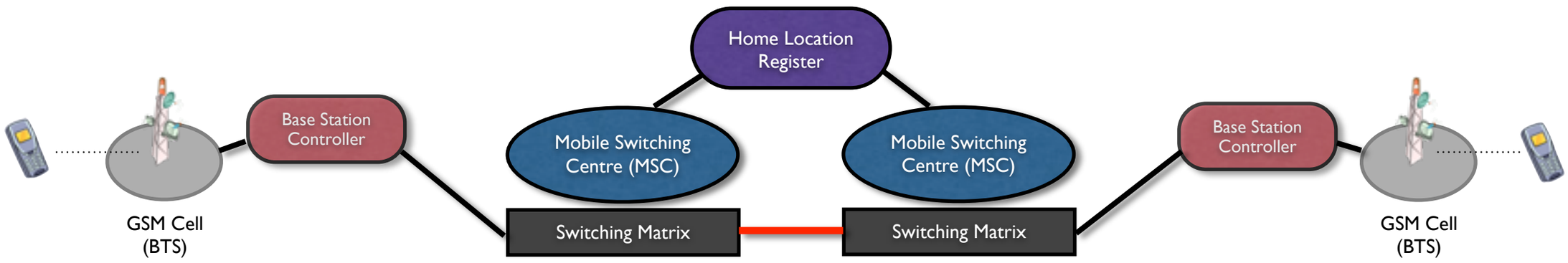
SIM operator functionality examples

- SIMS can offer operator functionality to the user, via the phones GUI
  - Example: Operator News
    - Subscriber can request current news from a menu option.
    - Call input (via the keypad) is forwarded to the SIM.
    - The SIM program generates an SMS message, which is forwarded back to the phone and sent to the network
    - The network responds with one or more SMS messages (containing news overview articles) which are returned to the SIM
    - These articles are then extracted and presented to the user
  - O2 Germany's *Genion*
    - Cheaper calls can be made if the user is in their "homezone"
    - The homezone is defined geographically on the SIM.
    - The SIM requests location information from the connected cell (broadcast using Cell Broadcast - CB)
    - The SIM then compares this with the homezone information. When the user is within this area, the string "Home" or "City" can then be presented on the phone's screen.

Circuit-Switched Data Transmission



- GSM networks originally designed as a circuit-switched network
  - When a call is made, a direct connection is established though a switching centre
    - The conversation is then transmitted via this connection
  - When the call ends, the switching centre frees the connection
- GSM dynamically manages the routing of a call as the user roams between BTSs



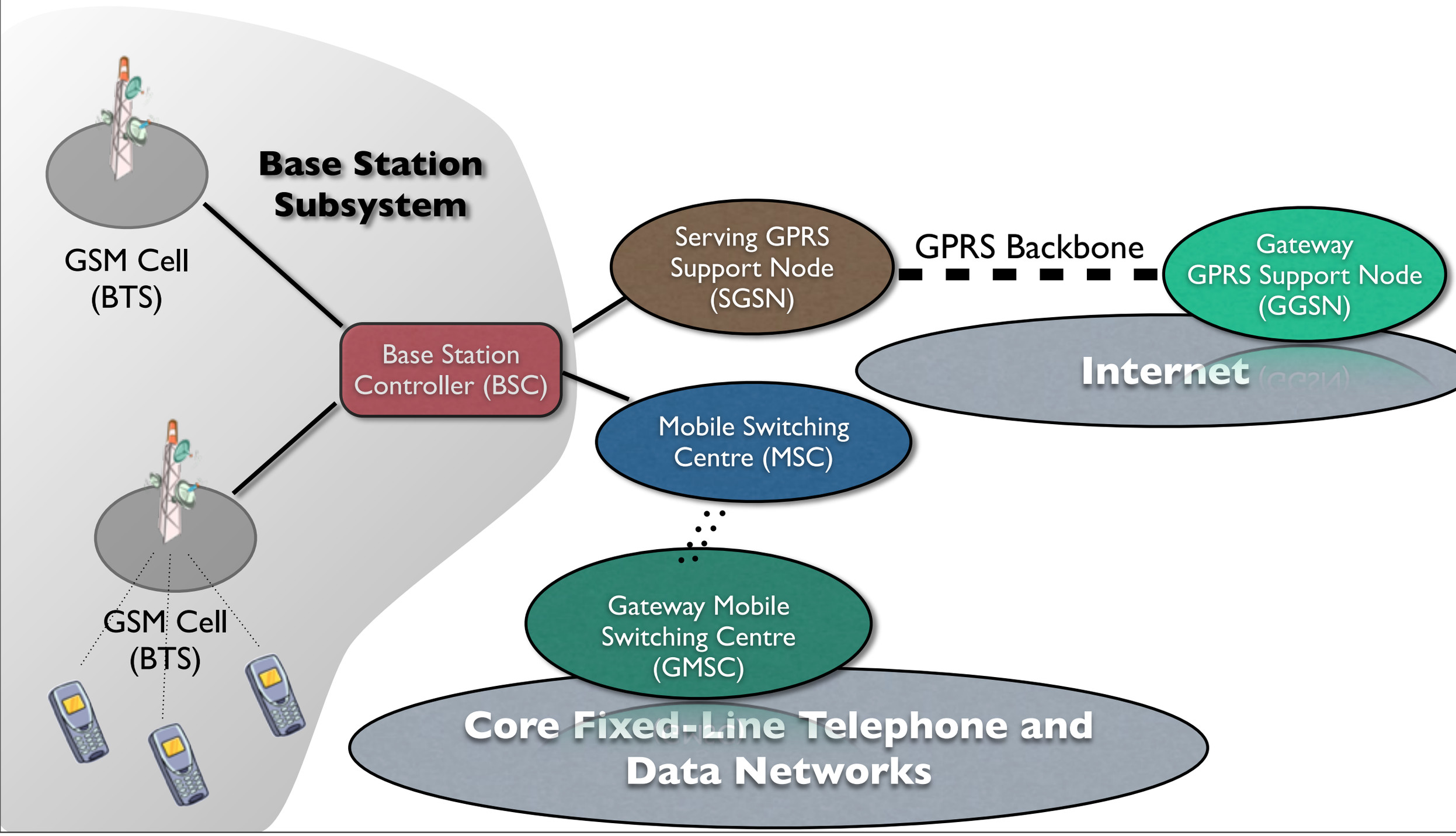
Circuit-Switched Data Transmission

- Circuits are uniquely assigned to each call
  - If no circuit is available, then MSC rejects the call
  - Once the circuit is established, calls cannot influence each other
- However, setup times can be long
  - If a connection is lost, reconnection can take several seconds
- Inefficient use of bandwidth, as the circuit is established for the entire call
  - Unsuited for burst data activity, such as web browsing, email etc
  - Hence high time-based charges for data communication

GPRS and Packet-Switched Data Transmission

- Provides *always-on* packet-switched communication
  - Extends existing GSM networks
  - Channels can be allocated more than 1 time slot per TDMA frame
  - However, this can vary over time to respond to traffic demand
- To update GSM, GPRS requires:
  - Software upgrades to Base Station Subsystem
    - But no hardware updates to Base Transceiver Stations, thus reducing migration cost
  - Hardware/software upgrades to BSCs, inc. Packet Control Unit (PCU)
    - To separate circuit-switched and packet-switched data
  - New Core Network to support packet-switched data
  - Compatible Phones!

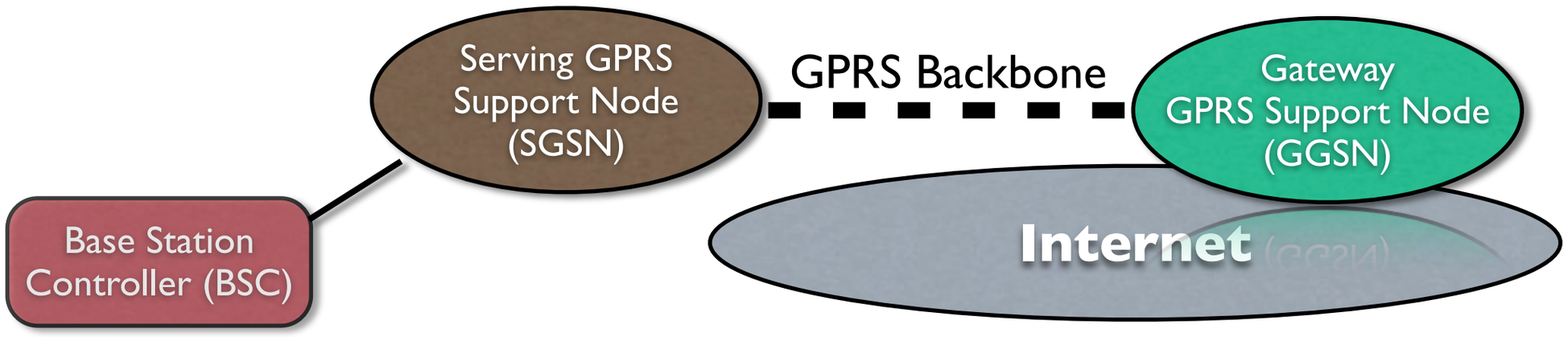
GPRS Overlay System Architecture



Serving GPRS Support Node (SGSN)

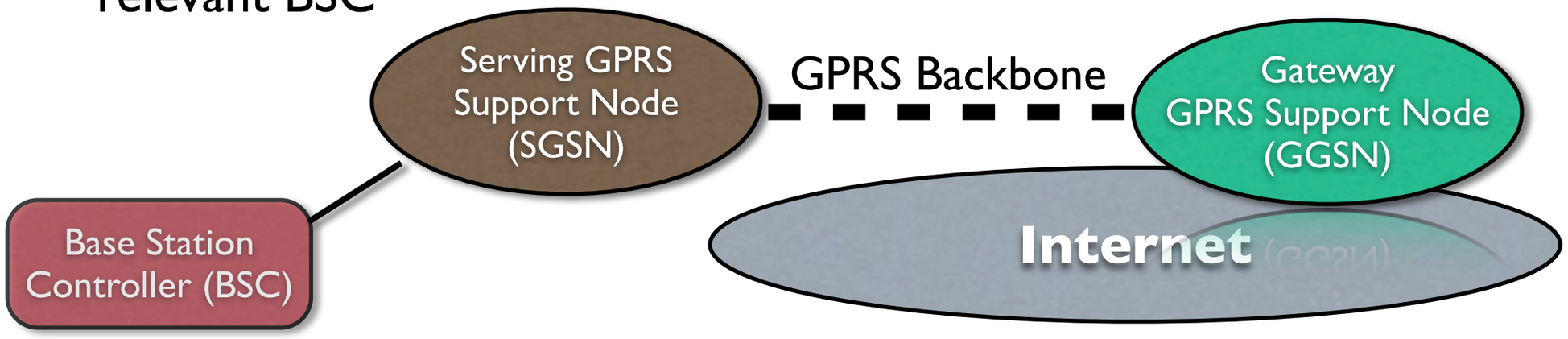
- Keeps track of associated BSC
  - Forwards data to the appropriate BSC as user roams
  - Acts as a router!

- When user moves to a new area (controlled by a new SGSN):
  - Packets buffered by old SGSN are discarded, and new packets are sent to new SGSN



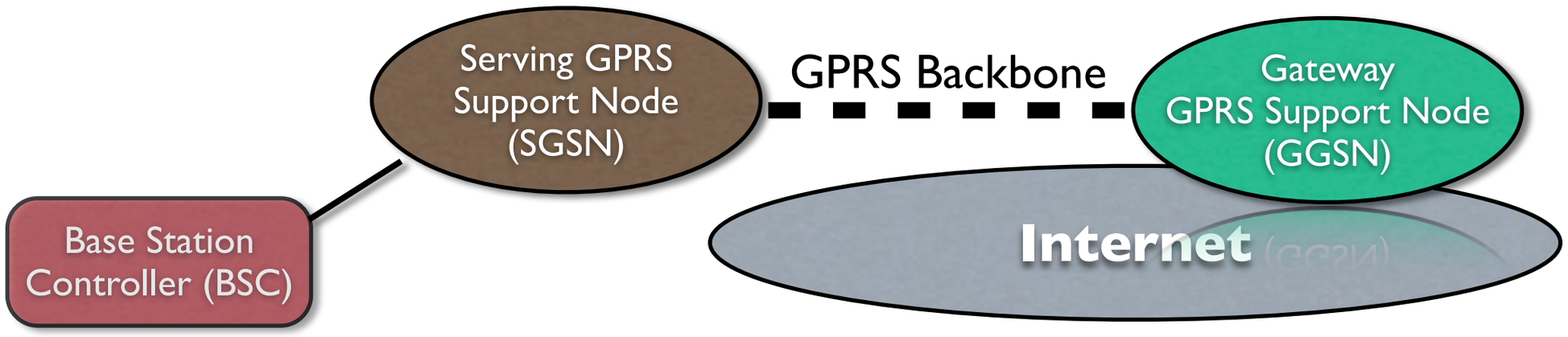
Gateway GPRS Support Node (GGSN)

- Provides an interface between GPRS and Internet
  - Each mobile device appears as a separate IP node
  - Uses the *GPRS tunnelling protocol* to forward packets
    - Packets for a device are encapsulated and sent to GGSN, which then forwards them to the relevant SGSN
    - SGSN retrieves original packet and forwards this via the relevant BSC



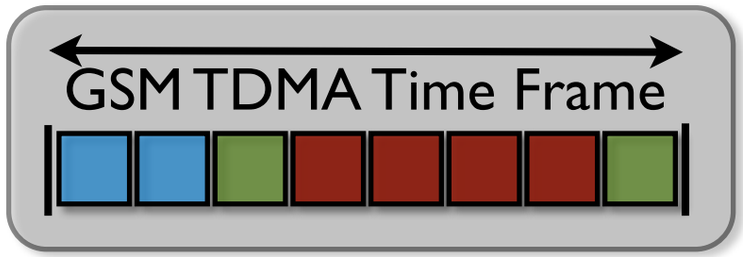
GPRS Backbone

- GPRS Backbone is a regular IP network
- Connects GGSN to different SGSNs and other key components, including...
  - Billing Gateways!!!



GPRS data over multiple GSM time slots

- During a circuit switched call, a subscriber is allocated exactly one channel in a GSM TDMA time frame
  - Allocated for the duration of the call
- For packet switched connections, data is sent as a burst of packets
  - Typically, at least four packets at a time
  - Depending on the volume of data, a single time slot can be used by several subscriber
- If several time slots are available, then multiple slots can be allocated to a single subscriber
  - Thus, transmission speed can be increased
  - Typically, more slots are allocated for downlink than uplink traffic
    - e.g. Multislot class 10 supports up to 4 slots for downlink data, and 2 for uplink data
  - However, using more time slots requires more power, which can affect battery life



Advantages of GPRS

- Faster and more reliable connection establishment
  - GPRS takes about 5 seconds to establish a data connection, rather than 20 seconds to make a GSM circuit connection.
    - GPRS connections are not dropped during handover, or when signal is lost; communication just "pauses"
    - "Always-on" functionality
- Better capacity utilisation
  - Bandwidth is only used by a user when needed, so others can share network capacity
  - As charges based on data usage, not connection times, this results in:
    - More flexible billing options
- Faster data rates
  - By flexibly allocating bandwidth on the air interface, increased data rates are achieved
    - Theoretical speeds are in excess of 100kbit/s
    - Actual data rates are closer to 40kbit/s
- Relatively cheap to deploy!!!

3G, or more formally...
International Mobile Telecommunications-2000 (IMT-2000)

- IMT-2000, or "3G" is a family of standards for mobile telecommunications
  - Includes:
    - GSM EDGE
      - Extends GSM - sometimes reported as a 2.75G technology
    - UMTS
      - Significant improvement on GSM, though much of the core subsystem is reused
    - CDMA2000
      - Evolutionary upgrade to the cmdaOne technology used in the USA
  - Several releases of standards allow 3G to evolve
    - IP Multimedia SubSystem (UMTS Release 5)
    - High Speed Packet Access (HSPA)
      - Consisting of HSDPA (Release 5) and HSUPA (Release 6)

Enhanced Data Rates for GSM Evolution - EDGE

- EDGE extends GSM with a new modulation approach
  - i.e. encoding data for air interface transmission
    - Modulation approach encodes three bits for each signal change (GPRS encoded 1 bit)
    - increases data per slot, yielding 3-4 fold increase in data rate (up to 384kbit/s)
    - modulation and encoding schemes adapt to current radio conditions
    - "Incremental Redundancy" reduces bits sent, whilst retaining good error correction
- Requires only minor upgrades to the GSM infrastructure
  - No hardware / software changes to the GSM core
  - Hardware update for transceiver (BTS), but Base Station Controller (BSC) typically requires only a software upgrade
- Technically a 3G technology
  - Considered a cheaper migration than the more complex UMTS

Incremental Redundancy

- Simple example to illustrate the idea:
  - Imagine wanting to send the following message:

  - The message can be sent with 10 fewer characters, but is still readable

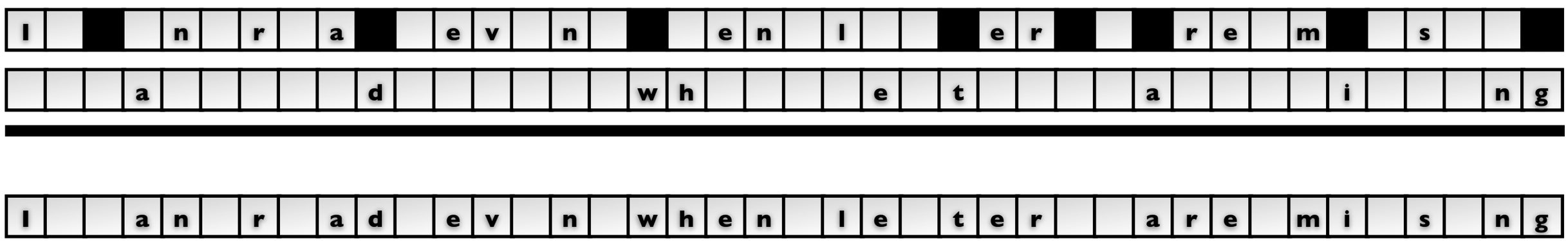
  - But if, due to noise, another 8 bits are lost...

Incremental Redundancy

- The noisy message is unreadable

- Instead of retransmitting the original message, additional bits could be sent

- By adding them together with the original message, a new message can be constructed



Thanks to Dave Shield for the inspiration for these slides on Incremental Redundancy

UMTS

- Follow-on technology from GSM/GPRS
  - Used in most countries
  - Combines circuit-switched voice network with packet-switched data network
- Parts of the network are evolutionary
  - Much of the Core Subsystem form GSM is reused, and upgraded through software updates
- The Air Interface is revolutionary
  - Re-designed from scratch based on faster processors within mobile phones (supporting sophisticated wireless comms)

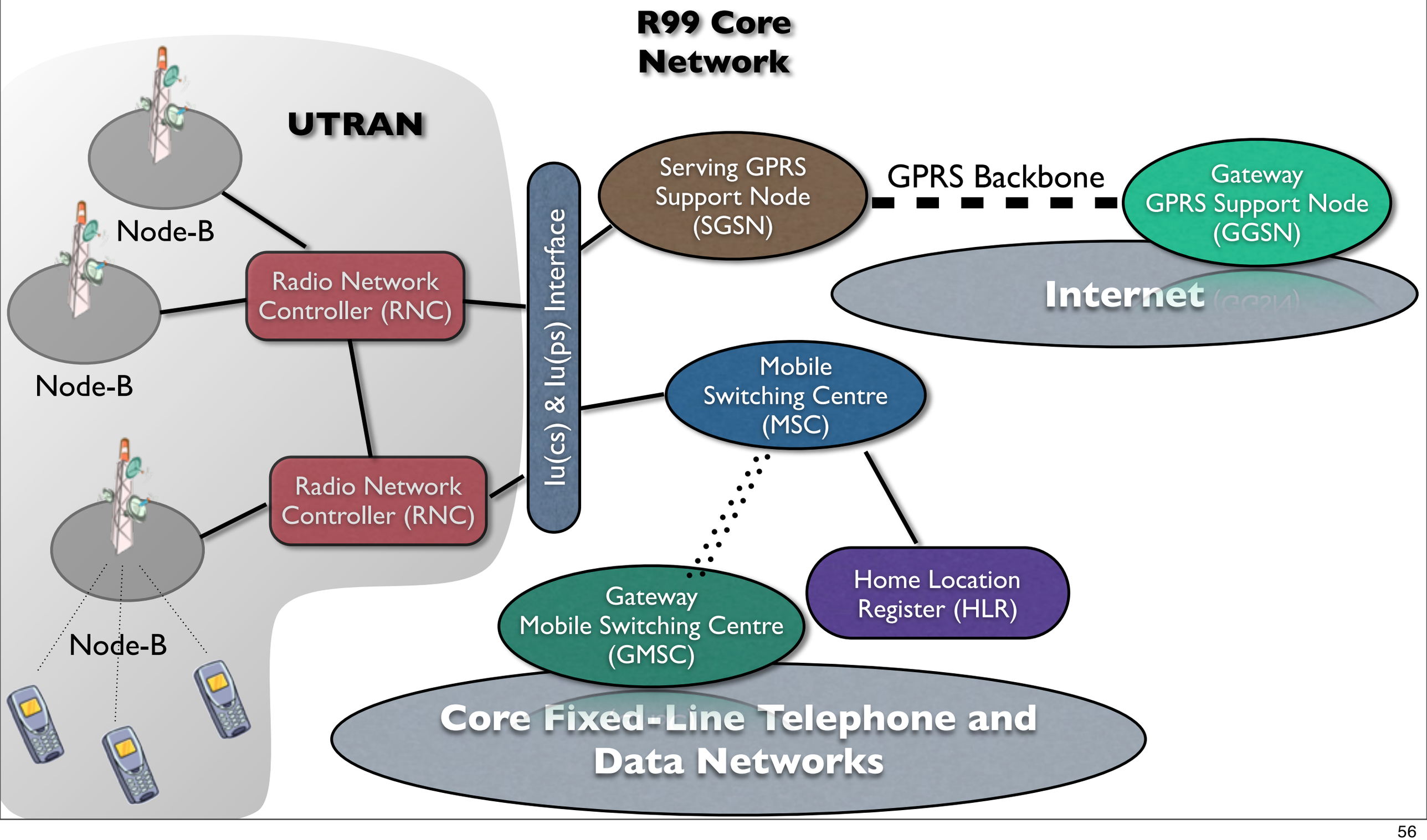
Early UMTS Network (Release 99)

- Release 99 - first step of UMTS
  - Re-designed radio access network:
    - UTRAN - UMTS Terrestrial Radio Access Network
      - Equivalent to GSM's Base Station Subsystem
      - Replaces the Time/Frequency multiplexing with WCDMA over a wider range of frequencies
        - The bidding war for new spectrum led to an EU-wide Telecoms Crash!!!
      - Enables significantly faster data rates (384kbit/s) across air interface
  - GSM BTS renamed "Node-B"
  - GSM BSC renamed "Radio Network Controller" (RNC)

Updates from GSM to UMTS R99

- Improvements:
  - SGSN improved to tunnel data packets more efficiently
  - HLR and authentication software enhanced to support new UMTS features
  - New Iu(cs) and Iu(ps) interfaces to route data from RNC to MSC and SGSN respectively
- Similarities facilitated seamless rollout and backward compatibility with existing GSM system

UMTS System Architecture



UMTS Extensions

- UMTS Release 4: Enhancements for Circuit Switched Core Network
  - Circuit-Switched network revised
    - Introduction of the BICN (Bearer Independent Core Network)
      - Previously, digital voice stream was sent via 64kbit/s time slots on a dedicated backbone
      - Can now be encoded as IP or ATM packets, via a Media Gateway
- Thus both circuit-switched and packet-switched traffic can share the same backbone
  - Reduced cost to network operators in the long term

UMTS Extensions

- UMTS Release 5: Introduction of the IP Multimedia Subsystem (IMS)
  - Circuit-Switched MSC and Iu(cs) interfaces removed
    - All data (inc voice) sent via packet-switched IP
    - Introduction of the Call Session Control Function (CSCF)
      - A SIP architecture designed for Voice over IP (VoIP)
- Release 5 allows full end to end VoIP from phone to phone
  - However, gateways still necessary to for UTMS Release 5 users to talk to users of other network standards

UMTS Extensions

- UMTS Release 5: High Speed Downlink Packet Access (HSDPA)
  - New data transmission scheme
    - Improves downlink speeds from 384kbit/s to between 1.4-3.6Mbit/s with existing equipment (potentially up to 14.4Mbit/s for new devices)
  - Main deployment cost
    - Updating the backhaul links between cells and network, due to increased traffic
- UMTS Release 6: High Speed Uplink Packet Access (HSUPA)
  - Introduced similar uplink speeds as HSDPA to support:
    - User-to-user applications such as video conferencing
  - Increased number of users who could simultaneously send data in the same cell

UMTS/WCDMA

- GSM/GPRS had several shortcomings
  - Legacy design was inefficient for data
    - Practical use of GPRS packet bundling over a GSM TDMA time frame was inefficient
      - Rarely used more than 50% of available capacity
    - Much of the existing network hardware designed for lower transmission rates
  - GPRS time slot allocation slow and on demand
    - Done when required, but could take up to 700ms to establish
    - Tolerable when large data segments are transferred
    - For short/bursty data (e.g. web browsing) delays are noticeable

UMTS/WCDMA

- UMTS / WCDMA (Wideband Code Division Multiple Access) addressed these shortcomings...
  - Bandwidth per carrier frequency extended from 200kHz to 5MHz
  - GSM TDMA replaced by CDMA
    - Transmission Power is dependent on the number of users within the same cell
    - User's data bit is combined with others in the same carrier frequency, and split into several (e.g 128) chips
      - Known as Spreading
      - Builds in error correction

Transmission Power

- Transmission Power is increased as more interference appears on a frequency
  - Due to an increase in the number of users
  - Consider these analogies:
    - Communication in a lecture (low power, little interference)
    - Communication at a party (medium power to overcome general interference)
    - Communication at a disco (high interference, compromising communication)
- Higher transmission speeds also need better signal-to-noise ratio
  - Thus transmission power should be increased

CDMA and data spreading

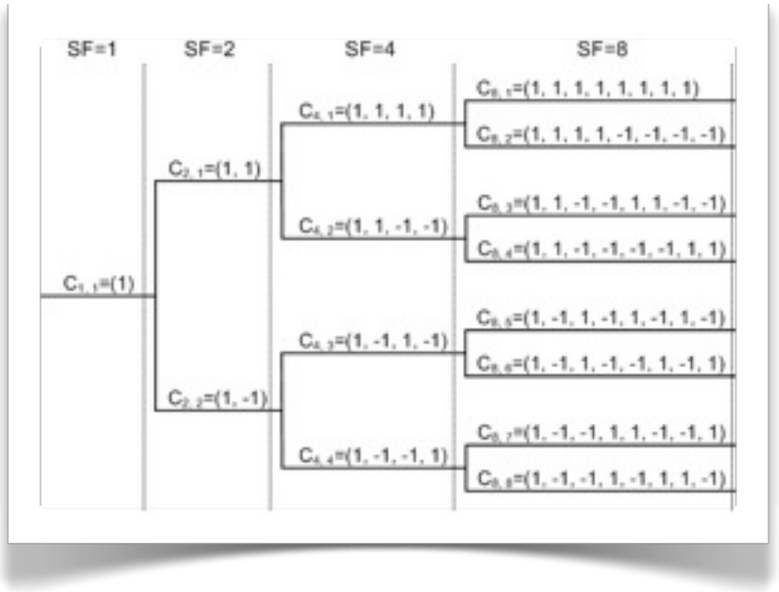
- A sends single bit A_d=1 with spreading code A_k = 010011
  - A sends chips A_s=A_d*A_k = (-1, +1, -1, -1, +1, +1)
    - Data bit and values within spreading code are assigned as "0"=-1 and "1"=+1
- B sends single bit B_d=0 with spreading code B_k = 110101
  - B sends chips B_s=B_d*B_k = (-1, -1, +1, -1, +1, -1)
- When transmitted, the three signals are constrictively combined (i.e. added) over the air interface, resulting in: A_s+B_s = (-2, 0, 0, -2, +2, 0)
- Bitwise Application of spreading codes (inner product) reproduce original bit (result > 0, bit is "1" else "0")
  - A_e = (-2, 0, 0, -2, +2, 0) · A_k = (-2*-1) + (0*1) + (0*-1) + (-2*-1) + (2*1) + (0*1)
    - A_e = 2+0+0+2+2+0 = 6. Therefore, $A_{d'}$=1
  - B_e = (-2, 0, 0, -2, +2, 0) · B_k = (-2*1) + (0*1) + (0*-1) + (-2*1) + (2*-1) + (0*1)
    - B_e = -2+0+0-2-2+0 = -6. Therefore, $B_{d'}$=0

Spreading Factors

- Fragmenting 1 bit into many chips seams counterintuitive!
  - Higher spreading factors have lower data rates
  - More chips (longer codes) mean:
    - More possible channels (potential users) and better error correction
  - More actual users results in more noise!
    - However, in low-occupancy cells, signal-to-noise ratio is reduced
    - Thus, transmission power can be reduced
  - Fewer chips (shorter codes) increase communication speed
    - Though with less error correction, and possibly higher transmission power
- Thus, the spreading factor is varied dynamically based on current usage, and need for data transmission
  - Also varied to react to changes in signal quality or load

Orthogonal Variable Spreading Factors

- Th UMTS air interface assumes a constant chip rate of 3.84MChips/s
  - Therefore, if the spreading factor is constant, then all users of a cell communicate at the same speed!
  - Not desirable, however...
    - Some users may want to make voice calls
    - Others may want to browse the web (bursty data)
    - And others may want video calls
- Orthogonal Variable Spreading Factors (OVSF) allow different spreading factors to be used by different users
  - With OVSF codes, the data rate can be adapted to each user individually



These codes are derived from an OVSF code tree, and each user is given a different, unique code. An OVSF code tree is a complete binary tree that reflects the construction of Hadamard matrices.

Advantages of UMTS Radio Network vs GSM

- UMTS assigns dedicated channels for both voice and data
  - No connection or resource allocation delays
  - Possibly redundant if no data is sent
    - However, this reduces possibility of interference, and hence maintains lower power usage
  - Spreading factor can be adjusted during quiet periods
    - This can introduce slight delays when activity changes
- Better management during handoff
  - GPRS incurs significant interrupts (between 1-3s); UMTS unaffected
- Higher bandwidth means higher limits on data transmission
  - GPRS limited even when user load is very low

HSPA
High Speed Packet Access

- UMTS assumed dedicated channels per device for packet-switched data transmission
  - However, this was too inflexible, limiting data to 384kb/s with a spreading factor of 8.
    - This in turn limited the number of users to 8 in theory per bearer, and 2-3 in practice
  - Was also inefficient, as spreading codes were allocated per device
    - Thus, with bursty data, there were times when a code was not being used.

- HSDPA was proposed to improve efficiency for downlink data
  - This lead to additional enhancements in the uplink direction through HSUPA

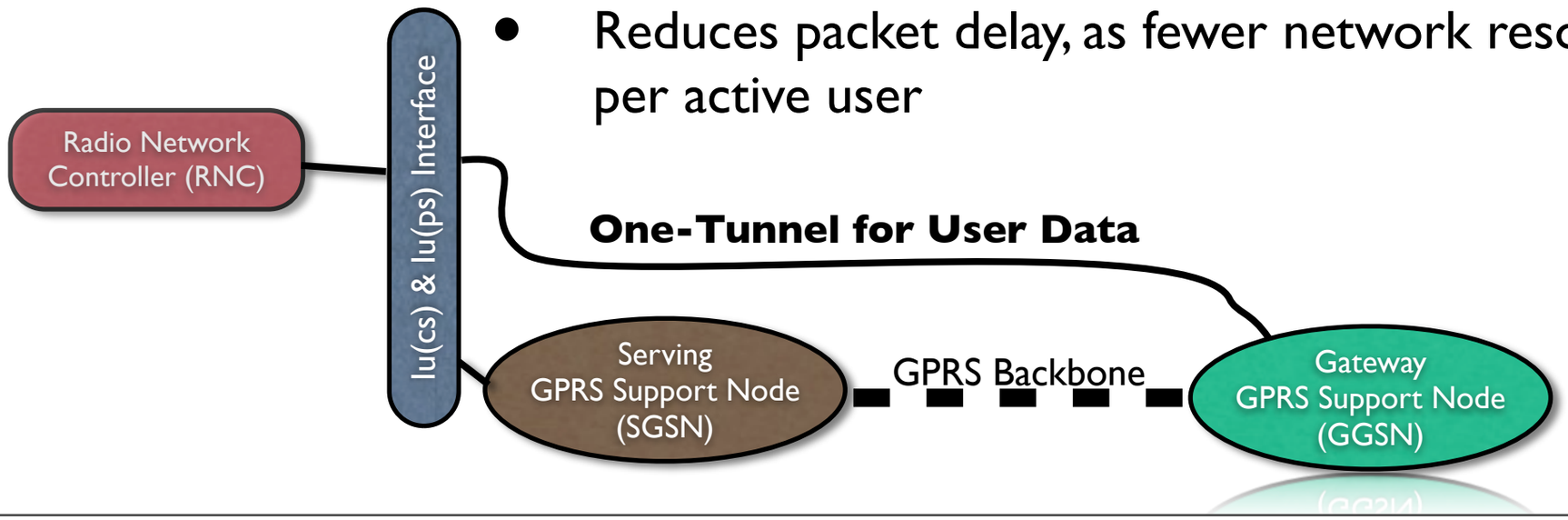
- HSPA represents the combination of HSDPA and HSUPA, to provide faster data access for UMTS
  - First networks appeared in late 2006

HSPA+ and other improvements

- Improvements are being made to HSPA to increase data throughput
  - ***Higher Order Modulation***
    - Release 7 introduced 64QAM to transmit 6 chips per transmission step, compared to HSDPA's 4 chips
      - Works well for micro cell deployments such as shopping malls
      - Not as effective when devices are far from cell transmitter as signal-to-interference level is too low
  - ***MIMO - Multiple In Multiple Out***
    - Uses multiple antennas to receive / send more data simultaneously
    - HSPA+ specifies 2 x 2 antennas, which doubles both down and uplink data rate
    - Has an impact on number of subscribers served within each cell!!!

HSPA+ and other improvements

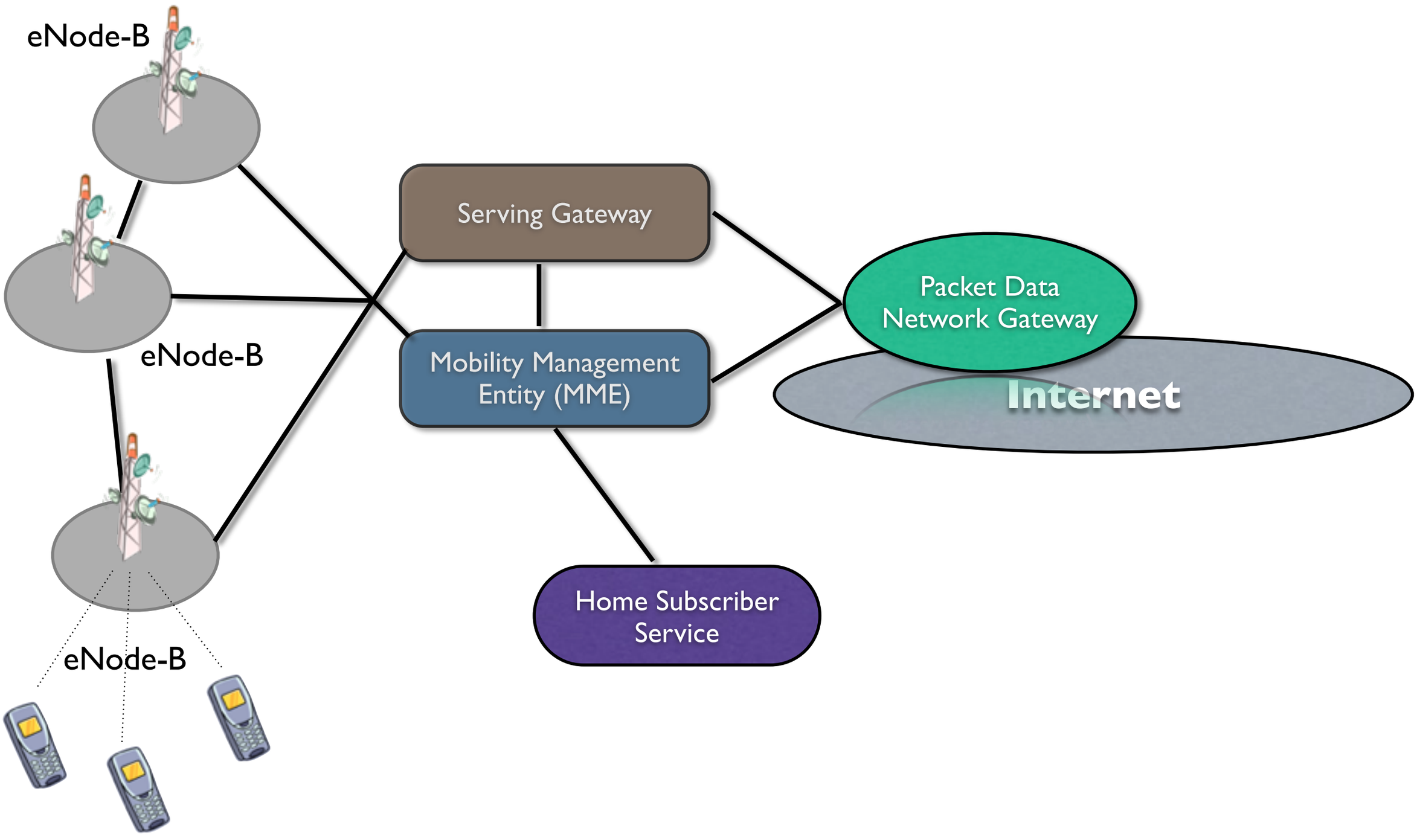
- ***Continuous Packet Connectivity***
  - Improves the signalling once a device has an IP address
  - Reduces signalling overhead, even when little data is sent
  - Also reduces power consumption
- ***One-Tunnel***
  - Removes the need for the Serving GPRS Support Node (SGSN) by tunnelling all packets from the RNC directly to the Gateway GPRS Support Node
  - Reduces packet delay, as fewer network resources are required per active user



LTE

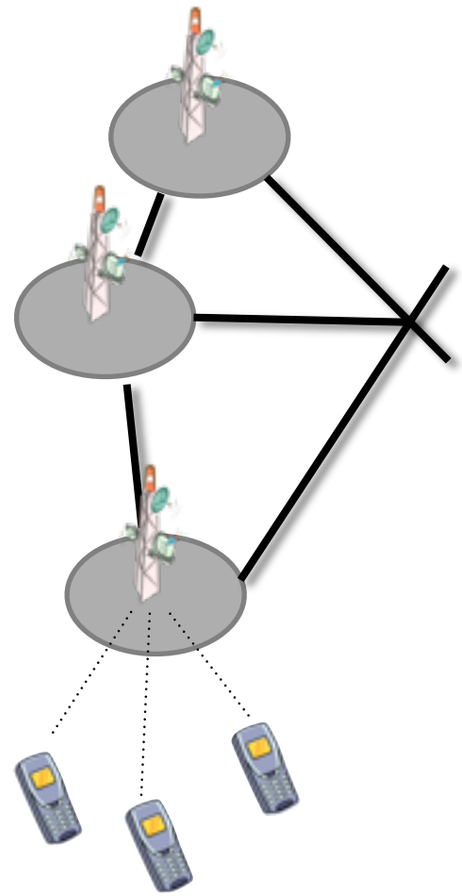
- LTE (Long Term Evolution) explored
  - Has produced similar improvements as HSPA+
    - Few advantages when using the 5MHz bandwidth
    - Benefits are expected once more bandwidth is available
  - Focusses on developing a new air interface architecture and radio network
- Aims are:
    - Reduce time for state changes compared to HSPA
    - Reduce transmission delay from 100ms to 5ms (similar to fixed line networks)
    - Make the bandwidth scalable beyond 5MHz
  - Achieved partly by eliminating the circuit switched network, and improving packet-switched network

LTE Architecture



Enhanced Base Stations

- The Node-B and Radio Network Controller (RNC) from UMTS has been combined to form the eNode-B
  - RNC functionality is now either in the base stations or core network gateway
  - eNode-B forms a mesh with other nodes to manage air interface
  - Something similar existed in HSPA for data, but RNC was responsible for the circuit switched networks
- eNode-B also responsible for handover
- Links to other components is based on IP protocol



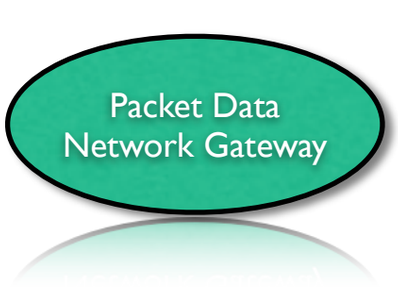
Mobile Management Entity (MME)

Mobility Management Entity (MME)

- MME is the "control plane" entity, responsible for:
  - Subscriber mobility and session management signalling
    - Including authentication, handover management between eNode-B and GSM/UMTS networks
  - Location tracking of idle devices
    - Necessary when no data packets are being exchanged
  - Selection of gateways to the Internet when the mobile device requests an IP address

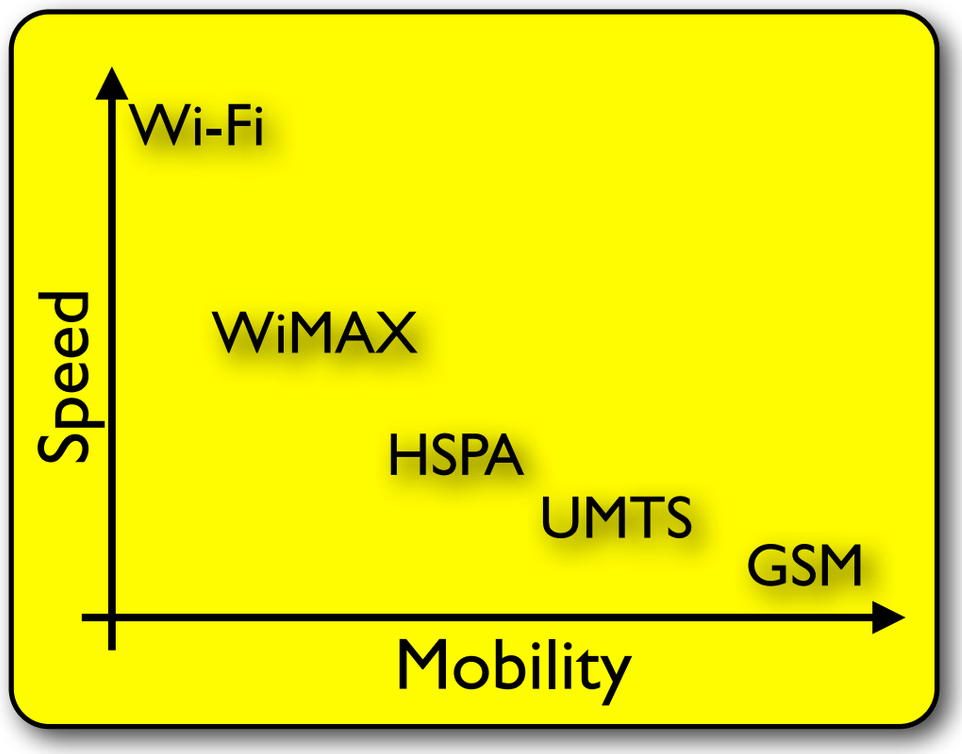
Other components

- The Serving Gateway is the "user plane" entity, responsible for:
  - Forwarding IP packets between mobile devices and the internet.
- Packet Data Network (PDN)-Gateway
  - Fulfils same role as the GGSN
    - Hides the mobility of the user from the Internet
- Home Subscriber Service
  - Similar to an extended Home Location Register
    - Responsible for managing subscriber information for GSM, GPRS, UMTS, LTE and IMS (UMTS Release 5)



WiMAX (802.16e)
Worldwide Interoperability for Microwave Access

- Fast wireless broadband
  - Speeds "theoretically" faster than 70Mbit/s
  - Offers "last mile" access as alternative to DSL or Cable
  - Connect Wi-Fi hotspots to the Internet
  - Data and Telecoms services (alternative to UMTS)
  - Backhaul for 3G networks in less developed areas
- More similar to 3G technologies than WiFi
  - Licensed frequencies
  - Long Range (<50 miles)
    - Lower speed at longer distances
- Operates in various modes
  - *Point-to-point* - acts as a bridge
  - *Point-to-multipoint* - consumer data access



Exercises...

- What is a handover, and which network components are involved?
- Discuss the modularisation approaches used within GSM, and discuss how EDGE improves throughput.
- What are the main differences between the GSM and UMTS radio network?
- Given the following three 8 chip spreading codes, calculate the bits sent by receivers A B and C with the combined transmitted chips (1,1,1,-3,3,-1,-1,-1).
  - A_k = 11001100
  - B_k = 10101010
  - C_k = 10010110

To Recap...

- In this lecture set, we covered:
  - A review of changes in the last 20 years on data communications over Fixed and Wireless networks
    - How increased bandwidth drove consumer Internet use, which in turn drove demand on mobile devices
  - Underlying principles of Mobile Communications, including multiplex schemes and handover
  - 2G GSM technology
    - Underlying Architecture
    - Evolution to the 2.5 G Packet-Switch Network GPRS
    - Evolution to the 3G EDGE Network
  - 3G WCDMA/UMTS/HSPA technology
  - Beyond 3G - LTE and WiMax

Glossary

AC - Authentication Centre

AMPS - Advanced Mobile Phone System

BICN - Bearer Independent Core Network

BSC - Base Station Controller

BTS - Base Transceiver Station

CB - Cell Broadcast

CDM - Code Division Multiplexing

CDMA - Code Division Multiple Access

CSCF - Call Session Control Function

DSL - Digital Subscriber Lines

EDGE - Enhanced Data Rates for GSM Evolution

EIR - Equipment Identity Register

FDD - Frequency Division Duplex

FDM - Frequency Division Multiplexing

GGSN - Gateway GPRS Support Node

GPRS - General Packet Radio Service

GSM - Global Systems for Mobile Communications

HLR - Home Location Registers

HSDPA - High Speed Downlink Packet Access

HSPA - High Speed Packet Access

HSUPA - High Speed Uplink Packet Access

IMEI - International Mobile Equipment Identity

IMS - IP Multimedia Subsystem

IMSI - International Mobile Subscriber Identity

ISDN - Integrated Services Digital Network

Kc - cyphering key

Ki - individual key per subscriber

LTE - Long Term Evolution

MIMO - Multiple In Multiple Out

MME - Mobile Management Entity

MSC - Mobile Switching Centres

OFDMA - Orthogonal Frequency Division Multiple Access

OVSF - Orthogonal Variable Spreading Factors

PSTN - Public Standard Telephone Network

QAM - Quadrature Amplitude Modulation

QPSK - Quadrature Phase Shift Keying

RNC - Radio Network Controller

SDM - Space Division Multiplexing

SC-FDMA - Single Carrier Frequency Division Multiple Access

SGSN - Serving GPRS Support Node

SIP - Session Initiation Protocol

SMS - Short Messaging Service

SRES - signed response

TDD - Time Division Duplex

TDM - Time Division Multiplexing

TDMA - Time Division Multiple Access

UMTS - Universal Mobile Telecommunications System

UTRAN - UMTS Terrestrial Radio Access Network

VLR - Visitor Location Registers

VoIP - Voice over IP

WCDMA - Wideband Code Division Multiple Access

WiMAX - Worldwide Interoperability for Microwave Access

Further Reading

- ***M-Commerce***
  Norman Sadeh (Wiley, 2002)
  - Chapter 3

- ***Beyond 3G: Bringing Networks, Terminals, and the Web Together***
  Martin Sauter (Wiley, 2009)
  - Chapter 1

- ***Communication Systems: for the Mobile Information Society***
  Martin Sauter (Wiley, 2006)
  - Chapter 1

- ***Wikipedia !!!***