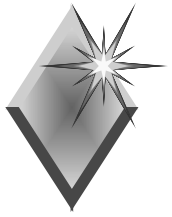
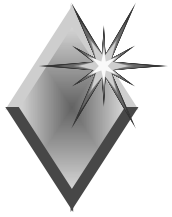


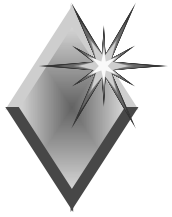
Course Overview

- Introduction and History
- Regulatory Issues
- Fundamentals of Cellular Systems
- AMPS and CDPD (Cellular Digital Packet Data)
- GSM (Global System for Mobile communication)
- Mobile IP
- TCP over Wireless Link
- Issues in Mobile Application Design
- Outlook and Conclusions



GSM: Global System for Mobile communication

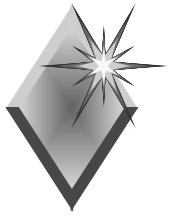
- Why talk about GSM?
  - I am European and GSM is a European standard :-)
  - GSM represents “second generation cellular” (CDPD is based on the “first generation cellular” system AMPS)
  - opportunity to discuss issues specific to mobile computing (handover, mobility management, etc.) in context of concrete system
  - GSM is the base system of many successful systems, such as DCS1800 and PCS1900 (for “personal communication systems”) and ongoing research on “third generation cellular” systems (UMTS: Universal Mobile Telecommunications System, and FPLMTS: Future Public Land (or: LAN) Mobile Telecommunications System)



GSM History

- 1978 - Europe allocated 2 x 25 MHz spectrum in 900 MHz range for mobile communications
- 1982 - Groupe Special Mobile formed under CEPT (French acronym for European Conference of Posts and Telecommunications)
- 1987 - GSM Memorandum of Understanding (MoU) signed by first members, which includes agreements between operators for roaming, numbering and routing aspects, tariffs and accounting.
- 1988 - GSM transferred to newly formed ETSI (European Telecommunication Standards Institute)

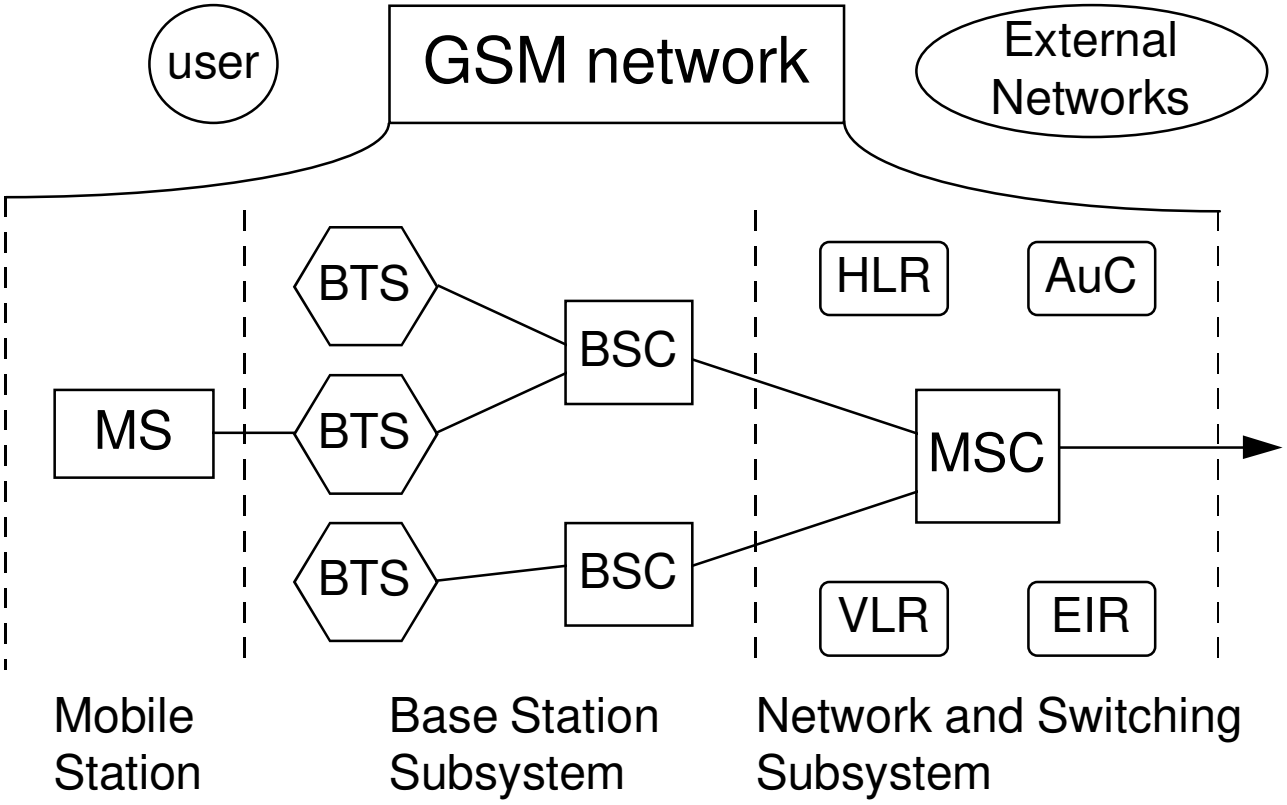
(thanks to John Scourias for providing many of the GSM transparencies)



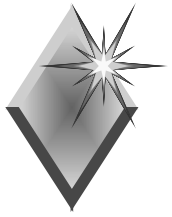
GSM History (ctd.)

- 1990 - DCS1800 standardization begins, after request by United Kingdom
- 1990 - Phase I GSM specifications frozen and published
  - form basis of presentation, due to information available
  - will provide outlook on phase 2 specifications
- 1991 - First operational GSM networks appear
- 1994 - Phase 2 GSM specifications completed

GSM Network Architecture

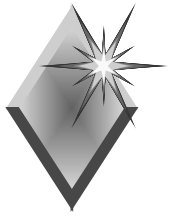


(as was shown on previous transparency, under "Fundamentals of Wireless Systems")



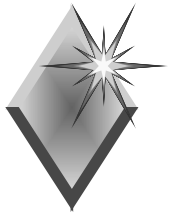
GSM: Mobile Station

- subscriber identity module
  - ISO compliant removable smart card, with limited storage and computational functionality
  - necessary for operation of mobile station, and involved in location management, authentication, and ciphering
  - one or more directory numbers per SIM, one or more SIMs per subscriber
  - SIM realizes model of “personal mobility” (e.g., the subscriber is the focus of attention and it is he/she who is mobile)
- mobile equipment
  - only emergency calls allowed without SIM
  - calls routed to SIM, not mobile equipment



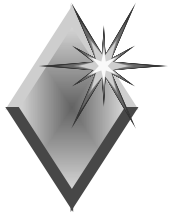
GSM: Base Station Subsystem

- Base Transceiver Station (BTS)
  - contains one or more transceivers (TRX), one for each allocated frequency
  - handles radio signal processing and transmission over the radio interface
  - high density of deployed BTSs, so requirements include compactness, reliability, and low cost
- Base Station Controller (BSC)
  - contains processing power and some switching necessary for management of several BTSs
  - manages channel setup, frequency hopping and handover



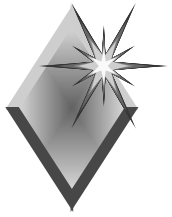
GSM: Network and Switching Subsystem

- Mobile Services Switching Center (MSC)
  - main switching function
  - interfaces with several BSCs and with external networks
  - interacts and coordinates with other NSS functions using Signaling System No. 7
- Home Location Register (HLR)
  - central store of subscriber information, such as subscribed services and charging, as well as current location of subscriber
  - intelligent database function that coordinates location management
  - one logical HLR per mobile network although it may be physically distributed



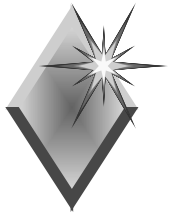
GSM: Network and Switching Subsystem

- Visitor Location Register (VLR)
  - contains subset of HLR information associated with subscribers currently roaming in controlled geographical area
  - associated with one or more MSCs to avoid constant querying of HLR
  - in practice associated with exactly one MSC
- Authentication Center (AuC)
  - protected part of HLR containing secret subscriber key K_i
  - manages authentication and ciphering in cooperation with SIM
- Equipment Identity Register (EIR)
  - stores lists of International Mobile Equipment Identities (IMEI) of valid mobile stations



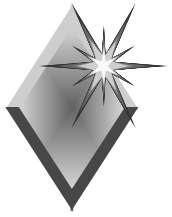
GSM Services

- speech (the “mother of all cash cows”)
  - most important and widely used service
  - uses discontinuous transmission and voice activity detection
    - transmit at about 40% of time, when user actually speaks
    - complete silence at receiver unnerving - comfort noise
- data
  - different services available, depending on end-to-end transmission type, transmission mode, terminal capability
  - supports data rates of 300 bps up to 9600 bps
- facsimile
- short message service
  - alphanumeric messages of up to 160 characters
  - messages saved on SIM



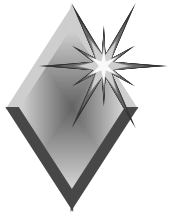
GSM: Radio Transmission Aspects

- spectrum allocation
  - in 1978 Europe allocated 2x25 MHz in the 900 MHz range for mobile communications
    - 890 - 915 MHz for the uplink (mobile station to base station)
    - 935 - 960 MHz for the downlink (base station to mobile station)
  - top 10 MHz in each band reserved for a pan-European mobile system, since band was also used by national analog systems
- multiple access:
  - GSM divides allocated bandwidth into carriers spaced 200 kHz apart, starting 200 kHz from the edge - maximum of 124 carriers in GSM900, 374 carriers in DCS1800 (2x75 MHz allocation)
  - TDMA divides time on each carrier frequency into burst periods lasting 15/26 (0.577) ms



GSM: Radio Transmission Aspects

- channels defined by number and position of time slots occupied in an always cyclic organization
- time slots are implicitly numbered, with an overall period of about 3.5 hours
- numbering on uplink (mobile-to-base) equals numbering on downlink (base-to-mobile) plus 3 burst period delay
- mobile stations with an exclusive radio connection are in *dedicated* mode, otherwise they are in *idle* mode

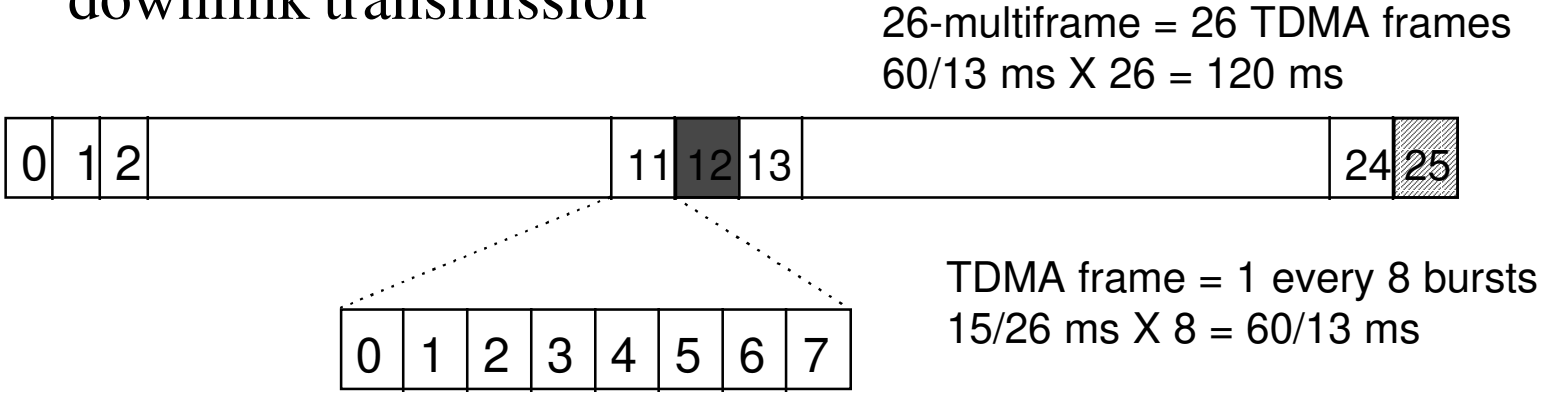


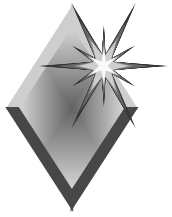
GSM: Dedicated Channels

- traffic channels (TCH) carry user speech and data, as well as some signaling
- a TCH is always allocated with a corresponding Slow Associated Control Channel (SACCH) used for reporting handover measurements
- TCH slots may be ‘stolen’ from a traffic channel for Fast Associated Control Channel (FACCH) signaling, used for call establishment, handover execution, and authentication
- full rate TCH/SACCH occupies one time slot every 8 burst periods (TDMA frame), allowing 8 traffic channels per carrier frequency

GSM: Full Rate TCH/SACCH

- Time slot Number (TN) equals burst number modulus 8, and identifies a particular channel
- cycles every 26 TDMA frames (120 ms, defined so as to be ISDN compatible)
- uplink transmission delayed by 3 burst periods from downlink transmission



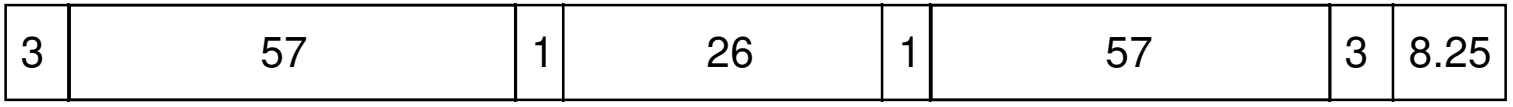


GSM: Other Dedicated Channels

- eighth rate TCH/SACCH or Stand-alone Dedicated Control Channel (SDCCH)
  - either group 8 (called SDCCH/8 in specs), or group 4 plus other common channels (called SDCCH/4), to form equivalent of full-rate TCH
  - used only for signaling, no user data mode specified (but could well be imagined, for example telemetry)
  - complex definition, with 8 traffic slots and 4 SACCH slots every 102 burst periods
- half rate TCH/SACCH
  - not included in Phase I recommendations, although partly specified by 1990
  - occupies, on average, one time slot every 16 burst periods

GSM: Normal Burst Structure

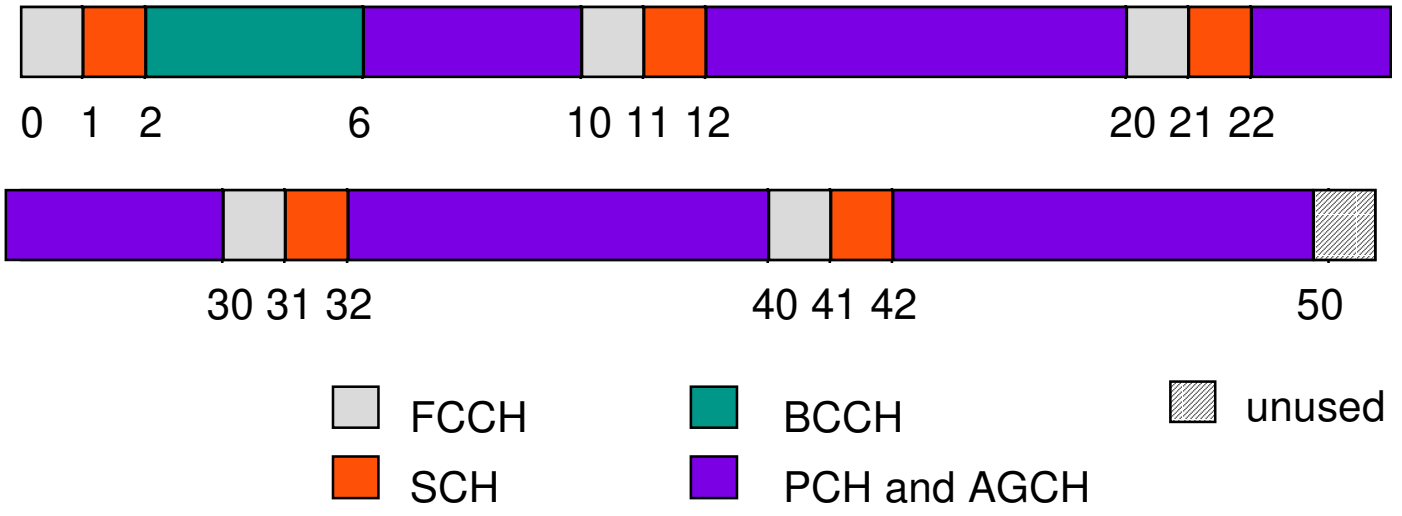
- normal bursts are sent on traffic channels and most control channels, specific burst structures used for some signaling functions
- carry 114 information bits in two blocks of 57 bits, a stealing bit on each block, a 26 bit training sequence (one of eight different ones), and 3 tail bits (set to 0) at each end, with equivalent to 8.25 bits guard time, for a total of 156.25 bits transmitted in 15/26 ms (0.577 ms)

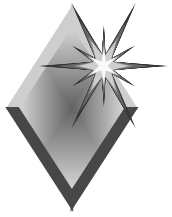


$$\frac{156.25 \text{ bits}}{0.577 \text{ ms}} = 270.833 \text{ kbps raw bit rate per channel}$$

GSM: Common Channels

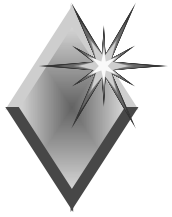
- common channels are accessible by all mobiles, both in idle and dedicated mode
- all common channels have cycle of 51 TDMA frames:
  - allows access by dedicated mobile stations (during one unused time slot in full-rate TCH) every once in a while
  - allow grouping of common channels (all share same cycle)





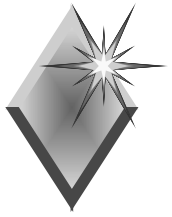
GSM: Common Channels

- Frequency Correction Control Channel (FCCH) and Synchronization Channel (SCH) - downlink
  - mobile stations listen to the FCCH and SCH to acquire time synchronization with base station
  - FCCH transmits a unique radio burst (F burst with 142 bits set to 0)
  - SCH immediately follows FCCH, and its burst (S burst with 64 bit training sequence) gives cell's burst numbering - all frequencies in cell follow same numbering
  - exactly one set of FCCH and SCH channels per cell, by definition on TN 0, on a non-hopping frequency called the *beacon frequency*



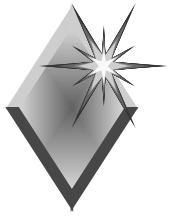
GSM: Common Channels

- Broadcast Control Channel (BCCH) - downlink
  - carries general information including parameters to control cell selection, control channel configuration, random access parameters, and beacon frequencies of neighboring cells
- Paging Channel (PCH) and Access Grant Channel (AGCH) - downlink
  - time separation between PCH and AGCH depends on cell parameters
  - discontinuous reception increases battery life by dividing PCH into paging sub-channels
    - mobiles belong to sub-channels in pre-determined way
  - smaller PCH/AGCH possible, of 1/3 capacity
  - PCH/AGCH may be extended in up to three extra TNs along with BCCH and RACH on the uplink



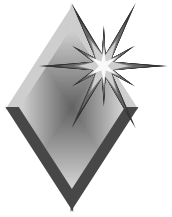
GSM: Common Channels

- Random Access Channel (RACH) - uplink
  - slotted Aloha channel accessed by mobiles wishing to enter dedicated mode
  - special short burst (Access burst with 36 information bits, 41 training bits) used to account for unknown timing advance
- Cell Broadcast Channel (CBCH) - downlink
  - used for Cell Broadcast Short Message Service
  - replaces eighth rate TCH



GSM: Transmission Process

- information in bursts is not raw user data or signaling due to high radio path losses
- different forward error control and interleaving done, depending on channel type and transmission mode
- channel coding
  - block convolutional codes
    - add redundancy for error correction in the form of binary additions of shifted versions of the input sequence
  - fire codes
    - version of cyclic redundancy code which divides the sequence by a known factor, and appends the remainder to the sequence
    - GSM uses generator polynomial of degree 40, thus adding 40 bits

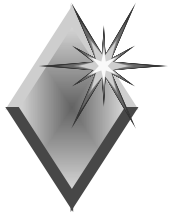


GSM: Transmission Process

- parity codes
  - small parity codes added for error detection in RACH and SCH, as well a parts of speech frames
- interleaving
  - performed on all channel types except SCH and RACH
  - code word spread over several successive bursts to randomize occurrence of errors, especially with frequency hopping
  - interleaving over more bursts involves tradeoff between better error performance and increased delay
  - channel coder outputs code words 456 bits long and each burst carries two half-bursts of 57 bits
    - 114 bits per burst over 4 consecutive bursts
    - 57 bits per burst over 8 consecutive bursts
    - 6, 12, 18, or 24 bits per burst over 22 consecutive bursts (historically called *19 burst interleaving*)

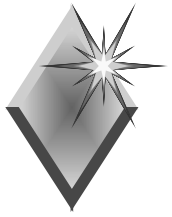
GSM: Transmission Process

Channel and transmission mode	Input rate (kbps)	Input size (bits)	Channel coding	Output size (bits)	Interleaving
TCH/F Speech	13	260	Parity & conv.	456	8 bursts
TCH/F 9.6 TCH/H 4.8	12 6	240	Convolution	456	22 bursts
TCH/F 4.8	6	120	Convolution	456	22 bursts
TCH/F 2.4	3.6	72	Convolution	456	8 bursts
TCH/H 2.4	3.6	144	Convolution	456	22 bursts
SCH		25	Parity & conv.	78	S burst
RACH		8	Parity & conv.	36	Access burst
FACCH		184	Fire & conv.	456	8 bursts
TCH/8, SACCH BCCH, PCH, AGCH		184	Fire & conv.	456	4 bursts



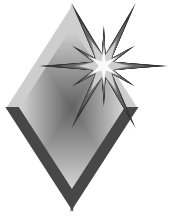
GSM: Transmission Process

- ciphering
  - protect transmission (speech, data) from eavesdropping
  - after interleaving, 114 information bits of normal bursts are enciphered by XORing with 114 bit ciphering sequence
- burst formation and modulation
  - 114 information bits (for normal bursts) are split in two 57 bit blocks
  - one of several possible 26 bit training sequences are used for equalization
  - tail bits are added for the Gaussian Minimum Shift Keying (GMSK) modulation with BT=0.3
  - GMSK also used in DECT and Mobitex for spectral efficiency and relative ease of demodulation



GSM: Frequency Hopping

- GSM uses slow frequency hopping, changing the transmission frequency before every burst
- frequency diversity improves reception since different frequencies are affected differently during propagation
- interferer diversity improves reception by distributing relative interference of particular frequency among many calls
- hopping sequences are sets of (time slot number, frequency) pairs, where frequency is one of up to 64 different frequencies
  - Mobile Allocation Index Offset (MAIO) is a value between (1, number of allocated frequencies in cell)
  - Hopping Sequence Number (HSN) is a value between (0, 63)
  - MAIO and HSN combination determine a pseudorandom hopping sequence

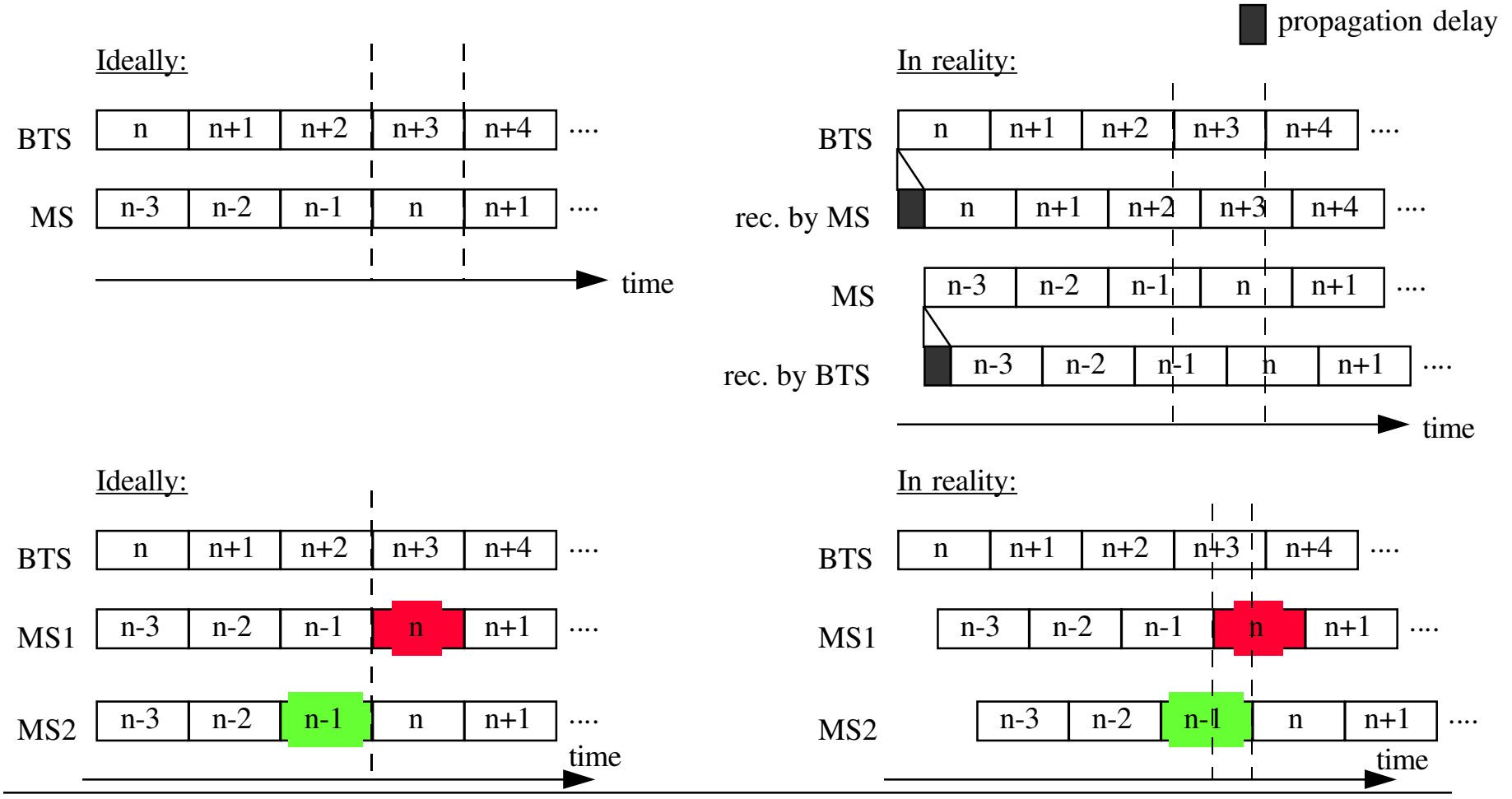


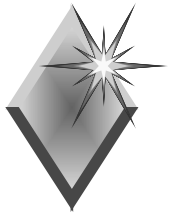
GSM: Radio Resource Management

- Radio Resource (RR) layer includes the functions required to manage the radio interface
- concept of RR session
  - started when mobile station leaves idle mode, and terminated when idle mode is re-entered
  - contains signaling and data path between mobile station and MSC, which may be modified by handovers
  - characteristics such as transmission mode and cipher mode may be altered
  - more than one communication is possible during an RR session
- handles access (including paging), transmission management, **timing advance, handover, power control**

GSM: Radio Resource Management

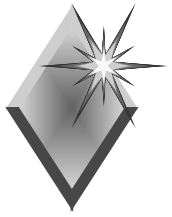
Timing Advance





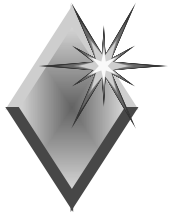
GSM: Radio Resource Management

- timing advance
  - bursts received at BTS from multiple mobile stations must fit within their allocated time slots, which occur 3 burst periods after corresponding transmission
  - mobile station advances its transmission by twice the propagation time between the BTS and the mobile station
  - maximum cell radius of 35 km partly determined by maximum value of timing advance (233 microseconds at the speed of light)
  - synchronization of cells (same slot numbering) allows calculation of timing advance by mobile station - improves speed and efficiency of handover
  - for handover between unsynchronized cells or at initial access, timing advance estimated by BTS from access burst, whose frame number is implicitly known by both entities



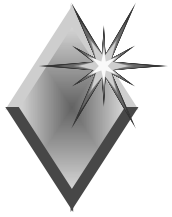
GSM: Radio Resource Management

- handover
  - procedure to change serving cell during a communication
  - efficient handover important for spectral efficiency and quality of service
  - three types of handover can occur
    - Case A: Inter-cell handover - same BSC
    - Case B: Inter-BSC handover - different BSC, same MSC
    - Case C: Inter-MSC handover
  - three reasons for handover exist
    - To provide signaling and data path as subscriber moves from cell to cell
    - To distribute subscribers to neighboring cells during peak traffic situations
    - To distribute subscribers to neighboring cells to reduce overall interference levels



GSM: Radio Resource Management

- handover measurements
  - certain measurements are required for the handover decision
    - downlink measurements performed by the mobile include transmission quality (raw bit error rate), reception level of current cell and of best six neighboring cells
    - uplink measurements performed by the BTS include transmission quality, reception level of current channel, and timing advance
    - static measurements include maximum transmission power of mobile station, current cell and neighboring cell capacity and current load
  - mobile station reports measurements on SACCH at least twice a second
  - measurements performed during gaps between reception and transmission

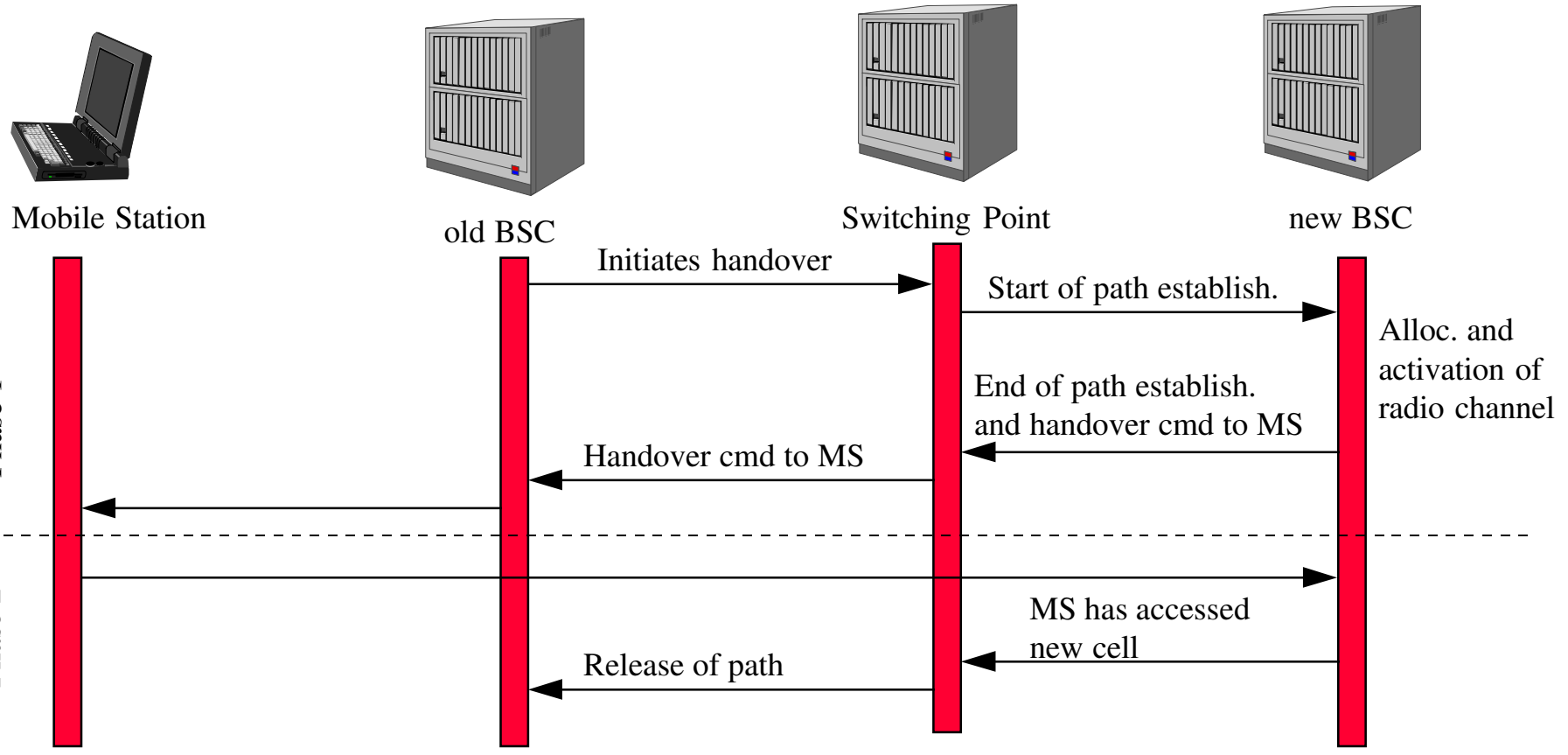


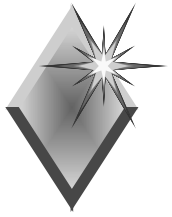
GSM: Radio Resource Management

- measurements on neighboring cells are on beacon frequency (transmitted on current cell's BCCH)
  - Base Station Identity Code (BSIC) is color code to distinguish between cells using same beacon frequency, in case of co-channel interference
- due to interleaving over four bursts, delay is 480 ms, which is also the measurement reporting period
- non-transmission from discontinuous transmission (for speech channel) would be interpreted as bad reception level
  - minimum of 12 bursts required on channel during each reporting period - 8 bursts carry interleaved silence descriptor frame for comfort noise, and 4 bursts carry interleaved SACCH measurements
  - one set of measurements is only on these mandatory slots, second set of measurements is on *all* bursts (no difference for a TCH/8 channel)
- actual algorithm for handover decision not specified, but handover decision is taken by BSC

GSM: Radio Resource Management

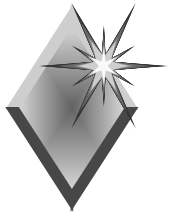
General Handover Execution Scheme





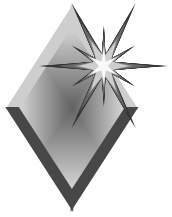
GSM: Radio Resource Management

- handover execution
  - type and mode of new channel may be different from old channel
  - general two-step procedure involves establishment of new path up to switching point and notification of mobile station, and access of new path by mobile station and release of old path
  - path establishment phase, inter-cell handover
    - switching point is the same BSC
    - BSC already has all necessary information
    - new link on BTS-BSC interface may need to be established for new cell
    - BSC sends RIL3-RR HANDOVER COMMAND to mobile station indicating new channel parameters



GSM: Radio Resource Management

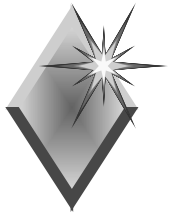
- path establishment phase, inter-BSC handover
  - switching point is same MSC
  - Old BSC sends BSSMAP HANDOVER REQUIRED message to MSC, which includes current cell and one or more target cells, transmission mode, cipher mode, mobile station classmark
  - MSC establishes SCCP connection with new BSC and forwards relevant information in a BSSMAP HANDOVER REQUEST message
  - new BSC sends RIL3-RR HANDOVER COMMAND to MSC which forwards it to mobile station
- path establishment phase, inter-MSC handover
  - switching point is anchor MSC
  - after old (relay) MSC receives BSSMAP HANDOVER REQUIRED message, it translates it to a MAP PERFORM SUBSEQUENT HANDOVER message sent to the anchor MSC, which forwards it to the new MSC



GSM: Radio Resource Management

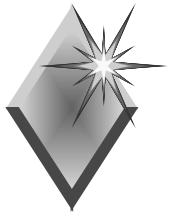
- new MSC proceeds as for inter-BSC handover, and when it receives the RIL3-RR HANDOVER COMMAND from the new BSC, it translates it to a MAP PERFORM HANDOVER ACKNOWLEDGMENT message sent to the anchor MSC that includes a *handover number* required for establishing a circuit through the PSTN or ISDN
- anchor MSC sets up circuit to new MSC using the handover number and sends a MAP PERFORM SUBSEQUENT HANDOVER ACKNOWLEDGMENT to old MSC, which is forwarded to the mobile station as a RIL3-RR HANDOVER COMMAND as in the inter-BSC handover case

- failure indications are eventually forwarded to old BSC, which may retry handover in the same cell or another cell



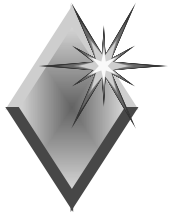
GSM: Radio Resource Management

- mobile station access phase
  - mobile station first informed of handover when it receives RIL3-RR HANDOVER COMMAND containing new channel description, including whether handover is synchronous or asynchronous
  - synchronous handover occurs when old cell and new cell are synchronized, i.e. have the same time slot numbering
    - timing advance can be calculated by mobile station given the old timing advance and the propagation difference
    - mobile station sends a few short Access bursts for BTS calculation, and then transmits normally
  - asynchronous handover is required if cells are not synchronized
    - BTS computes timing advance from access bursts and transmits value to mobile station



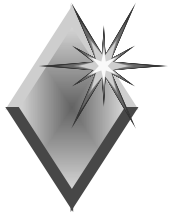
GSM: Radio Resource Management

- as an option for cases A and B, BTS may send a handover detect message to switching point to switch connection early
- completion involves the mobile station sending a RIL3-RR HANDOVER COMPLETE message up to the switching point which results in switching the communication path (if not already switched) and releasing the old channels



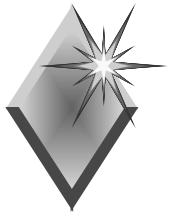
GSM: Radio Resource Management

- power control
  - mobile station and BTS transmission power can be independently modified
  - improves spectral efficiency by reducing system interference levels and increases mobile station battery life
  - each mobile station's transmission power can be changed in steps of 2 dB over the range specified by the power class of mobile station
  - either BSC or BTS manages power control in both directions
  - access messages and initial messages are sent at fixed power level specified in BCCH



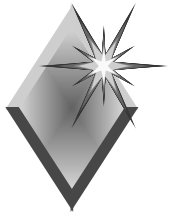
GSM: Mobility Management

- PLMN and cell selection
  - PLMN: Public Land Mobile Network
  - in idle mode, mobile station *camps* on one cell, on which it listens for paging messages
  - cell and PLMN selection has administrative and technical aspects
  - subscriptions are made with a home PLMN operator, who may have roaming agreements with other operators
  - PLMN selection occurs upon request from user or when user moves out of coverage area of serving PLMN



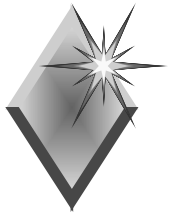
GSM: Mobility Management

- normal service case is when user is subscribed to one or more available PLMNs
  - SIM stores a *forbidden list* of previously found PLMNs which are not subscribed to
  - in manual mode, the *found list* of available PLMNs is presented to user, indicating whether a PLMN is in the *forbidden list*
  - in automatic mode, mobile station selects PLMN based on *preferred list, found list* and *forbidden list* contents
- limited service case is when user is not subscribed to an available PLMN - only emergency service available
  - selection of PLMN still important since it can determine country to provide emergency service in border areas
  - mobile station monitors 30 strongest carriers for a new PLMN
  - in automatic mode, mobile station attempts selection of newly found PLMNs not on *forbidden list*



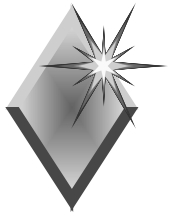
GSM: Mobility Management

- cell selection of best cell within serving PLMN always done automatically by mobile station
  - selection of best cell determined by C1 criterion
  - C1 = *average receive level - p1 - max((p2 - maximum MS power level), 0)*
    - p1 is value between -110 dBm and -48 dBm broadcast on BCCH
    - p2 is value between 13 dBm and 43 dBm indicating maximum transmit power on RACH - also on BCCH
  - only cells with positive C1 (which are not barred) within the selected PLMN are considered, and cell with highest value of C1 is selected
  - C1 effectively determines cell boundaries
    - hysteresis value may be used to delay cell selection requiring location update



GSM: Mobility Management

- cell selection at switching on
  - first PLMN tried must be home PLMN
  - mobile searches all frequencies (124 for GSM900, 374 for DCS 1800), or looks up stored beacon frequencies on SIM, for C1 positive and non-barred cells, and selects cell with highest C1
  - if new location area is same as stored value of last location area, IMSI attach is performed, otherwise normal location update is performed
- cell selection during normal service (idle mode)
  - serving cell broadcasts beacon frequencies of neighboring cells in same PLMN
  - if one of neighboring cells has a higher C1 value, and belongs to same location area, mobile starts listening on new cell's paging channel
  - if better cell belongs to new location area, mobile station switches cells and performs location update

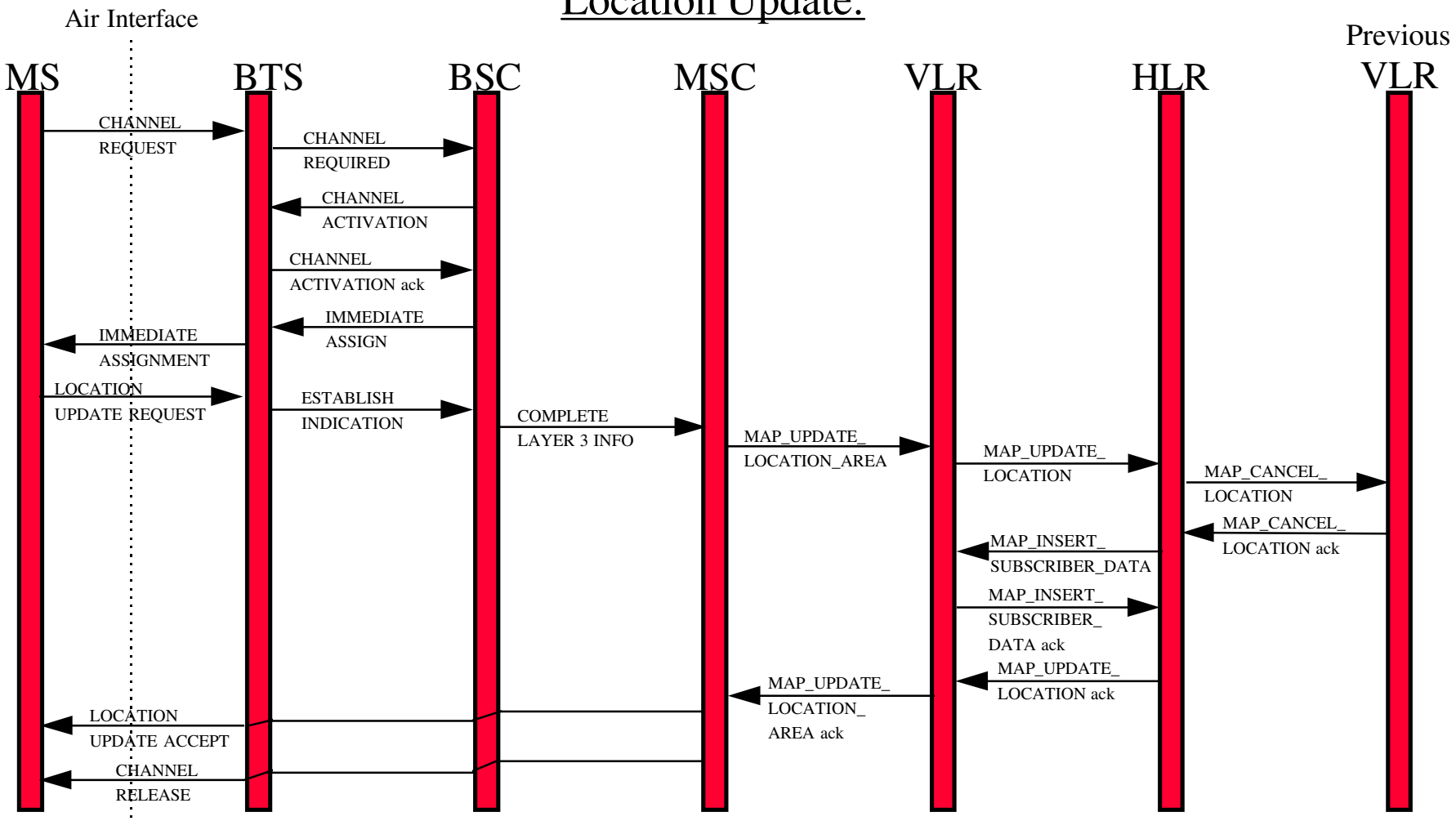


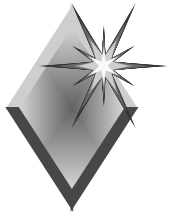
GSM: Mobility Management

- cell selection upon change to new PLMN
  - since no beacon frequency list is on the SIM, mobile station scans all frequencies and selects 30 strongest frequencies, stored in *found list*
  - once PLMN is selected, cell from *found list* with best C1 value belonging to selected PLMN is selected and location update is performed
- concept of location area
  - compromise between system-wide paging and per-cell location updating
  - one or more cells forming smallest location element
  - location update required when first entering new location area - all cells within location area paged for incoming calls
  - definition of location areas up to operator - only constraint is that they must belong to the same VLR

GSM: Mobility Management

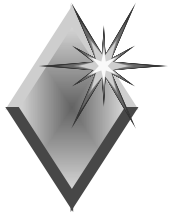
Location Update:





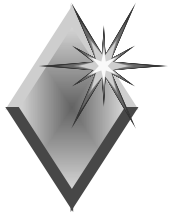
GSM: Mobility Management

- location updating procedure
  - mobile subscriber is identifiable by the International Mobile Station Identity (IMSI) which consists of a Mobile Country Code, a Mobile Network Code identifying the operator, and a Mobile Subscriber Identity Number, whose first digits may indicate subscriber's HLR
  - mobile station sends a RIL3-MM LOCATION UPDATE REQUEST message to the new MSC containing the IMSI
    - if mobile subscriber is already in the VLR, or if the HLR is not reachable, new MSC replies with accept or reject message



GSM: Mobility Management

- MSC sends MAP UPDATE LOCATION message to subscriber's HLR, containing IMSI and SS7 address of the visited MSC
- if subscription allows registration, HLR is updated, new VLR is sent relevant subscriber data for managing calls, and old VLR is sent cancellation message if subscriber was previously registered
  - otherwise, subscriber is deregistered and cancellation message is sent to old MSC
- periodic location updating is a user option which allows quicker recovery in case of HLR failure

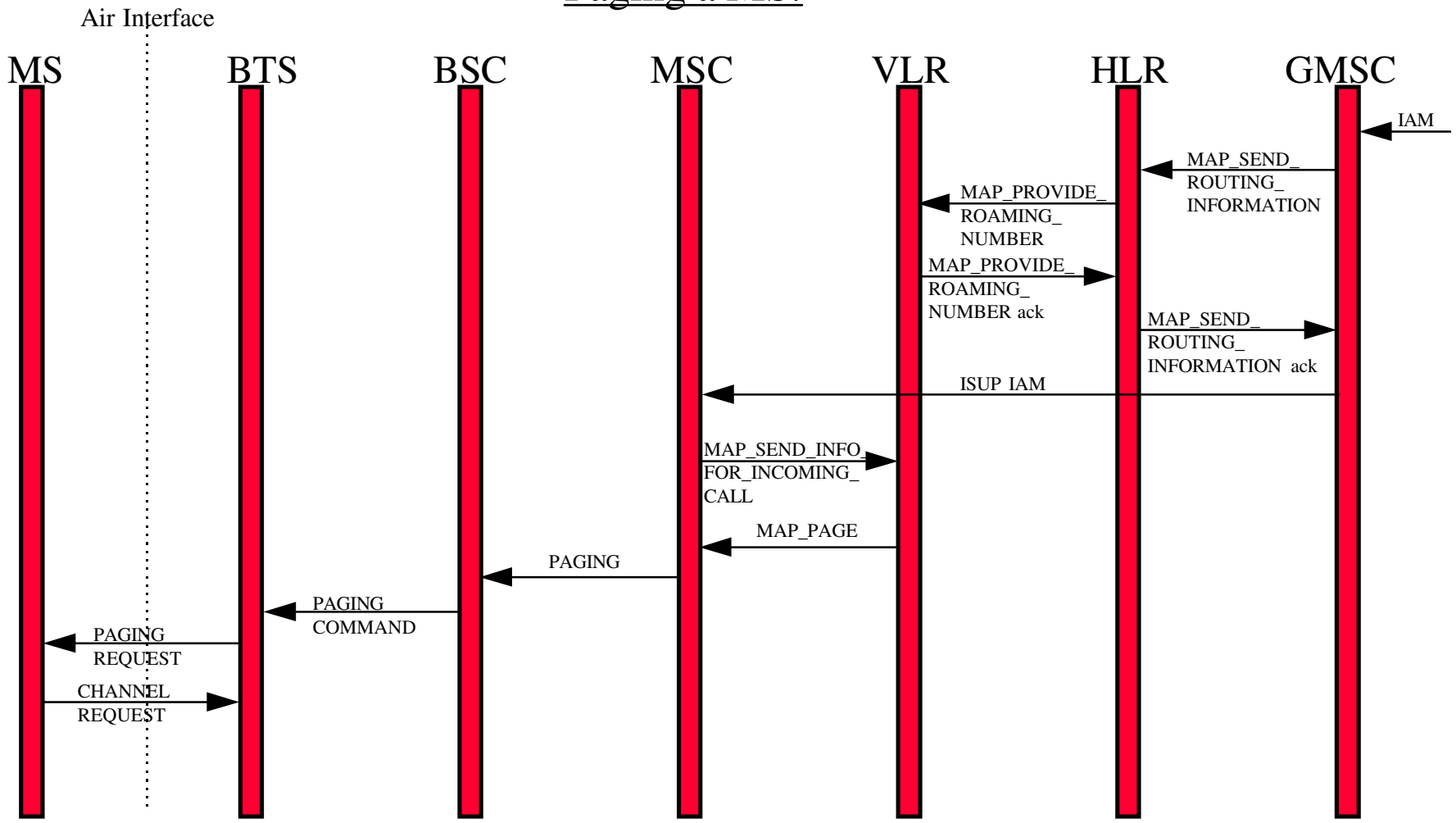


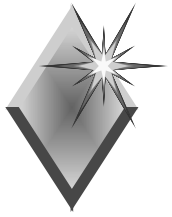
GSM: Mobility Management

- IMSI attach and detach functions
  - if mobile station is switched off or SIM is removed, subscriber is unreachable and paging would be wasting resources
  - a bit in subscriber's record in HLR indicates whether paging attempt is useful
  - IMSI detach marks the subscriber as unreachable, and IMSI attach marks subscriber as reachable, if new location area is same as previous one

GSM: Mobility Management

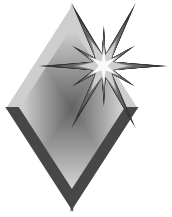
Paging a MS:





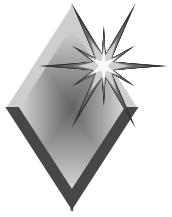
GSM: Paging a Mobile Subscriber

- paging is actually a function of the radio resource management (though not directly linked with a specific RR session), not directly part of mobility management
  - originating PSTN switch derives Gateway MSC address from the dialed digits (mobile subscriber's MSISDN) and will issue an Initial Address Message (IAM), indicating an incoming call
  - Gateway MSC contacts HLR to eventually obtain a roaming number (MSRN) to route call to destination MSC
  - HLR looks up current location and contacts appropriate VLR, which assigns a MSRN and returns this (via HLR) to Gateway MSC
  - Gateway MSC continues call routing by sending IAM to destination MSC, using the newly assigned MSRN



GSM: Paging a Mobile Subscriber

- MSC contacts VLR, which triggers paging in known location area. MSC will block until subscriber responded to paging.
- VLR sends paging requests (via MSC) to appropriate BSCs, including information such as IMSI, TMSI (if one has been allocated already), a list of cells to be paged, and if applicable and known, the type of channel required for incoming call (e.g., speech or data)
- BSCs issue paging messages to each BTS specified, adding information about *paging group* (section of paging channel, for discontinuous reception by mobile to conserve battery power)
- paging messages are normally repeated an operator-configurable number of times to decrease chance of lost pages
- when mobile successfully receives a paging message, it initiates a channel assignment procedure (similar to location update step), which will complete connection establishment



GSM: Mobility Management

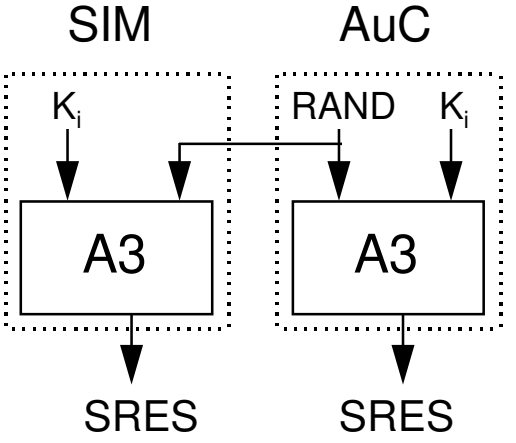
- authentication
  - authentication proves to network that subscriber SIM is who it claims to be
  - authentication and ciphering based on secrecy of subscriber key K_i, stored in the SIM and in the AuC
  - procedure initiated by visited MSC at various events, such as call setup or location update

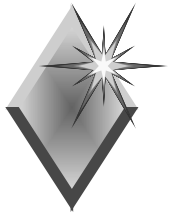
MSC sends RIL3 AUTHENTICATION REQUEST message containing 128 bit random number (RAND) from AuC

given RAND and K_i, SIM (and AuC) calculate a Signed Response (SRES) using secret and operator-dependent algorithm A3

normally, triplets of (RAND, SRES, K_c) are sent to visited MSC/VLR in advance, upon registration

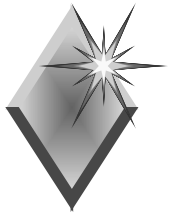
if both SRES are equal, SIM is authenticated





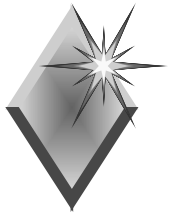
GSM: Mobility Management

- ciphering
  - provides user privacy by coding the transmission so that only authorized entities can decode message
  - encryption is an operator option - not up to user
  - 64 bit ciphering key K_c obtained by SIM and AuC from K_i and the initial random number RAND input into the operator-dependent A8 algorithm
  - ciphering procedure uses 22 bit frame number (time slot number mod 8) and K_c to produce two 114 bit sequences through the A5 algorithm, which are XORed with the 114 information bits in each traffic direction
  - single A5 algorithm is used, distributed by MoU committee



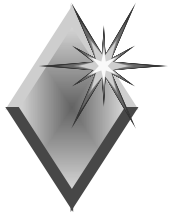
GSM: Mobility Management

- subscriber identity confidentiality
  - unique IMSI (International Mobile Subscriber Identity) transmitted in the clear during initial access
  - temporary Mobile Subscriber Identity (TMSI) is shorter identity, relevant only within a location area (i.e., in combination with Location Area Identifier (LAI))
  - TMSI first allocated during registration in a particular VLR, and deallocated when subscriber deregisters
  - during location update to another MSC/VLR, TMSI in combination with old LAI can be sent by mobile station, and used to query old MSC/VLR for the IMSI



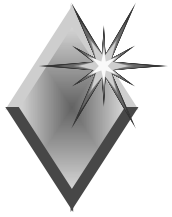
GSM: Mobility Management

- equipment identity checking
  - Equipment Identity Register (EIR) maintains database related to mobile equipment (hardware) identified by International Mobile Equipment Identity (IMEI)
  - IMEI consists of Type Approval Code (granted when mobile station type passes type approval testing to ensure mobile station behaves properly), Final Assembly Code (indicating manufacturing plant), and the equipment serial number
  - EIR stores three lists of IMEIs
    - white list contains ranges of IMEIs of type approved mobile stations, maintained by MoU
    - black list contains IMEIs which are stolen or malfunctioning, and are subsequently barred
    - gray list contains IMEIs which should be supervised for possible malfunctions



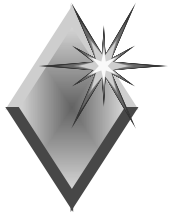
GSM: Future Developments

- evolution of GSM in Phase 2 and Phase 2+
  - GSM architecture intended for future evolution
  - half-rate speech coders and channels accounted for from the start
  - other developments occurred as system evolved, such as radio interface specifications at 1.8 GHz (DCS1800) and 1.9 GHz (PCS1900)
  - upward compatibility is a requirement for Phase 2 and later developments, so that old infrastructure and mobile stations will be able to interwork with new equipment and protocols
  - manufacturers and operators given freedom to develop their own solutions, where this did not interfere with interworking principle
  - full advantage of improvements in digital signal processing and VLSI can be taken



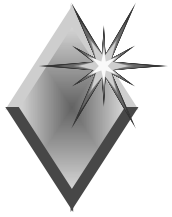
GSM: Future Developments

- phase 2+
  - enhanced full rate speech
    - uses improvements in speech coding to provide wireline quality on current full rate channels
    - possible to use different speech coding algorithms, or use adaptive tradeoff between channel and source coding
  - **GPRS: General Packet Radio Service**
  - high-speed data rates
  - group call allows one group member to talk while others listen, with efficient use of radio channels
  - interworking with satellite communications
  - interworking with developments in fixed networks, in particular Universal Personal Telecommunications (UPT) and Intelligent Networks (IN)



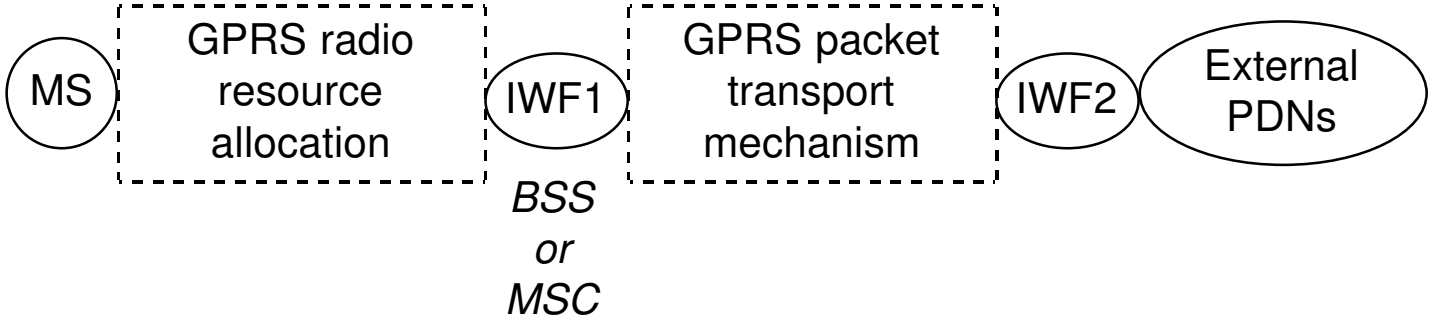
GSM: Future Developments

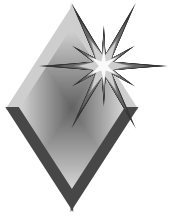
- General Packet Radio Service (GPRS)
  - applications such as credit card validation require frequent relatively short transactions
    - problems with current connection-oriented data services include long call setup times, inefficient use of circuit connection (radio and fixed links)
    - problems with current Short Message Service include limit on message length, unidirectional nature of service, relatively long delay, limited signaling resources
  - GPRS goals
    - efficient usage of radio and wireline resources
    - authentication and ciphering
    - smooth integration into existing GSM system
    - simultaneous operation with other GSM services



GSM: Future Developments

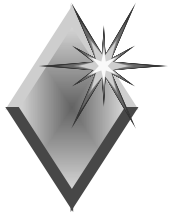
- GPRS functional architecture
  - GSM transmission must deal with two semi-independent aspects so is divided into two functional entities
    - GPRS radio resource allocation deals with efficient usage of radio interface channels
    - GPRS packet transport mechanism deals with efficient packet routing through GSM infrastructure to the interworking function (IWF2) with the external Packet Data Network (PDN)
    - two functions are connected by another interworking function (IWF1)





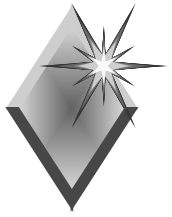
GSM: Future Developments

- radio resource allocation
  - proposal one
    - normal traffic channel used with modified access and setup mechanism
    - Radio Link Protocol (RLP) used for retransmission
    - standard authentication and ciphering applied
  - proposal two
    - special GPRS Packet Channel (GPCH) allocated in every cell
    - reservation procedure reserves channel for duration of transaction
    - number of allocated GPCHs should be dynamically allocated depending on traffic (one user per GPCH)
    - RLP can be used
    - ciphering and authentication require some modification due to shared channel (shared over time, no multiplexing)



GSM: Future Developments

- proposal three
  - GPCHs allocated per cell
  - packets from multiple users are multiplexed on channel
  - RLP and security mechanisms need to be modified
  - requires dynamic allocation of GPCH depending on traffic
- packet transport mechanism
  - proposal one
    - use existing signaling network along with SMS (Short Message Services)
    - Gateway MSC contains IWF2 which queries HLR for routing information
    - message size constrained to SMS limit: max. frame length of 272 octets on A interface (between MSC and BSC), overhead of higher protocol layers leaves 140 octets, enough for 160 7-bit ASCII characters
    - transfer delay must be improved



GSM: Future Developments

- proposal two
  - use external Packet Data Network
  - IWF1 incorporates IWF2 function - concentrates packets and performs protocol conversions
    - IWF1 located in BSS (Base Station Sub-system) requires many access units to external network
    - IWF1 located in MSC requires functions to route packets to proper BSC
  - router able to access HLR (and VLR if IWF1 is located in BSS) required in external PDN
- proposal three
  - use dedicated GPRS packet network from IWF1 to IWF2
  - protocol routers interface with HLR (and VLR if IWF1 is located in BSS)
  - packet routing information could be cached at routers to avoid HLR check for individual packets