The Global System for Mobile telecommunication is a European standard for mobile communications, optimized to facilitate roaming and operating at 900MHz. GSM provides mobility across the network and independent of the mobile platform by assigning to users a subscriber identity module which carries a user phone number and information. Because of its efficiency GSM is currently used as a standard reference for the development of new protocols.

Cellular mobile communications is based on the reuse of frequency. The narrow usable band is divided into non-overlapping frequency channels which are all assigned to a hexagonal area called a cell. Network access if provided to users within a cell by a Base Station Subsystem (BSS), which manage the radio resources.

The cellular network is a star architecture network superposed on the existing landline infrastructure, which handles routing calls. A cluster of BSS are linked together within a Mobile Switching Center (MSC) which acts as gateways for mobile users to the global switched landline network and sometimes a public data network offering packet switching. MSCs also control call signaling and processing and they coordinate call handover from one BSS to another while roaming. There may also exist inter-MCS links which enable cellular user to bypass telephony networks altogether.

GSM uses many network databases to manage users. Most importantly, the Home Location Register (HLR) and the Visiting Location Register (VLR) are used to record the position of a user within the network. The Authentication Center (AC) is used to encrypt private information and user data across the network. MSCs are equipped with a Service Switching Point (SSP) which is used to query locations and service plans for routing calls. The addressing used in GSM is called MSISDN and follows the same protocol as landline numbering: a country code, a national destination code, and finally a subscriber number. Routing is achieved using HLR and VLR information.

GSM uses 2 frequency bands: 890-950MHz for mobile to BSS and 935-96-MHz for BSS to mobile communication. The bands are split up into 124 carriers spaced by 200 kHz. Each cell is assigned a certain number of carriers. The 200 kHz spectrum is assigned using time-division multiple access (TDMA) which enables a gross bit rate of up to 270 kb/s.

Connection handoff can be done between channels in the same cell, different cells, different BSS (all above are called internal) and even different MSCs (called external). The handoff decision is made based on signal strength information provided by the MSs, or for traffic management purposes. Location information is stored in the user’s HLR associated to his home MSC. Upon user location change, if a new BSS detects the user, it reports it to its VLR, which in turn forwards this information to the user’s HLR. As it is received, the HLR send a message to the old location VLR to discard the data.

For routing a call to a mobile user, first the network needs to locate him. From a landline, the PSTN may use the MSISDN to route the call to the closest Gateway MSC within the mobile’s PLMN. The GMSC in turn uses the MSISDN to query the mobile’s HLR for the routing information required to route the call to the visiting MSC of the mobile user at the time. The visited VLR is identified in the mobile’s HLR. The user’s current MSC then pages the mobile with a broadcast to all BSSs of the cell. After a compatibility check, the BSS assigns a channel and once the call is answered, the mobile sends a connect message to the MS.

GSM uses a 3 layers protocol, similar to the OSI, except that layer 3 encloses some of the OSI’s higher layers and is divided in the following sub-layers: resource management (RR) implemented over the link between the MS and the BSS, the mobility management (MM) and connection management (CM). The data link layer over the radio link (connecting the MS to the BSS) is based on a LAPD-like protocol, called LAPDm.

The RR management sub-layer is implemented in the BSS and performs the functions of establishing physical connections over radio for the purpose of transmitting call-related signaling information. The MM sub-layer is terminated at the MSC and the related messages from or to the MS are relayed transparently in the BSS using the DTAP process. MM provides functions classified into three types of procedures: the MM specific procedures, the MM common procedures, and the MM connection related procedures. The CM sub-layer terminates at the MSC and contains entities that currently consist of CC including call-related supplementary services, SMS, and call independent supplementary services support (SS).

Because of its efficiency and versatility, the GSM has been extended to a new standard called the General Packet Radio Service (GPRS). The drive for change comes from the fact that GSM data rated are slow (9.6kb/s) and connection times are high (few seconds) because communication is done in a circuit switching way. Users of GPRS benefit from shorter access times (< 1 sec) and higher data rates (~50kb/s).

To integrate GPRS into the GSM network, new nodes responsible for the delivery and routing of data packets, called GPRS support nodes (GSN), have been introduced. These nodes are further subdivided in Support nodes (SGSN), responsible for the delivery of data packets from and to the mobile stations within its service area, and Gateway nodes (GGSN) which serves as an interface between the GPRS backbone network and the external packet data networks.

GPRS offers 2 kinds of end-to-end packet switched data transfer: point-to-point (PTP) service and point-to-multipoint (PTM) service, which is similar in some sense to multicasting. GPRS also allows the use of different QoS profiles which can be negotiated on a per call basis and are: service precedence, reliability, delay, and throughput. As an addition to the GSM network, GPRS can be used simultaneously to handle packet switching while the underlying GSM network handles the circuit switching required for calls.

To use GPRS, a mobile needs to register with a SGSN on the network and attach itself. The disconnection from the GPRS network is called GPRS detach and can be initiated by the mobile station or by the network. Once attached, a mobile needs to request an IPv4 address from the PDN IP network called a Packet Data Protocol (PDP) address. The allocation of the PDP address can be static, when the user’s home PLMN network permanently assigns an address to the mobile, or dynamically assigned once the mobile accesses the PDP network. For routing, SGSN to which the mobile is registered encapsulates incoming IP packets, examines the PDP context, and routes them through the intra-PLMN GPRS backbone to the appropriate GGSN. The GGSN decapsulates the packets and sends them out on the IP network, where they are routed as regular traffic.

To handle location management, the MS frequently sends location update messages to its current SGSN, which reduces the need of paging. An MS can be in either one of three states: IDLE, when it is not reachable, READY, after a GPRS attach and STANDBY, when it is synchronized and ready to operate packet transfers.

On the physical layer, the channel allocation in GPRS is different from GSM because it allows a single mobile station to transmit on multiple time slots of the same TDMA frame. To avoid conflicts, a cell supporting GPRS may allocate physical channels for GPRS traffic. Besides the physical channels, GPRS defines multiple logical channels to handle different functions: signaling, broadcast of general system information, synchronization, channel assignment, paging, or payload transport. These logical channels are mapped onto the GSM TDMA frames over time and frequency. Channel coding is also performed by GPRS in a similar fashion than GSM to protect packets against errors.

GPRS architecture is divided into many planes. The backbone (SGSN and GGSN) encapsulates IP/X.25 packets over GTP packets over UDP/TCP-IP transport architecture. The Subnetwork Dependent Convergence Protocol (SNDCP) is used for sending packets between SGSN and MS and also performs multiplexing connections and user data compression/decompression. Below, we have the Data Link Layer which operates wirelessly, and finally the signaling plane which comprises protocols for control and support of the functions in the transmission plane.

Overall, GPRS is a mobile station friendly wireless extension on the internet which enables users to enter the IP network and provide them with a packet switched fast and reliable network access.