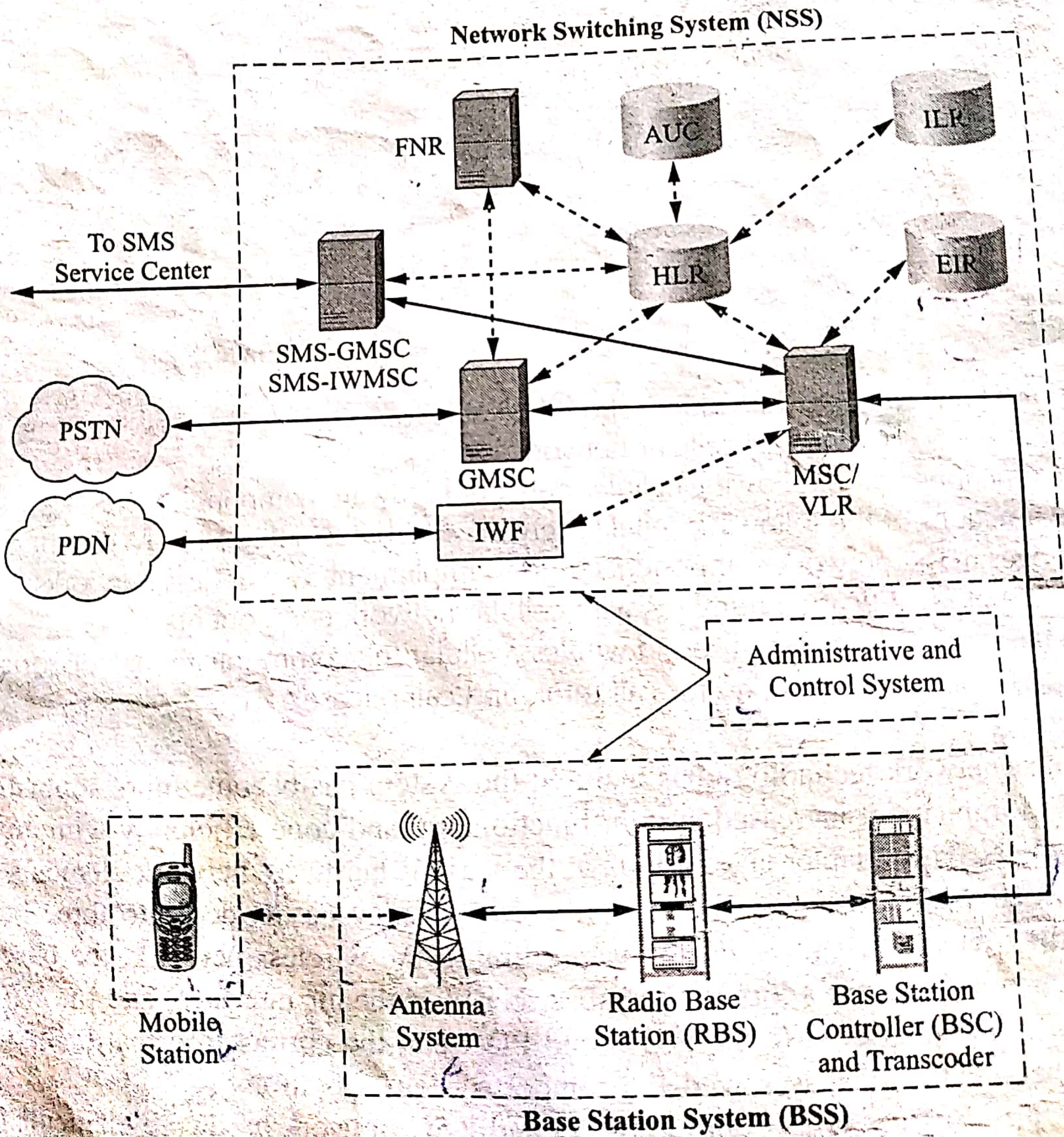
1 COMMON CELLULAR NETWORK COMPONENTS

e typical post–first generation (1G) wireless cellular telecommunications system as shown in Figur nsists of several subsystems or network elements designed to perform certain operations in support ire system. For 2G and 2.5G cellular networks, the air interface functions are typically performe ed radio base station (RBS) and a mobile station (MS) or subscriber device (SD) that provide user . The radio base station is usually controlled by a base station controller (BSC) and this portion llular system is usually referred to as the base station system (BSS).



igure 3–1 Typical wireless cellular system components.

The base station

Figure 3–1 Typical wireless cellular system components.

The base station system is connected to a fixed switching system (SS) that handles the routing of b voice calls and data services to and from the mobile station or subscriber device. This switching syst usually consists of a mobile switching center (MSC) and various databases and functional nodes used support the mobility management and security operations of the system. The switching system is usua connected to the PSTN, the PDN, other public land mobile networks (PLMNs), and various data messagi networks through gateway switches (GMSCs). Other typical connections to the switching system are to n work management systems and other accounting or administrative data entry systems.

The various network elements that make up the wireless system are interconnected by communicatio links that transport system messages between network elements to facilitate network operations and deliv the actual voice call or data services information. The rest of this section is devoted to descriptions of thes network elements and brief overviews of their basic functions. It should be pointed out again that all cellular wireless systems are standards based and therefore both the names of the system subunits and the communication interfaces between them are defined by the standard for the particular type of technology used by the system (GSM, NA-TDMA, CDMA, etc.).

In this chapter, the subject matter will be dealt with in as generic a way as possible using common terms and definitions. Later chapters devoted to particular systems will present the names of the system components and interfaces using the correct nomenclature for them as specified by the appropriate system standard.

Subscriber Devices

The first generation of wireless cellular systems provided connectivity to the PSTN for voice service. The initial term used in several standards for the mobile transceiver supplied to the cellular system users was mobile station. As cellular systems have matured and added ever faster data service delivery to the traditional teleservices available to the user, the term *subscriber device* (SD) has come to be used to describe the mobile transceiver for these newer systems. As the wireless network evolves toward an all-IP network, the expression used for the mobile transceiver is expected to morph one more time with the eventual adoption of the term **end terminal** (ET). This name change will be in keeping with the mobile station's ability to connect to an all-IP network and thus provide the functionality of an end terminal device.

The **subscriber device** is the link between the customer and the wireless network. The SD must be able to provide a means for the subscriber to control and input information to the phone and display its operational status. Additionally, the SD must be able to sample, digitize, and process audio and other multimedia (e.g., video) signals; transmit and receive RF signals, process system control messages; and provide the power needed to operate the complex electronics subsystems that provide the functionalities mentioned earlier. Therefore, as shown in Figure 3–2, the basic sections of the SD are as follows: some form of a man-machine interface, an RF transceiver section, a signal processing section, a system control processor, and a power supply/management section.

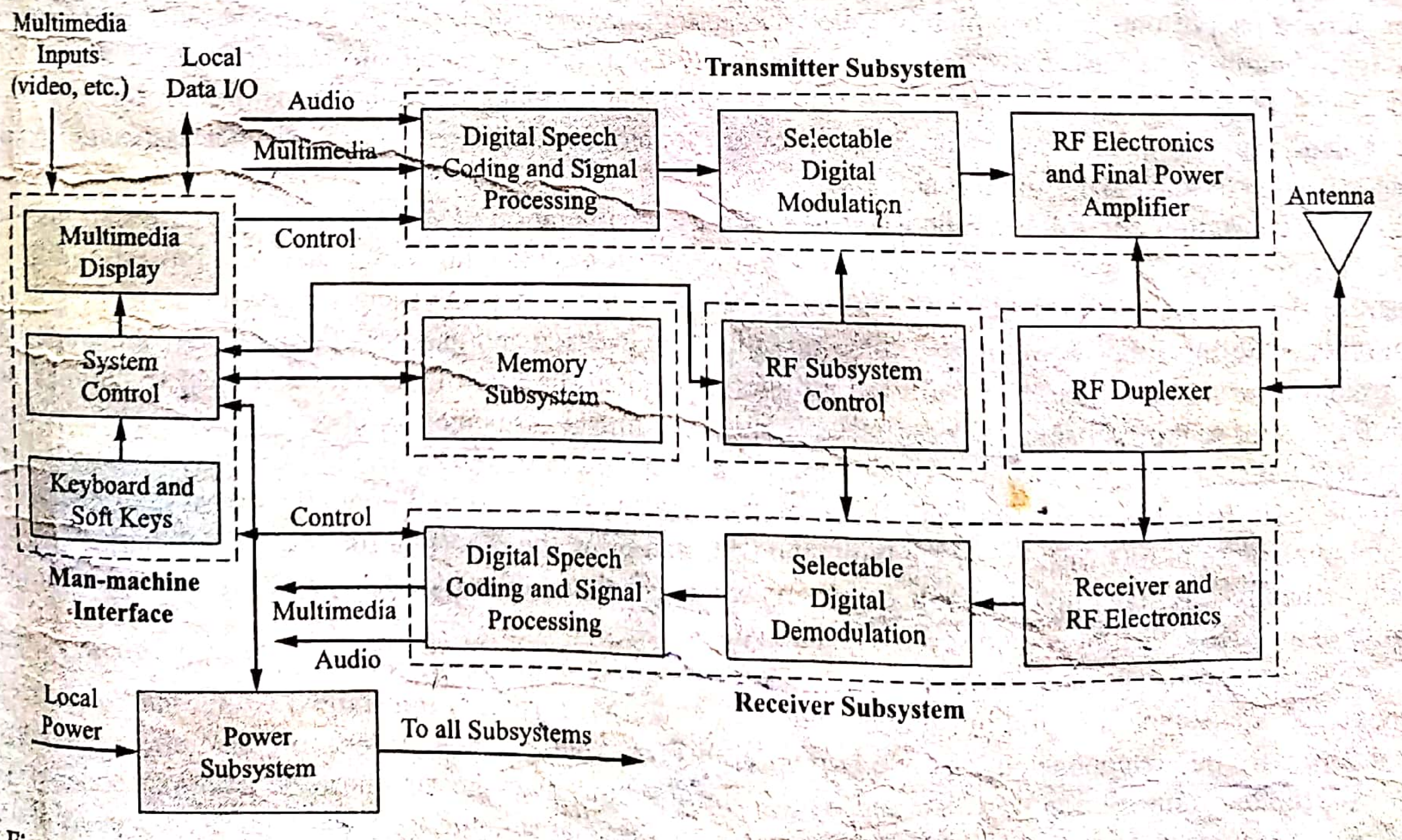


Figure 3–2 Typical subscriber device block diagram.

The man-machine interface can be as simple as a standard telephone keypad, an alphanumeric text display, and a microphone/speaker combination. Or, it may be more sophisticated with soft-key keypad functions and multimedia capability with a high-resolution color display and video camera or cameras for the transmission and display of video messages. Additional accessory interfaces usually also exist to provide the option of hands-free operation, battery charging, and a service port or a data port for connection to a PC.

The RF transceiver section contains the high-frequency RF electronics needed to provide the proper digital modulation and demodulation of the air interface RF signals and the ability to transmit and receive these RF signals. This section must also permit both variable power output and frequency agility under system software control.

The signal processing section of a subscriber device is usually based on digital signal processor (DSP) technology. Some of the functions performed by this section are speech sampling and coding, channel coding, and audio and video processing.

The system control processor provides overall subscriber device management. It implements the required interface with the other wireless network elements to provide radio resource, connection management, and mobility management functions through software control of the various functions and operations it must perform to set up and maintain the air interface radio link.

Finally, the power supply section provides the power to energize the entire system. Usually, the SD is battery operated with sophisticated algorithms built into the system to save and minimize power usage as much as possible in an effort to extend the battery life. When the battery becomes discharged, it may be recharged through a home accessory battery charger or through the accessory connector of one's car.

... System Components

Base Station System Components

The **base station system** handles all radio interface-related functions for the wireless network. The BS typically consists of several to many radio base stations (RBSs), a base station controller (BSC), and transcoder controller (TRC). It should be noted that these last two network elements did not exist in the fir analog cellular systems. In 1G systems the RBSs were connected directly to the MSC. The radio equipme required to serve one cell is typically called a base transceiver system (BTS). A single radio base stati might contain three base transceiver systems that are used to serve a cell site that consists of three 12 degree sectors or cells. The radio base station equipment includes antennas, transmission lines, pov couplers, radio frequency power amplifiers, tower-mounted preamplifiers, and any other associated har ware needed to make the system functional.

The base station controller's function is to supervise the operation of a number of radio base stations th provide coverage for a contiguous area (see Figure 3–3). It provides the communication links to the fix part of the wireless network (PSTN) and the public data network (PDN) and supervises a number of a interface mobility functions. Some of these tasks include location and handoff operations and the gatheri of radio measurement data from both the mobile device and the radio base station. The base station co troller is used to initially set up the radio base station parameters (channels of operation, logical cell name handoff threshold values, etc.) or change them as needed. The BSC is also used to supervise alarms issu by the radio base stations to indicate faults or the existence of abnormal conditions in system operati (including those of its own). For some faults the BSC can bring the reporting subsystem back into operati automatically (i.e., clearing the fault or alarm) whereas other faults require operator intervention in th form of an on-site visit by a field service technician.

The transcoder controller performs what is known as rate adaptation. Voice information that has be converted to a standard digital pulse code modulation (PCM) format is transmitted within the PSTN o standard T1/E1/J1 telephone circuits at 64 kbps. Both TDMA and CDMA systems use data rates of 16 kb or less for the transmission of voice and control information over the air interface. The transcoder co troller's function is to convert the PCM data stream to a format suitable for the air interface. **Vocodin**

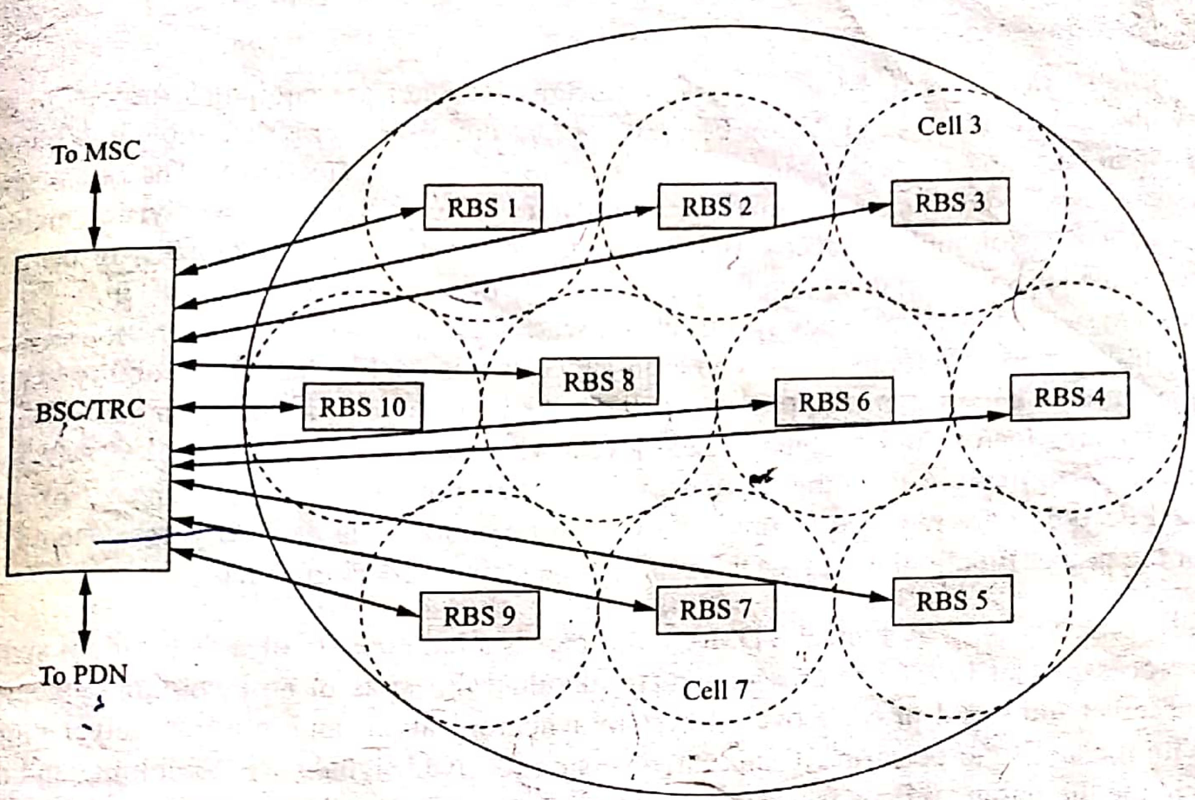


Figure 3–3 The base station controller's function.

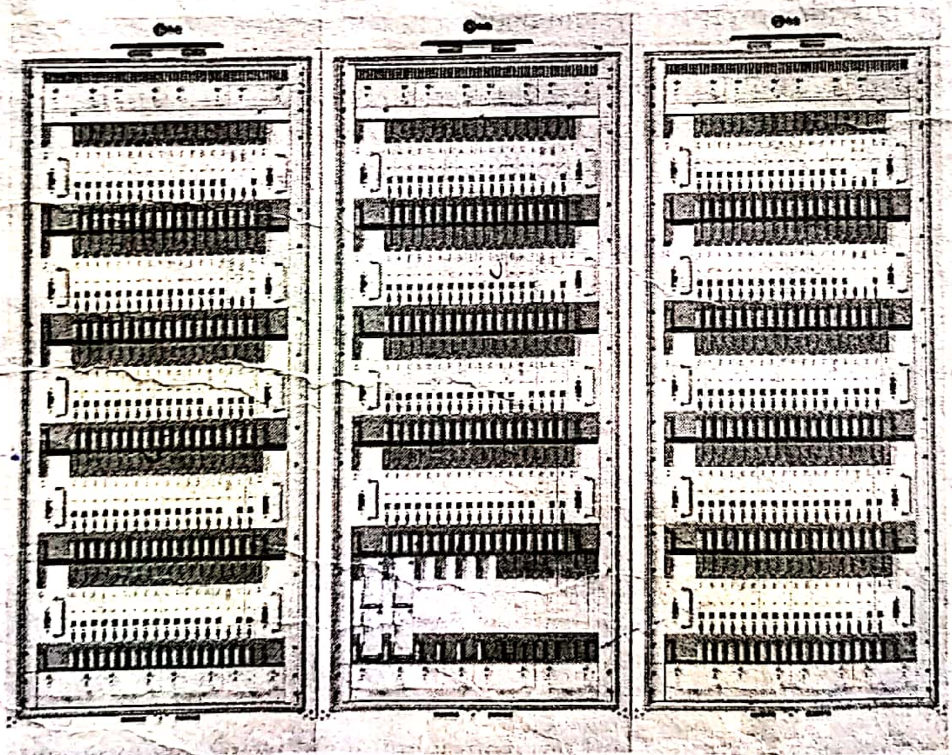


Figure 3–4 Typical cellular wireless equipment (BSC, TRC, and RBS) (Courtesy of LG Electronics Corp.).

another common term used for the process of converting audio to a digital format suitable for cellular transmission.

Physically, these units (BSC, TRC, and RBSs) are contained in standard radio relay rack enclosures. Figure 3–4 shows what a typical system looks like. Within the rack enclosure are subsystems devoted to functions such as power supply and control, environmental conditioning, switching, communications, processing, and so on. Additional hardware details about cellular base station systems will be presented in Chapters 5 through 8.

Radio Base Station

The **radio base station** consists of all radio and transmission interface equipment needed to establish a radio link with the MS. The typical RBS is composed of several subsystems that allow it to transmit to the MS on one frequency and to receive signals from the MS on another frequency. The two major wireless cellular systems used today for the air interface function are a form of either time division multiple access (TDMA) or code division multiple access (CDMA). The architecture and functionality of the air interface components of the RBS will depend upon the particular type of access system it is used in.

For TDMA systems, since frequency spectrum is a scarce resource, the primary function of the BSS is to optimize the use of available frequencies. The RBS supports this goal by having the ability to perform frequency hopping and support dynamic power regulation and the use of discontinuous transmission modes. All of these features tend to reduce interference levels within a TDMA system. For CDMA systems, all transmission is performed on the same frequency. However, precise timing, power control, and CDMA encoding and decoding are required to optimize system operation. The necessary subsystem components required for the proper functioning of a CDMA radio base station reflect this fact.

TDMA Radio Base Stations A typical TDMA radio base station consists of a distribution switch and an associated processor that is used to cross-connect individual timeslots of an incoming data stream to the correct transceiver units and provide overall system synchronization, multiple transceiver units (one per timeslot) with the ability to perform RF measurements on received signals, RF combining and distribution units to combine the output signals from the transceiver units and also distribute received signals to all the transceivers, an energy control unit to supervise and control the system power equipment and also to regulate the environmental conditions of the RBS, and power supply components (both rectified AC and battery-supplied DC) to provide power for system operation.

CDMA Radio Base Stations A typical CDMA radio base station consists of many of the same switching function, RF transceiver, power supply, and environmental conditioning components as the TDMA radio base station with the addition of a timing and frequency module that receives timing information from a **Global Positioning System** (GPS) receiver colocated with the RBS and channel cards that are responsible for the CDMA encoding and decoding functions on the forward and reverse links to and from the subscriber devices. For CDMA radio base stations, a typical design might consist of a main and a remote unit. The main unit provides all the functions except for RF power amplification. The two units are linked by fiber-optic communications cables and power supply cables. These cables supply all the signals needed by the high-power RF amplifier and the remote electronics that are typically mounted on a tower near the system antenna.

Base Station Controller

Base Station Controller

The **base station controller** functions as the interface between the mobile switching center and the **packet core network** (PCN) and all of the radio base stations controlled by the BSC. The PCN is a term used for the interface node (network element) between the BSC and the public data network. Figure 3–5 shows how the systems are interconnected.

Aside from the necessary power supply and environmental conditioning components, the BSC typically consist of several subsystems all colocated in a main cabinet or possibly several cabinets. The system organization tends to divide up these subsystems into those that are used to provide a connection or link between the MSC and the radio base stations and those subsystems that control the operation of these aforementioned units. The typical connection from BSC to the MSC or TRC (if it is not integrated into the BSC) is over standard T1/E1/J1 PCM links as is the connection from BSC to RBSs. A standard switching fabric is used within the BSC to direct incoming voice calls from the MSC to the correct RBS. Another switching fabric that can deal with subrate transmissions (less than 64 kbps) is usually also available within the BSC adding increased functionality to the system. If the TRC is colocated with the BSC, transcoding functions are also performed within the combined BSC/TRC unit.

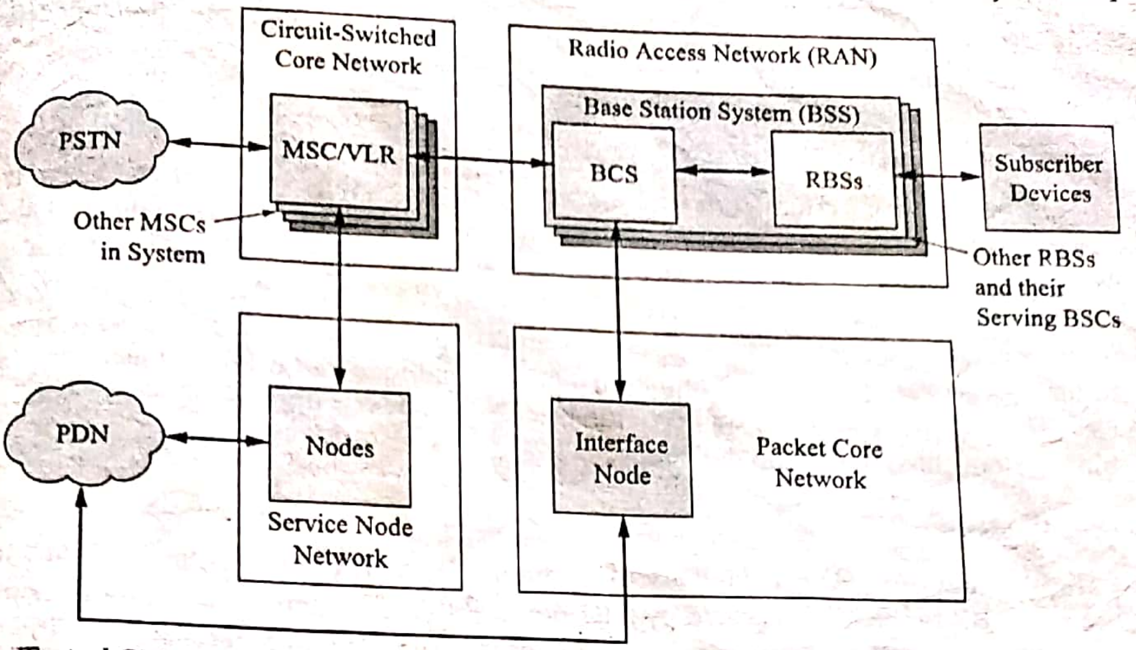


Figure 3–5 Typical CDMA wireless system (Courtesy of Ericsson).

The operation of each of these subsystems is controlled by processors under stored program control. Furthermore, the BSC system provides timing signals and connectivity to every subsystem within it and computer interfaces to the entire system for either network or element (subsystem) management functions.

Additionally, the BSC will supply signaling toward the MSC using message transfer part (MTP) protocol to transfer the messages over a PCM link connected to SS7 signaling terminals located within the MSC and the BSC. Signaling between the BSC and the RBSs is done over a PCM link using link access protocol on D-channel modified for mobile (LAPDm) signaling functions.

Connections to the PDN through an interface unit (PCN) connected to the BSC will be discussed in greater length and detail in Chapter 7.

Transcoder Controller

The **Transcoder Controller** (TRC) consists of subsystems that perform transcoding and rate adaptation. The TRC can be either a stand-alone unit or, more commonly, combined with the BSC to yield an integrated BSC/TRC. The TRC also can support the power saving option of discontinuous transmission. If pauses in speech are detected, the mobile station will discontinue transmission and the TRC will generate "comfort noise" back toward the MSC/VLR. An integrated BSC/TRC can typically handle many 100s of RBS transceivers.

Both TDMA and CDMA systems transmit speech over the air interface using digital encoding techniques that yield data rates of less than 16 kbps. The PSTN uses a PCM encoding scheme that yields a data rate for voice of 64 kbps. Therefore, voice messages coming from the PSTN must be transcoded to a rate suitable for the cellular system and, similarly, voice messages originating from a mobile station must be transcoded into a format suitable for the PSTN. This operation takes place in the TRC. The incoming PCM signal from the PSTN is converted back to an analog signal. At this point, 20-ms segments of the analog signal are converted to a digital code by a device known as a **vocoder.** The vocoder compares the 20-ms speech segment against a table of values. The entry in the table that is closest to the actual value is used to produce a code word that is much shorter than the corresponding PCM codes for the same 20-ms period. This compressed code word is what gets transmitted by the system. At the MS, the process is reversed to obtain an analog voice signal. For voice signals going in the opposite direction the steps are duplicated but in the reverse order. The obvious advantage to the use of vocoding is the reduced data rate needed for speech transmission. Additional enhancements to this process have led to half-rate speech coders that encode speech signals in only 8 kbps, and other variations on this theme.

Swiching System Components

As stated earlier, the switching system performs several necessary cellular network functions. It provid the interface (MSC) both to the radio network portion of the system (BSS) and to the PSTN and oth PLMNs. It also provides an interface to the PDN and other network support nodes and gateways. Includ in the switching system are functional databases (HLR, VLR, AUC/EIR, etc.) that contain informatio about the system's subscribers, their network privileges and supplementary services, present SDs locatio and other information necessary to locate, authenticate, and maintain radio link connections to the su scriber's devices. The following sections will provide brief overviews of the functions and operation of t various switching system subsystems and databases.

Visitor Location Register

The **visitor location register** (VLR) is a database that temporarily stores information about any mobile sta tion that attaches to a RBS in the area serviced by a particular MSC. This temporary subscriber informatio is required by the MSC to provide service to a visiting subscriber. When an MS registers with a new MS service area, the new VLR will request subscriber information from the MS's home location registe (HLR). The HLR sends the subscriber information to the VLR and now if the MS either sends or receives call the VLR already has the information needed for call setup. In a typical wireless network the VLR i integrated with the MSC to form an MSC/VLR thus reducing the amount of SS7 network signaling nece sary to perform wireless network operations.

Mobile Switching Center

The **mobile switching center** (MSC) is at the center of the cellular switching system. It is responsible for the setting up, routing, and supervision of voice calls to and from the mobile station to the PSTN. These functions are equivalent to those performed by the traditional telephony circuit switch (e.g., 5ESS, DMS-100/200, and AXE 810) used in a central office by the wireline PSTN. The traditional equipment manufacturers of this type of switching system all sell a cellular version of their standard wireline switch. Most of these systems also combine VLR functionality, in addition to the telephony switching functions, yielding an integrated MSC/VLR system.

The basic functions performed by the MSC/VLR are as follows: the setting up and control of voice calls including subscriber supplementary services, providing voice path continuity through the use of the handoff process, call routing to a roaming subscriber, subscriber registration and location updating, subscriber data updating, authentication of MSs, delivery of short messages, signaling to other network elements (BSC, HLR, etc.) or networks (PSTN, PLMNs, etc.), and the performing of charging/accounting, statistical, and administrative input/output processing functions.

As shown in Figure 3–6, the typical MSC consists of the following components or subsystems devoted to network operations: a central processor and associate processors, group switch, traffic interfaces, timing and synchronization modules, and software to provide operations and maintenance (O&M) functions. The next several sections will provide some additional detail about the operation of a typical MSC.

MSC Interface and Switching Functions Today's "trunk" connections (i.e., high-capacity facilities) between local central office (CO) exchanges and gateways to long-distance provider facilities make available the transport of high bit-rate digital signals. These local and long-distance interoffice connections are most often supplied by fiber-optic cables that are carrying SONET-based optical signals at bit rates in the 100s of mbps range or higher (the STS-3 signal carried as OC-3 is 155.520 mbps). SONET is capable of transporting multiple T1/E1/J1 carriers and asynchronous transfer mode (ATM) traffic. The standard voice call is

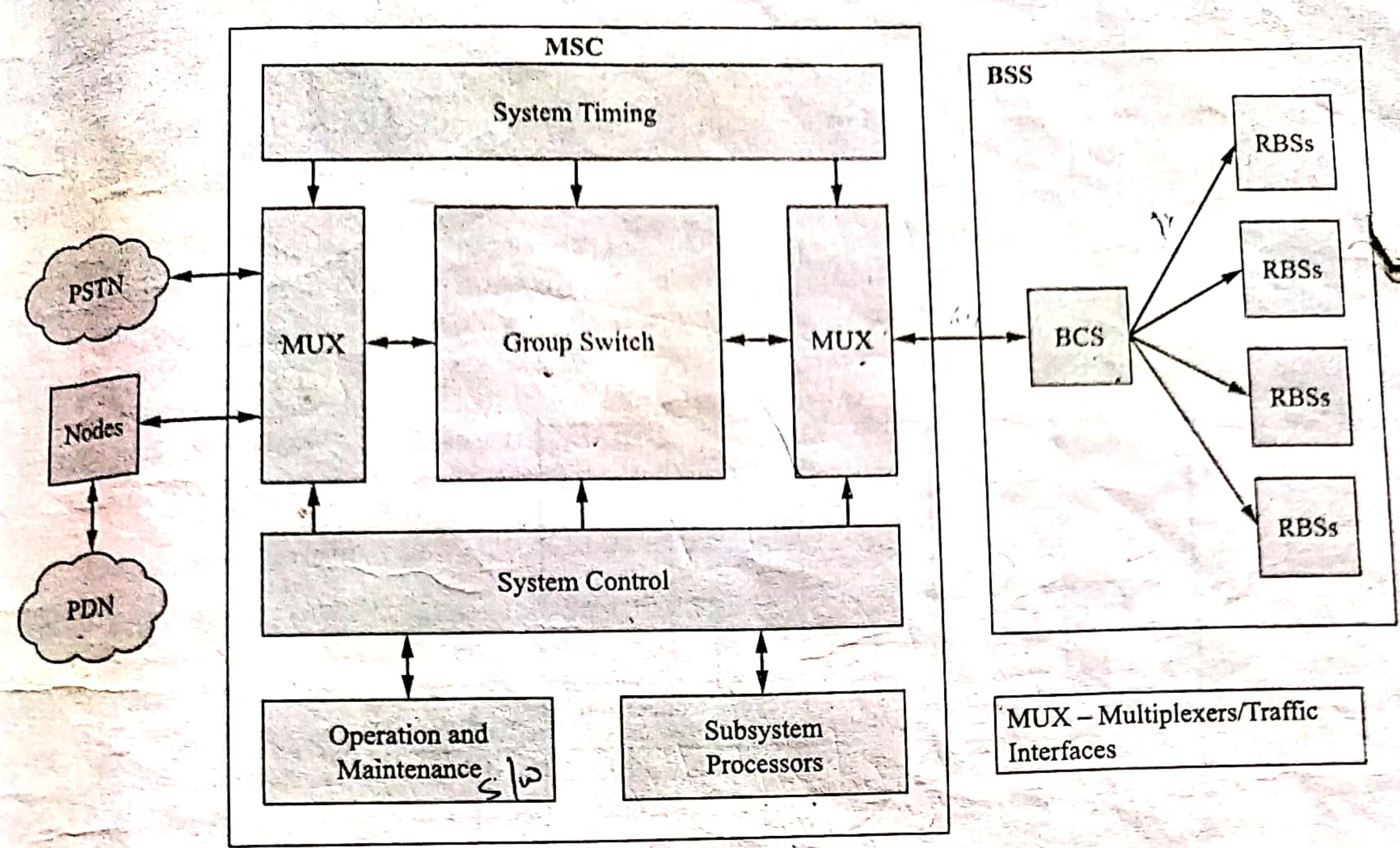


Figure 3–6 Typical MSC subsystems.

carried over these facilities as a DS0 signal that has a bit rate of 64 kbps. A T1/J1 carrier can transport twenty-four digitized voice calls and the E1 carrier has a capacity of thirty calls. The MSC can be thought of as just another central office exchange in that it has its own local exchange routing number(s) (i.e., N1/0N-NNX-XXXX where N1/0N is the three-digit area code and NNX is the exchange number). Therefore, the connection from the MSC to the PSTN or other PLMNs is usually provided in the same manner as other interoffice connections, over fiber trunk facilities or through traditional Tn/En/Jn carrier facilities depending upon the needed capacity.

Therefore, the MSC needs to provide the ability to multiplex and demultiplex signals to and from the PSTN. This functionality is built into the traffic interface subsystems (refer back to Figure 3–6). These interface units will bring the high bit-rate data streams down to the base T1/E1/J1 carrier signal after demultiplexing of the signals from the PSTN. Or conversely, they can be used to multiplex together many T1/E1/J1 signals to form a high bit-rate signal to be transmitted over a high-speed transmission facility back toward the PSTN (this operation is typically referred to as **backhaul**) or other networks as needed. The connection between the MSC and the base station controllers it services is also implemented with the same standard transmission T1/E1/J1 facilities or larger-capacity fiber facilities. Recently, cellular providers have been providing their own high-speed fixed point-to-point digital microwave backhaul networks with T1/E1/J1 or higher capacity from remote RBSs to BSCs and then from BSCs to the MSC location when traditional facilities are either not available or prove to be too costly to install and lease.

The **group switch** provides the same functionality in the MSC as it does in the PSTN local exchange. In both cases, the incoming voice calls on a particular T1/E1/J1 carrier arrive assigned to a particular timeslot. In order that the voice call can be directed to the correct BSC a combination space and timeslot interchange (TSI) switch must be used to redirect the voice call to both the correct output line and also to a free timeslot within the T1/E1/J1 carrier signal. The following example will describe the operation of a typical group switch in an MSC/VLR.

Example 3–1

A certain mobile subscriber is registered to a certain RBS in a cell that is located in an area that uses six BSCs to control the RBSs in that area. Show how the MSC directs an incoming call to the mobile subscriber if the MS's RBS is controlled by BSC #4.

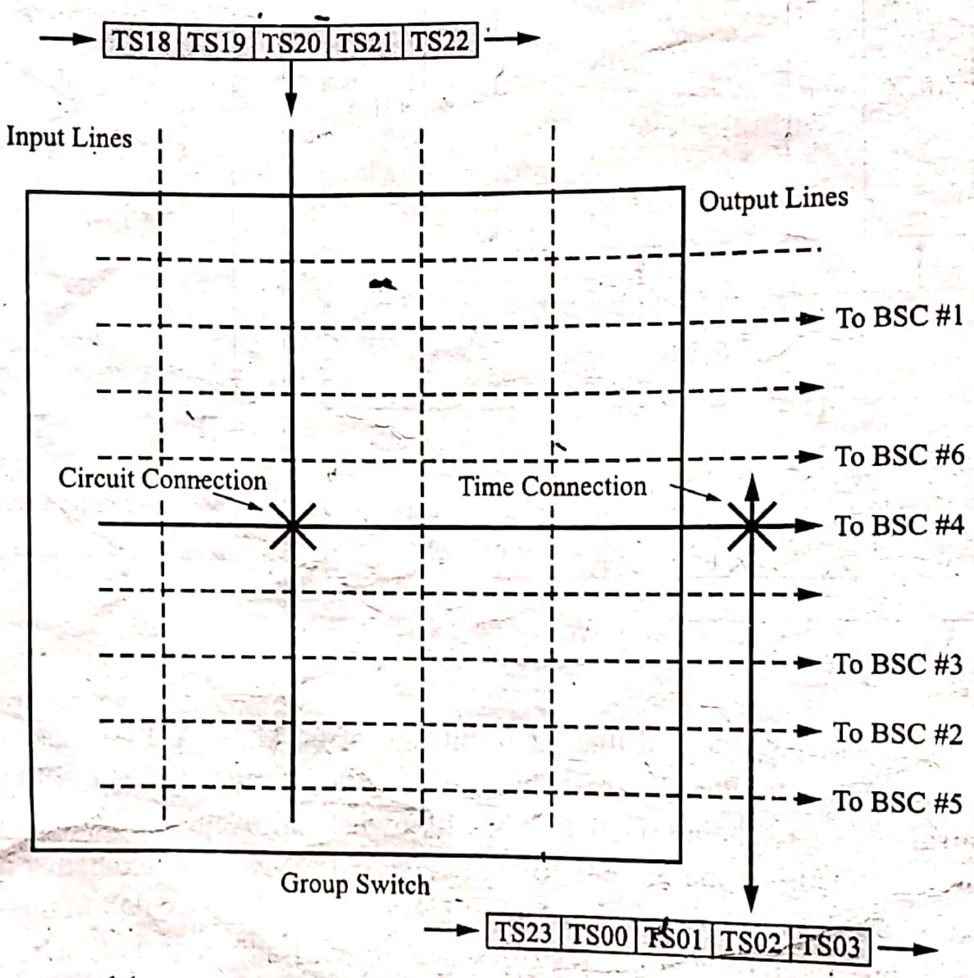


Figure 3–7 Operation of the group switch for Example 3–1.

Solution: Referring to Figure 3–7, assume that the incoming voice call occupies Timeslot #21 (any value from 0 to 23 could be used here) on a T1 carrier signal connected to a local exchange in the PSTN. After any necessary demultiplexing, the signal is applied to the group switch. The group switch processor implements a path that allows the signal to be redirected to available Timeslot #2 on the line connected to BCS #4 (this latter information is provided by the MSC). The switch performs this function as indicated by Figure 3–7 and the voice call is correctly routed toward BSC #4. The MSC and the BSC have been in contact by sending messages to one another over SS7 so that the BSC is aware of the new incoming voice call on Timeslot #2. Note that a functionally identical call path must also be established in the reverse direction to provide for duplex operation. There are duplicate subsystems available within the MSC to accomplish this task.

Home Location Register

The **home location register** (HLR) is a database that stores information about every user that has a cellular service contract with a specific wireless service provider. This database stores permanent data about the network's subscribers, information about the subscriber's contracted teleservices or supplementary services, and dynamic data about the subscriber's present location. The type of permanent data stored includes mobile station identification numbers that identify both the mobile equipment and the PSTN plan that it is associated with. This information would include a mobile station ID number that consists of a **country code**, either a national destination code or a number planning area code, and a subscriber number. Other ID numbers as defined and required by the particular wireless network are also stored by the HLR.

The HLR also plays a major role in the process of handling calls terminating at the MS. In this case, the HLR analyzes the information about the incoming call and controls the routing of the call. This function is usually supported by the transfer of information from the HLR to the VLR within the MSC where the subscriber's mobile is registered.

HLR Implementation and Operation An HLR can be implemented as a stand-alone network element or it can be integrated into an MSC/VLR to create an MSC/VLR/HLR system. The HLR itself consists of the following subsystems: storage, central processors, I/O system, and statistics and traffic measurement data collection. Additionally, SS7 signaling links are maintained between a network HLR and the MSC/VLRs and GMSC that compose a cellular network. Usually, a wireless service provider will have more than one HLR within a **public land mobile network** (PLMN) to provide the necessary redundancy to support disaster recovery. The information about subscriber subscriptions is usually entered into the HLR database through a service order gateway (SOG) or an operations support system (OSS) interface.

The HLR has two basic functions. It maintains databases of subscriber-related information. This information may consist of both permanent data such as subscriber-associated MS numbers and dynamic data such as location data. The HLR is able to support typical database operations like the printing and modification of subscriber data and the addition or deletion of subscribers. More complex operations like the handling of authentication and encryption information and the administration of MS roaming characteristics are also performed. The HLR also performs call handling functions such as the routing of mobile terminating calls, the handling of location updating, and procedures necessary for delivery of subscriber supplementary services.

HLR Subscription Profile A basic function of the HLR is to store a subscriber's profile. This profile defines a group of services that the subscriber has signed up for when first contracting for mobile service. The types of services available are typically referred to as **teleservices** (telephony, short message service, fax, etc.) and **bearer services** (i.e., data services). These services are typically grouped into basic service groups that are packaged for sales and promotion purposes. A user's profile stored by the HLR may be updated or modified at any time with vendor-specific computer commands or more easily by clicking on graphical user interface (GUI) icons in a Windows-based application program.

Supplementary services are system functions like call waiting and call holding, multiparty service, calling line and connected line identification, call forwarding, call barring, and so on. Within each of these categories, there are many options that may be selected. These supplementary services may be programmed into a user's profile fairly easily as mentioned earlier. As well as the normal services that may be specified by a particular system standard, systems will typically offer vendor-specific supplementary services that are used in an attempt to provide some form of marketplace differentiation.

HLR/AUC Interconnection The authentication center (AUC) provides authentication and encryption information for the MSs being used in the cellular network. For GSM systems, so-called triplets are provided for the authentication of a mobile. Upon a request from a VLR, the HLR will be delivered a **triplet** (i.e., a ciphering key, a random number, and a signed response) for a particular mobile subscriber. The HLR receives the triplet information in response to a request to the AUC for verification of a subscriber. The HLR forwards the random number to the MSC/VLR where it is passed on to the mobile. The mobile performs a calculation using the random number and returns it to the MSC/VLR and from there to the HLR. If the results are the same as the signed response, the mobile is **authenticated** and it is now able to access the radio resources of the network. The AUC contains a processor, a database for the storage of key information for each subscriber, maintenance functions for subscriber information, and an interface for communications with the HLR. CDMA systems use a similar system for authentication.

Interworking Location Register

Interworking location registers (ILRs) are used to provide for intersystem roaming. The ILR allows a subscriber to roam in several different systems. For instance, in a wireless cellular system using an appropriate ILR, a subscriber could roam between an AMPS system and a PCS system. In this case, the ILR would consist of an AMPS HLR and parts of a PCS VLR.

Authentication Center and Equipment Identity Register

The authentication center (AUC) is a database that is connected to the HLR. The authentication center provides the HLR with authentication parameters and **ciphering keys** for GSM systems. Using the cipher keys, signaling, speech, and data are all encrypted before transmission over the air interface. The use of encryption provides over-the-air security for the system.

The equipment identity register (EIR) database is used to validate the status of mobile equipment. In GSM systems, the MSC/VLR can request the EIR to check the current status of an MS through the global database maintained by the GSM Association. This global database is updated daily to reflect the current status of an MS. The MS can be "black listed" indicating that it has been reported stolen or missing and thus not approved for network operation. Or, the MS might be "white listed" and therefore registered and approved for normal operation. The hardware necessary to perform AUC/EIR functions might be colocated within a wireless network.