Introduction to GSM

Uplink/Downlink FDMA Frequencies Number Identifiers MSISDN IMSI IMEI IMEISV

Home

Introduction

GSM is an acronym that stands for **Global System for Mobile Communications**. The original french acronym stands for *Groupe Spécial Mobile*. It was originally developed in 1984 as a standard for a mobile telephone system that could be used across Europe.

GSM is now an international standard for mobile service. It offers high mobility. Subscribers can easily roam worldwide and access any GSM network.

GSM is a digital cellular network. At the time the standard was developed it offered much higher capacity than the current analog systems. It also allowed for a more optimal allocation of the radio spectrum, which therefore allows for a larger number of subscribers.

GSM offers a number of services including voice communications, Short Message Service (SMS), fax, voice mail, and other supplemental services such as call forwarding and caller ID.

Currently there are several bands in use in GSM. 450 MHz, 850 MHZ, 900 MHz, 1800 MHz, and 1900 MHz are the most common ones.

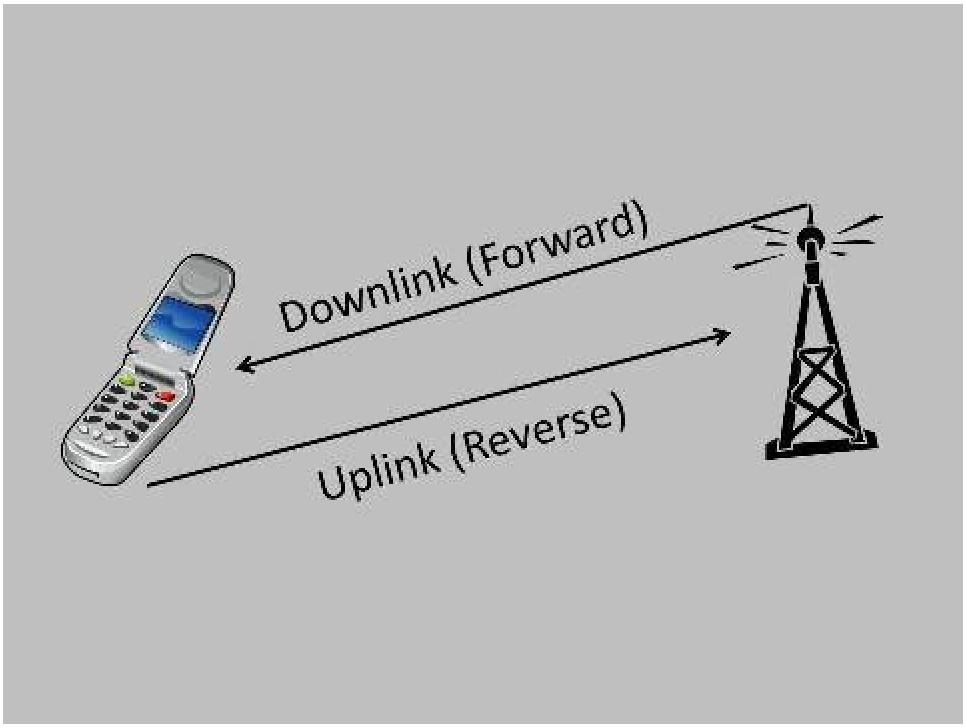
Some bands also have *Extended GSM (EGSM)* bands added to them, increasing the amount of spectrum available for each band.

GSM makes use of Frequency Division Multiple Access (FDMA) and Time Division Multiple Access (TDMA).
*TDMA will be discussed later

[Back to Top]

Uplinks/Downlinks & Reverse Forward

GSM allows for use of duplex operation. Each band has a frequency range for the uplink (cell phone to tower) and a separate range for the downlink (tower to the cell phone). The uplink is also known as the *Reverse* and the downlink is also known as the *Forward*. In this tutorial, I will use the terms uplink and downlink.



Uplink and Downlink

[Back to Top]

Frequency Division Multiple Access (FDMA)

GSM divides the allocated spectrum for each band up into idividual carrier frequencies. Carrier separation is 200 khz. This is the FDMA aspect of GSM.

Absolute Radio Frequency Channel Number (ARFCN)

The ARFCN is a number that describes a pair of frequencies, one uplink and one downlink. The uplink and downlink frequencies each have a bandwidth of 200 kHz. The uplink and downlink have a specific *offset* that varies for each band. The offset is the frequency separation of the uplink from the downlink. Every time the ARFCN increases, the uplink will increase by 200 khz and the downlink also increases by 200 khz.

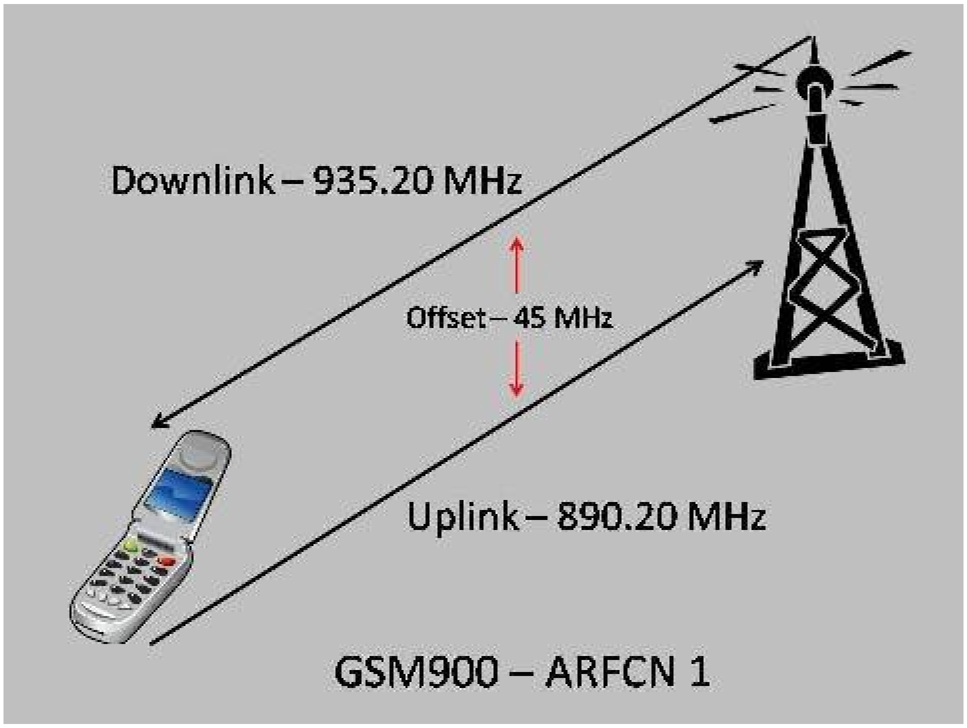
*Note: Although GSM operates in duplex (separate frequencies for transmit and receive), the mobile station does not transmit and receive at the same time. A switch is used to toggle the antenna between the transmitter and receiver.

The following table summarizes the frequency ranges, offsets, and ARFCNs for several popular bands.

	GSM 450	EGSM450	GSM850	GSM900	EGSM900	GSM1800	GSM1900
Uplink Freq. Range	450 to 458 MHz	478 to 486 MHz	824 to 849 MHz	890 to 915 MHz	880 to 915 MHz	1710 to 1785 MHz	1850 to 1910 MHz
Downlink Freq. Range	460 to 468 MHz	488 to 496 MHz	869 to 894 MHz	935 to 960 MHz	925 to 960 MHz	1805 to 1880 MHz	1930 to 1990 MHz
ARFCN	259 to 293	306 to 340	128 to 251	1 to 124	0 to 124 & 975 to 1023	512 to 885	512 to 810
Offset	10 MHz	10 MHz	45 MHz	45 MHz	45 MHz	95 MHz	80 MHz

GSM Bands

The following diagram illustrates an ARFCN with paired uplink and downlink frequencies for ARFCN 1 in the GSM 900 band.



GSM900 ARFCN 1

[Back to Top]

Calculating Uplink/Downlink Frequencies

The following is a way to calculate the uplink and downlink frequencies for some of the bands, given the band, the ARFCN, and the offset.

GSM 900

Up = 890.0 + (ARFCN * .2)
Down = Up + 45.0

example:

Given the ARFCN 72, and we know the offset is 45MHz for the GSM900 band:
Up = 890.0 + (72 * .2)
Up = 890.0 + (14.4)
Up = 904.40 MHz

Down = Up + Offset
Down = 904.40 + 45.0
Down = 949.40 MHz

The uplink/downlink pair for GSM900 ARFCN72 is 904.40/949.40 (MHz)

Here are the formulas for EGSM900, DCS1800, and PCS1900:

EGSM900

Up = 890.0 + (ARFCN * .2)
Down = Up + 45.0

DCS1800

Up = 1710.0 + ((ARFCN - 511) * .2)
Down = Up + 95.0

PCS1900

Up = 1850.0 + ((ARFCN - 512) * .2)
Down = Up + 80.0

[Back to Top]

Numbering System (Identifiers)

Mobile Subscriber ISDN (MSISDN)

The MSISDN is the subscriber's phone number. It is the number that another person would dial in order to reach the subscriber. The MSISDN is composed of three parts:
Country Code (CC)
National Destination Code (NDC)
Subscriber Number (SN)

MSISDN		
CC	NDC	SN

MSISDN

Country Code (CC) - This is the international dialing code for whichever country the

MS is registered to.

National Destination Code (NDC) - In GSM, an NDC is assigned to each PLMN. In many cases, a PLMN may need more than one NDC.

Subscriber Number (SN) - This is a number assigned to the subscriber by the service provider (PLMN).

The combination of the NDC and the SN is known as the National (significant) Mobile Number. This number identifies a subscriber within the GSM PLMN.

National (significant) Mobile Number	
NDC	SN

National (significant) Mobile Number

[Back to Top]

International Mobile Subscriber Identity (IMSI)

The IMSI is how the subscriber is identified to the network. It uniquely identifies the subscriber within the GSM global network. The IMSI is burned into the SIM card when the subscriber registers with PLMN service provider. The IMSI is composed of three parts:

Mobile Country Code (MCC)
Mobile Network Code (MNC)
Mobile Subscriber Identification Number (MSIN)

IMSI		
MCC	MNC	MSIN
3 digits	2 or 3 digits	Max 10 digits
<----------------------- Not to Exceed 15 Digits ----------------------->		

IMSI

Mobile Country Code (MCC) - This number identifies which country the subscriber's network is in. It has 3 digits.

Mobile Network Code (MNC) - This number identifies the home GSM PLMN of the subscriber (Cingular, T-Mobile, etc.). It has 2 or 3 digits. Some networks may have more than one MNC allocated to it.

Mobile Subscriber Identification Number (MSIN) - This number uniquely identifies a user within the home GSM network.

[Back to Top]

International Mobile Equipment Identity (IMEI)

The IMEI uniquely identifies the Mobile Equipment itself. It is essentially a serial number that is burned into the phone by the manufacturer. The IMEI is composed of three parts:

Type Allocation Code (TAC) - 8 digits
Serial Number (SNR) - 6 digits
Spare (SP) - 1 digit

IMEI		
TAC	SNR	Spare
8 Digits	6 Digits	1 Digit

IMEI

Type Allocation Code (TAC) - This number uniquely identifies the model of a wireless device. It is composed of 8 digits. Under the new system (as of April 2004), the first two digits of a TAC are the *Reporting Body Identifier* of the GSMA approved group that allocated this model type.

Serial Number (SNR) - This number is a manufacturer defined serial number for the model of wireless device.

Spare (SP) This number is a check digit known as a *Luhn Check Digit*. It is omitted during transmission within the GSM network.

On many devices the IMEI number can be retrieved by entering *#06#

Former IMEI Structure

Prior to April, 2004 the IMEI had a different structure:

Type Allocation Code (TAC) - 6 digits
Factory Assembly Code (FAC) - 2 digits
Serial Number (SNR) - 6 digits
Spare (SP) - 1 digit

IMEI			
TAC	FAC	SNR	Spare
6 Digits	2 Digits	6 Digits	1 Digit

Former IMEI Structure

As of April 2004, the use of the FAC was no longer required. The current practice is for the TAC for a new model to get approved by national regulating bodies, known as the *Reporting Body Identifier*.

[Back to Top]

International Mobile Equipment Identity/Software Version (IMEISV)

This is a newer form of the IMEI that omits the Spare digit at the end and adds a 2-digit *Software Version Number (SVN)* at the end. The SVN identifies the software version that the wireless device is using. This results in a 16-digit IMEI.

Type Allocation Code (TAC) - 8 digits
Serial Number (SNR) - 6 digits
Software Version Number (SVN) - 2 digits

IMESV		
TAC	SNR	SVN
8 Digits	6 Digits	2 Digits

IMEISV

Network Architecture

Home

GSM Network Architecture

A GSM network is made up of multiple components and interfaces that facilitate sending and receiving of signalling and traffic messages. It is a collection of transceivers, controllers, switches, routers, and registers.

A Public Land Mobile Network (PLMN) is a network that is owned and operated by one GSM service provider or administration, which includes all of the components and equipment as described below. For example, all of the equipment and network resources that is owned and operated by Cingular is considered a PLMN.

Mobile Station (MS)

The Mobile Station (MS) is made up of two components:

Mobile Equipment (ME) This refers to the physical phone itself. The phone must be able to operate on a GSM network. Older phones operated on a single band only. Newer phones are dual-band, triple-band, and even quad-band capable. A quad-band phone has the technical capability to operate on any GSM network worldwide.

Each phone is uniquely identified by the *International Mobile Equipment Identity* (IMEI) number. This number is burned into the phone by the manufacturer. The IMEI can usually be found by removing the battery of the phone and reading the panel in the battery well.

It is possible to change the IMEI on a phone to reflect a different IMEI. This is known as IMEI spoofing or IMEI cloning. This is usually done on stolen phones. The average user does not have the technical ability to change a phone's IMEI.

Subscriber Identity Module (SIM) - The SIM is a small smart card that is inserted into the phone and carries information specific to the subscriber, such as *IMSI, TMSI, Ki* (used for encryption), Service Provider Name (SPN), and *Local Area Identity* (LAI). The SIM can also store phone numbers (MSISDN) dialed and received, the *Kc* (used for encryption), phone books, and data for other applications. A SIM card can be removed from one phone, inserted into another GSM capable phone and the subscriber will get the same service as always.

Eadch SIM card is protected by a 4-digit Personal Identification Number (PIN). In order to unlock a card, the user must enter the PIN. If a PIN is entered incorrectly three times in a row, the card blocks itself and can not be used. It can only be unblocked with an 8-digit Personal Unblocking Key (PUK), which is also stored on the SIM card.

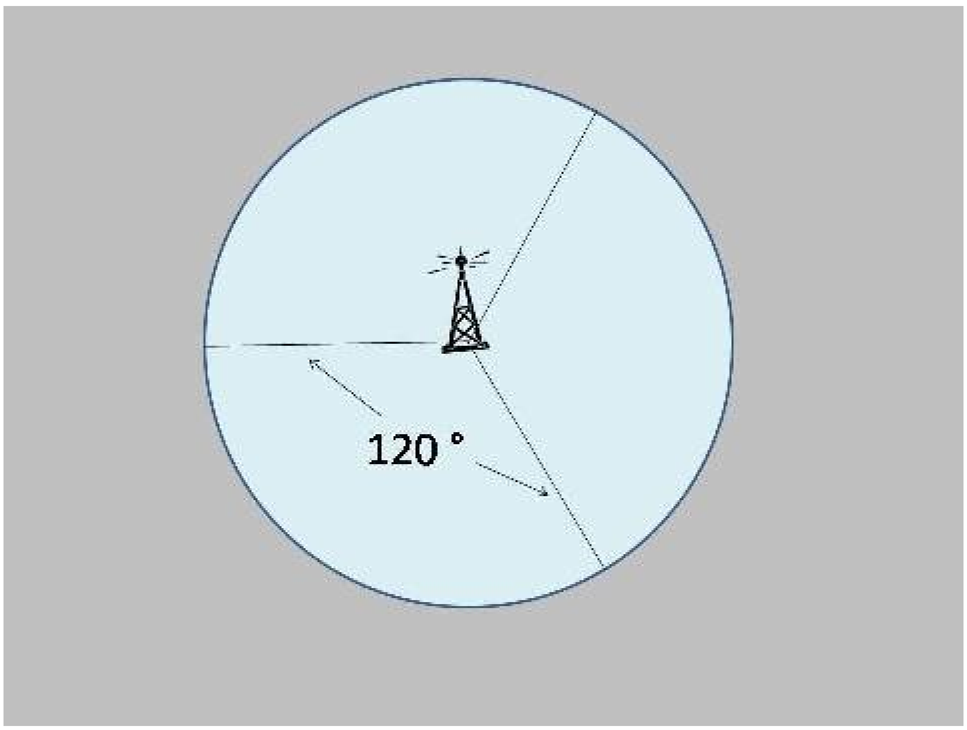
[Back to Top]

Base Transceiver Station (BTS)

Base Transceiver Station (BTS) - The BTS is the Mobile Station's access point to the network. It is responsible for carrying out radio communications between the network and the MS. It handles speech encoding, encryption, multiplexing (*TDMA*), and modulation/demodulation of the radio signals. It is also capable of frequency hopping. A BTS will have between 1 and 16 Transceivers (TRX), depending on the geography and user demand of an area. Each TRX represents one ARFCN.

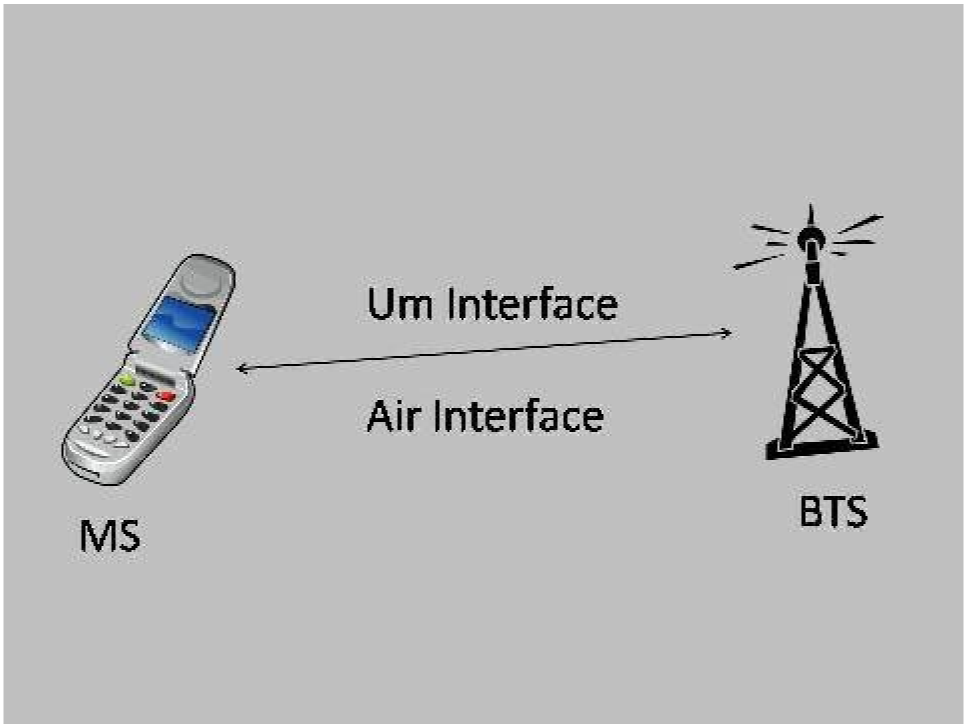
One BTS usually covers a single 120 degree sector of an area. Usually a tower with 3 BTSs will accomodate all 360 degrees around the tower. However, depending on geography and user demand of an area, a cell may be divided up into one or two sectors, or a cell may be serviced by several BTSs with redundant sector coverage.

A BTS is assigned a *Cell Identity*. The cell identity is 16-bit number (double octet) that identifies that cell in a particular *Location Area*. The cell identity is part of the Cell Global Identification (CGI), which is discussed in the section about the Visitor Location Register (VLR).



120 ° Sector

The interface between the MS and the BTS is known as the *Um Interface* or the *Air Interface*.



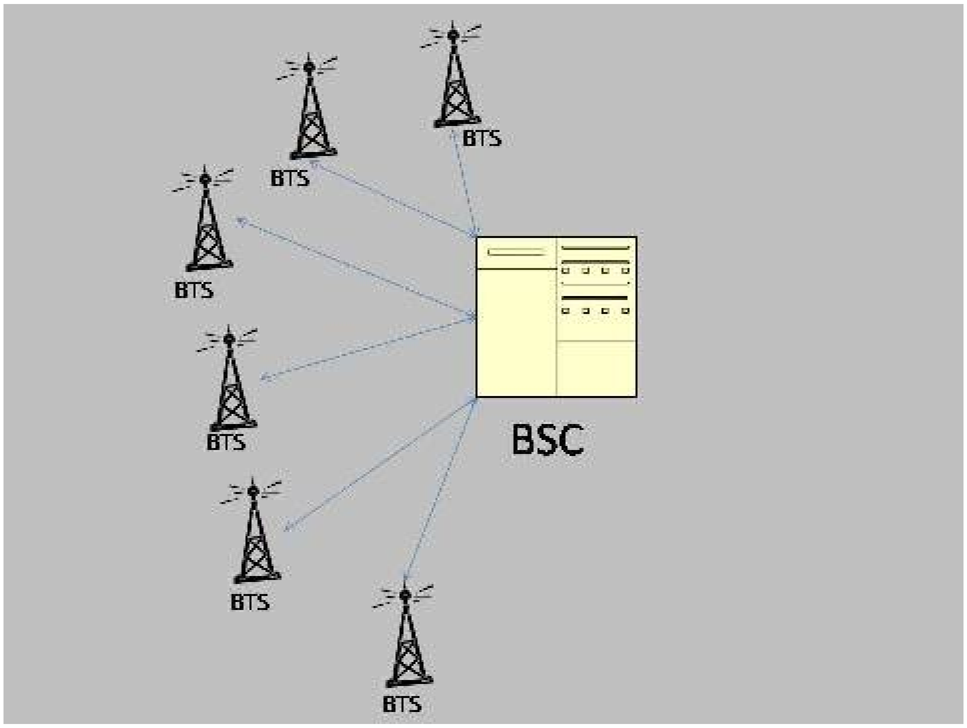
Um Interface

[Back to Top]

Base Station Controller (BSC)

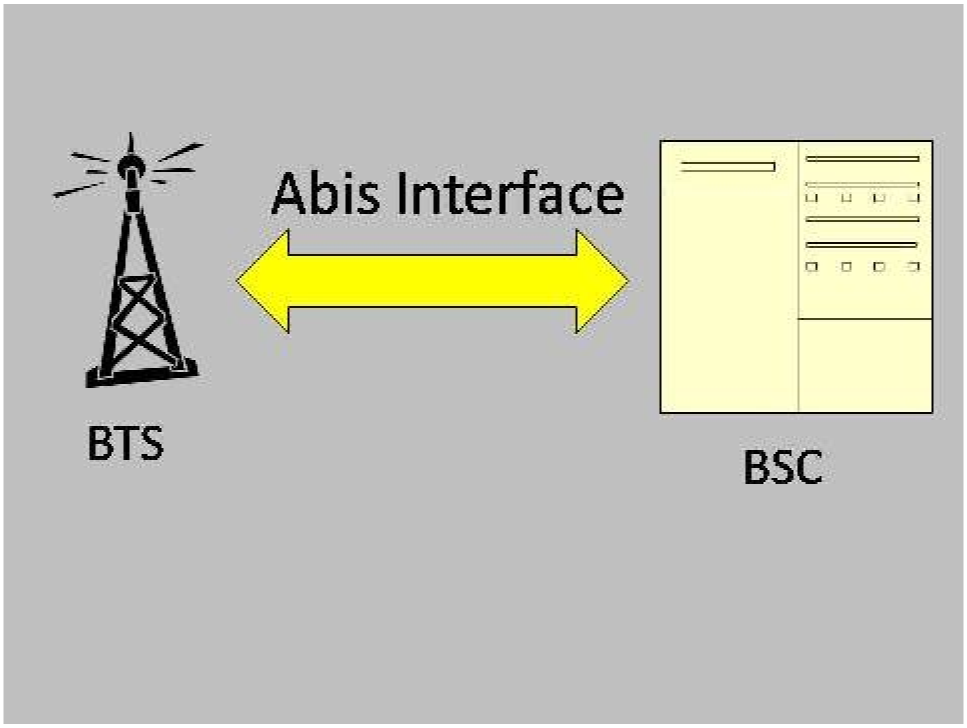
Base Station Controller (BSC) - The BSC controls multiple BTSs. It handles allocation of radio channels, frequency administration, power and signal measurements from the MS, and handovers from one BTS to another (if both BTSs are controlled by the same BSC). A BSC also functions as a "funneler". It reduces the number of connections to the *Mobile Switching Center* (MSC) and allows for higher capacity connections to the MSC.

A BSC my be collocated with a BTS or it may be geographically separate. It may even be collocated with the Mobile Switching Center (MSC).



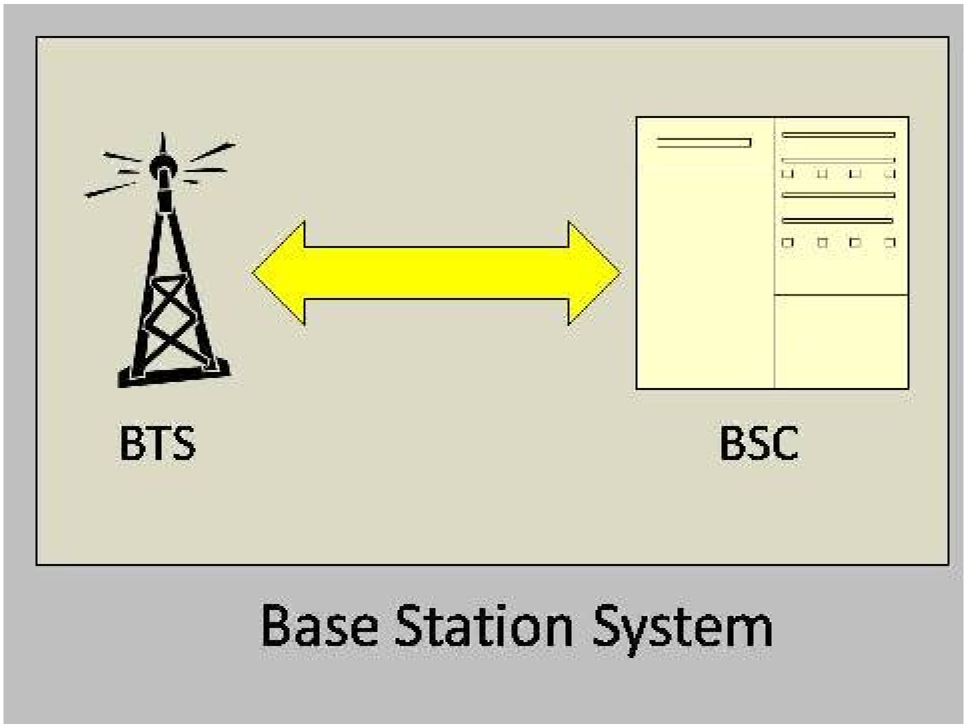
Base Station Controller

The interface between the BTS and the BSC is known as the *Abis Interface*



Abis Interface

The Base Transceiver Station (BTS) and the Base Station Controller (BSC) together make up the *Base Station System* (BSS).

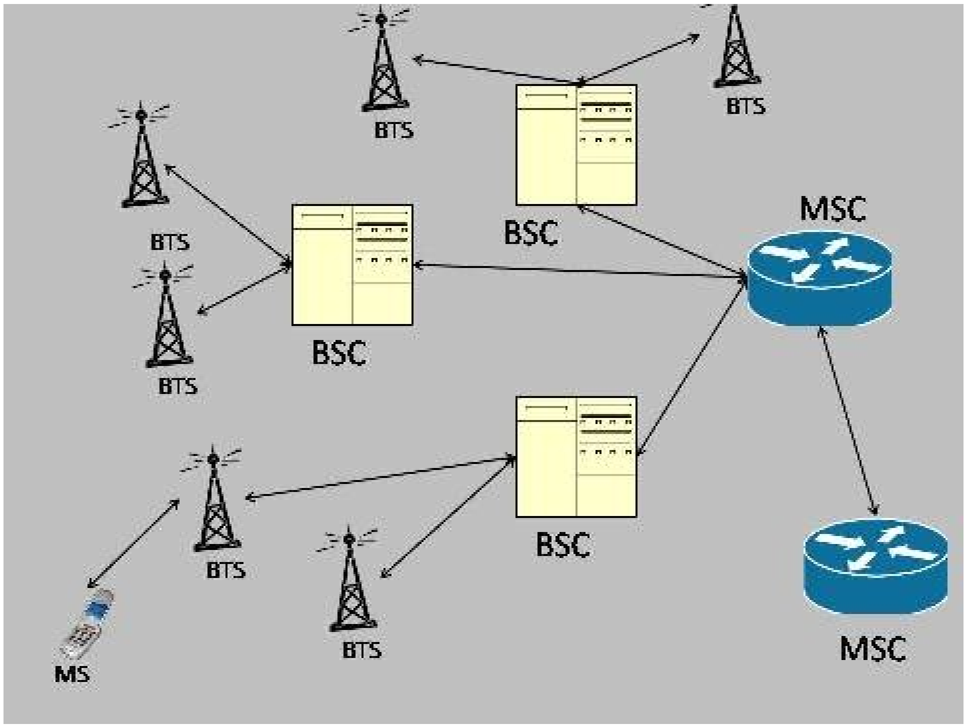


Base Station System

[Back to Top]

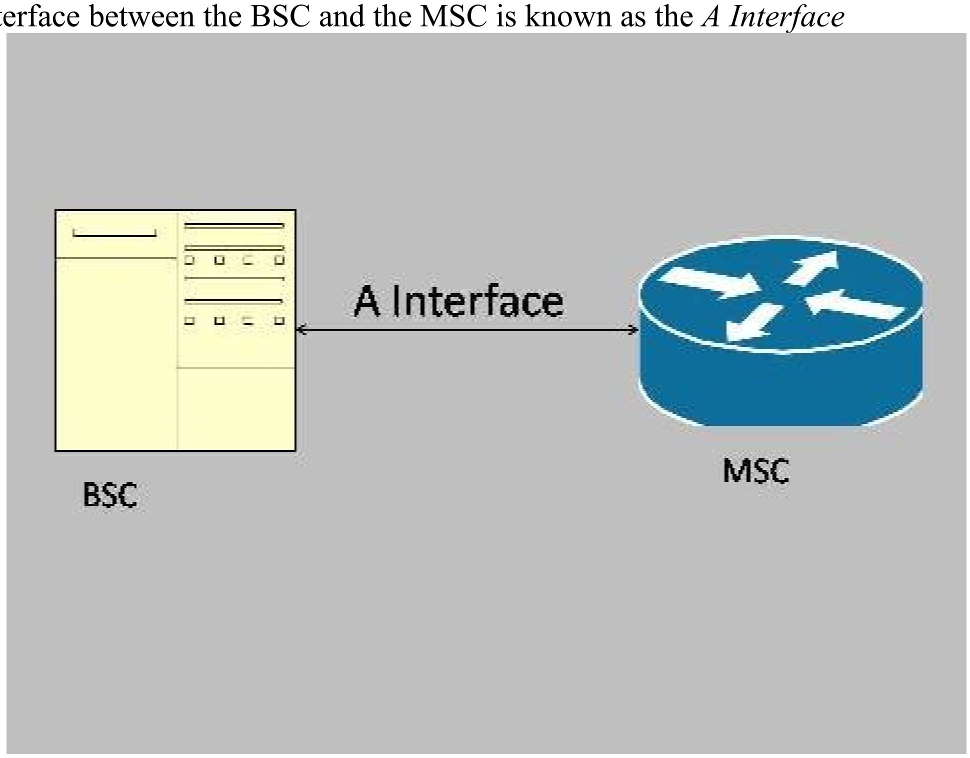
Mobile Switching Center (MSC)

Mobile Switching Center (MSC) - The MSC is the heart of the GSM netowrk. It handles call routing, call setup, and basic switching functions. An MSC handles multiple BSCs and also interfaces with other MSC's and registers. It also handles iner-BSC handoffs as well as coordinates with other MSC's for inter-MSC handoffs.



Mobile Switching Center

The interface between the BSC and the MSC is known as the *A Interface*

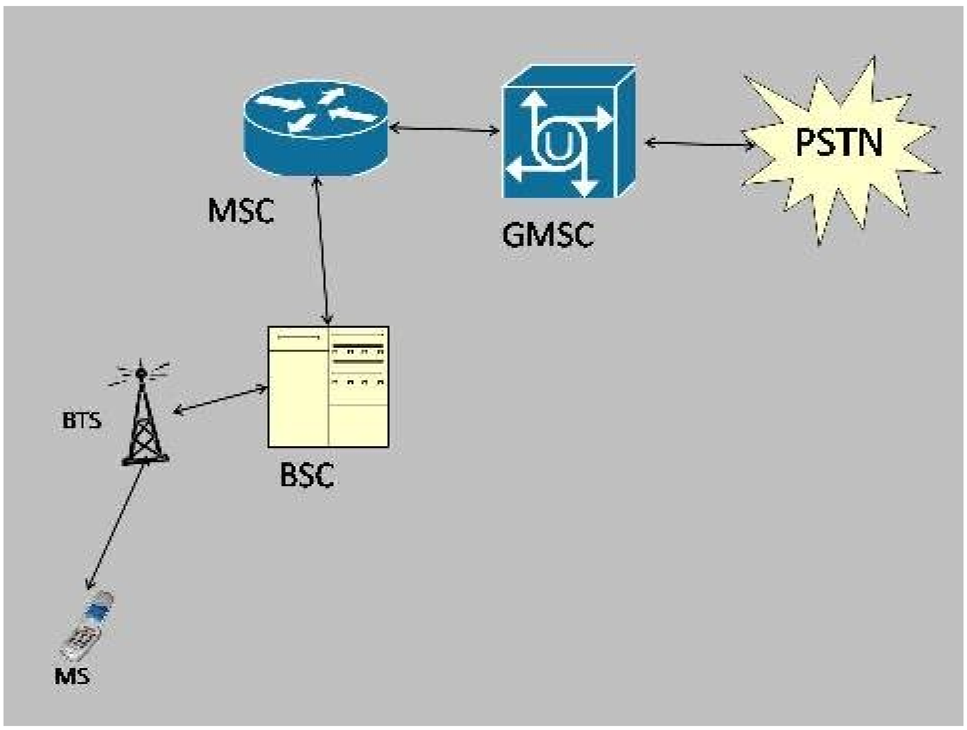


A Interface

[Back to Top]

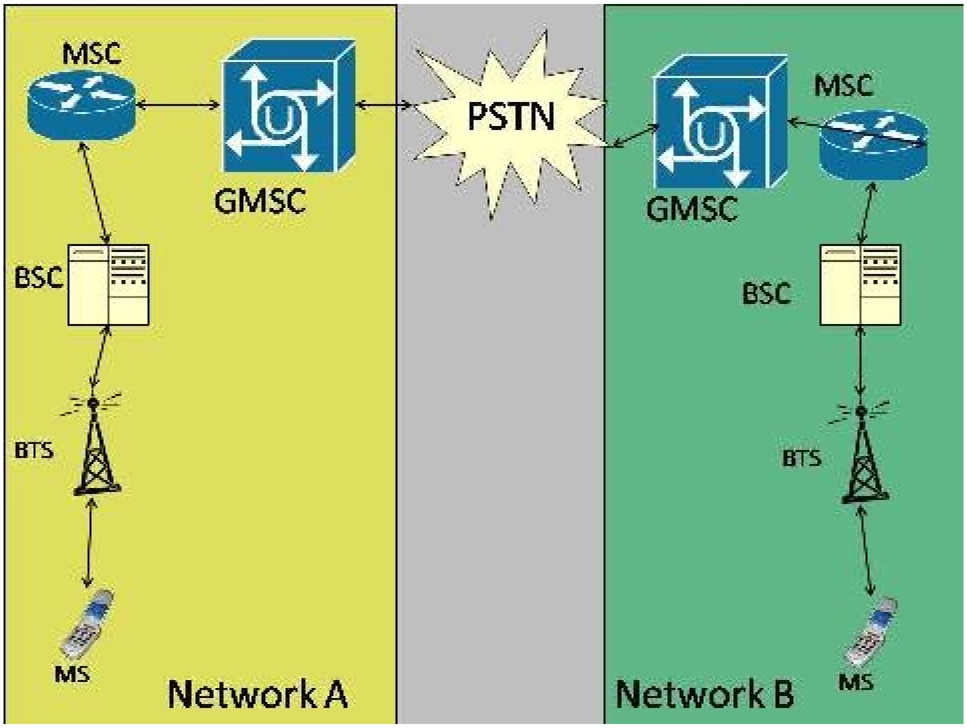
Gateway Mobile Switching Center (GMSC)

There is another important type of MSC, called a Gateway Mobile Switching Center (GMSC). The GMSC functions as a gateway between two networks. If a mobile subscriber wants to place a call to a regular landline, then the call would have to go through a GMSC in order to switch to the Public Switched Telephone Network (PSTN).



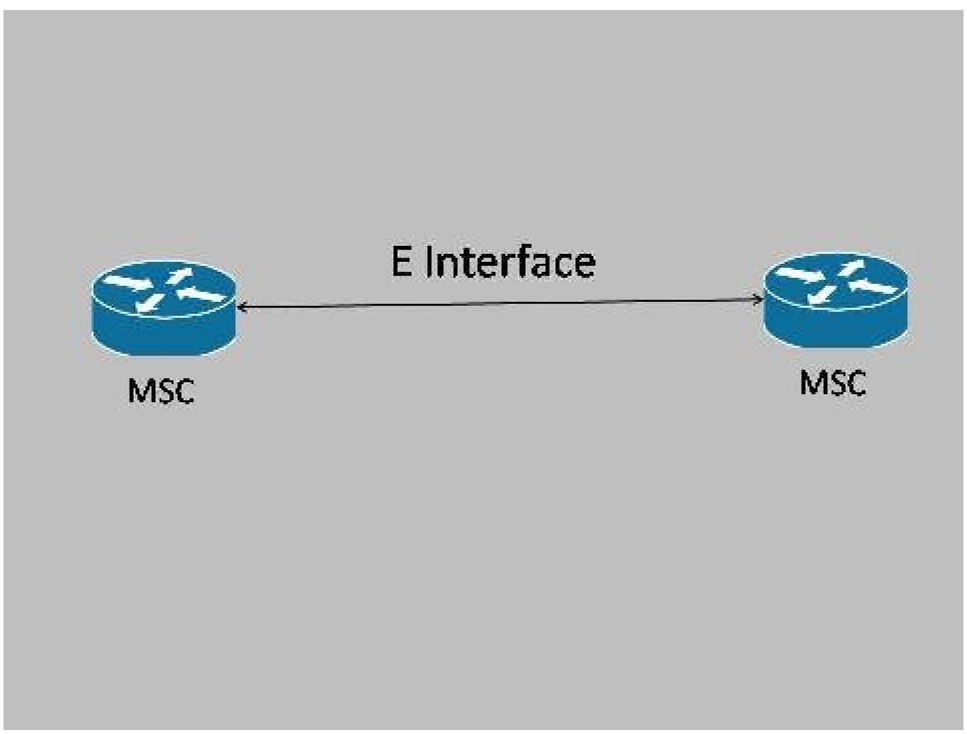
Gateway Mobile Switching Center

For example, if a subscriber on the Cingular network wants to call a subscriber on a T-Mobile network, the call would have to go through a GMSC.



Connections Between Two Networks

The interface between two Mobile Switching Centers (MSC) is called the *E Interface*



E Interface

[Back to Top]

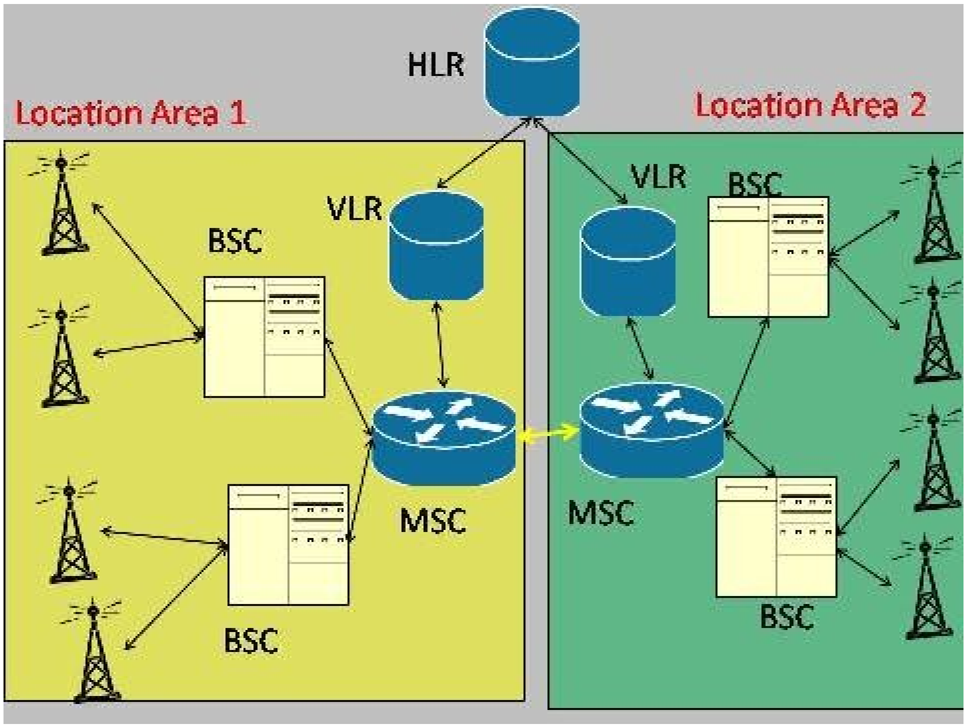
Home Location Register (HLR)

Home Location Register (HLR) - The HLR is a large database that permanently stores data about subscribers. The HLR maintains subscriber-specific information such as the MSISDN, IMSI, current location of the MS, roaming restrictions, and subscriber supplemental feautures. There is logically only one HLR in any given network, but generally speaking each network has multiple physical HLRs spread out across its network.

[Back to Top]

Visitor Location Register (VLR)

Visitor Location Register (VLR) - The VLR is a database that contains a subset of the information located on the HLR. It contains similar information as the HLR, but only for subscribers currently in its Location Area. There is a VLR for every Location Area. The VLR reduces the overall number of queries to the HLR and thus reduces network traffic. VLRs are often identified by the Location Area Code (LAC) for the area they service.



Visitor Location Register

Location Area Code (LAC)

A LAC is a fixed-length code (two octets) that identifies a location area within the network. Each Location Area is serviced by a VLR, so we can think of a Location Area Code (LAC) being assigned to a VLR.

Location Area Identity (LAI)
An LAI is a globally uniqe number that identifies the country, network provider, and LAC of any given Location Area, which coincides with a VLR. It is composed of the Mobile Country Code (MCC), the Mobile Network Code (MNC), and the Location Area Code (LAC). The MCC and the MNC are the same numbers used when forming the IMSI.

LAI		
MCC	MNC	LAC
3 digits	2 or 3 digits	5 digits

Location Area Identity (LAI)

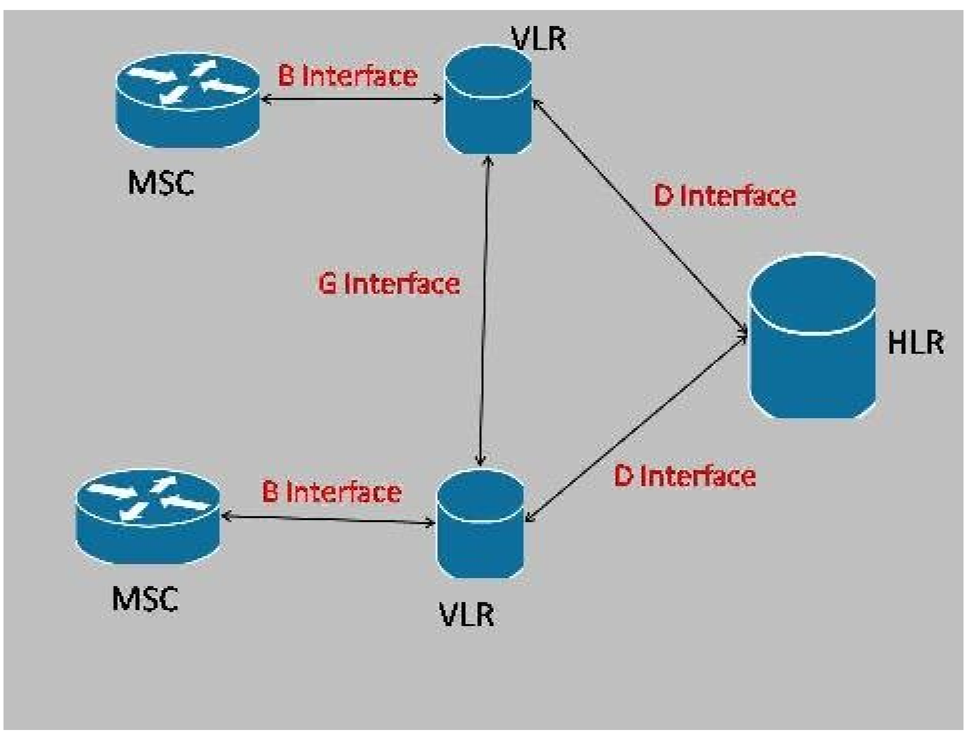
Cell Global Identification (CGI)
The CGI is a number that uniquely identifies a specific cell within its location area, network, and country. The CGI is composed of the MCC, MNC, LAI, and Cell Identity (CI)

MCC	MNC	LAC	Cell Identity
3 digits	2 or 3 digits	5 digits	5 digits

Cell Global Identity

The VLR also has one other very important function: the assignment of a Temporary Mobile Subscriber Identity (TMSI). TMSIs are assigned by the VLR to a MS as it comes into its Location Area. TMSIs are unique to a VLR. TMSIs are only allocated when in cipher mode.

The interface between the MSC and the VLR is known as the *B Interface* and the interface between the VLR and the HLR is known as the *D Interface*. The interface between two VLRs is called the *G Interface*



B and D Interfaces

[Back to Top]

Equipment Identity Register (EIR)

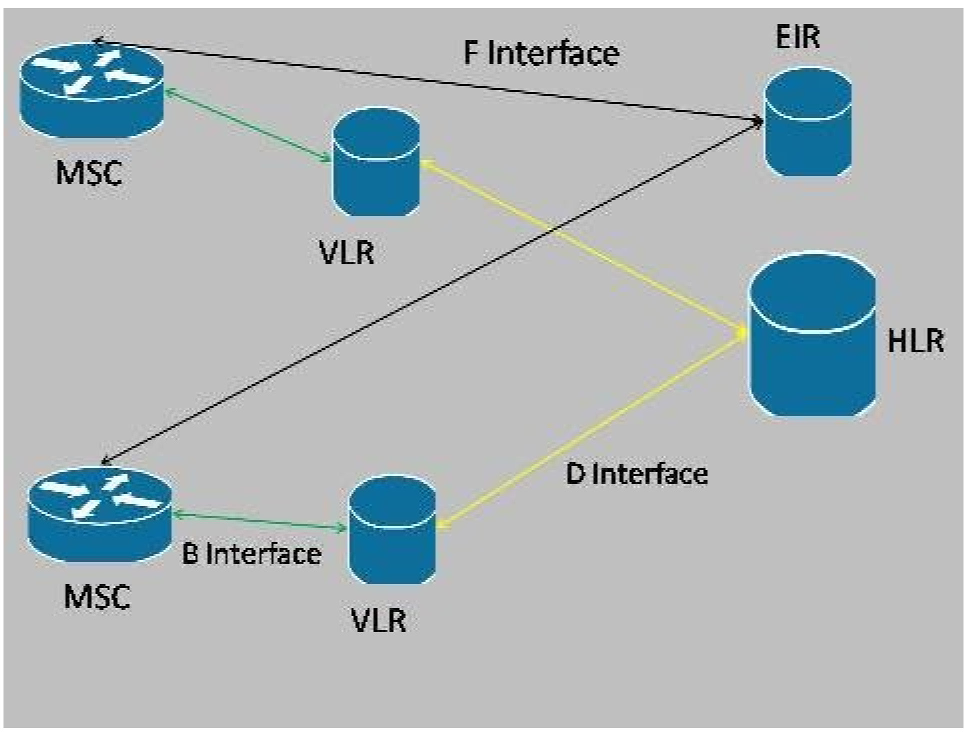
Equipment Identity Register (EIR) - The EIR is a database that keeps tracks of handsets on the network using the IMEI. There is only one EIR per network. It is composed of three lists. The white list, the gray list, and the black list.

The black list is a list if IMEIs that are to be denied service by the network for some reason. Reasons include the IMEI being listed as stolen or clonedor if the handset is malfunctioning or doesnt have the technical capabilities to operate on the network.

The gray list is a list of IMEIs that are to be monitored for suspicous activity. This could include handsets that are behaving oddly or not performing as the network expects it to.

The white list is an unpopulated list. That means if an IMEI is not on the black list or on the gray list, then it is considered good and is "on the white list".

The interface between the MSC and the EIR is called the *F Interface*.

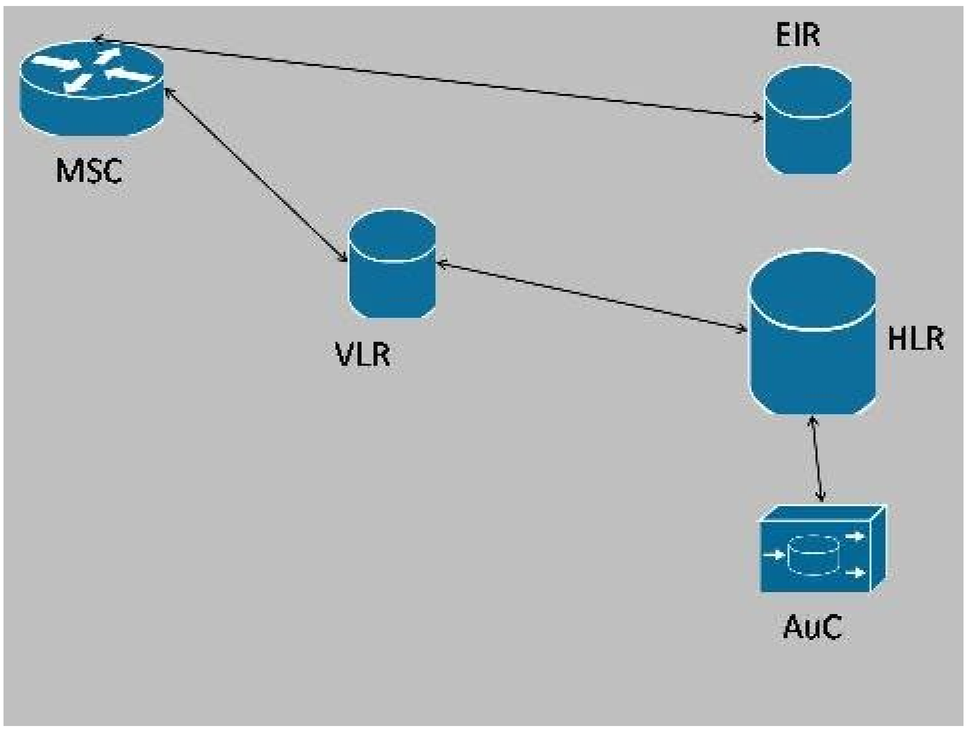


Equipment Identity Register

[Back to Top]

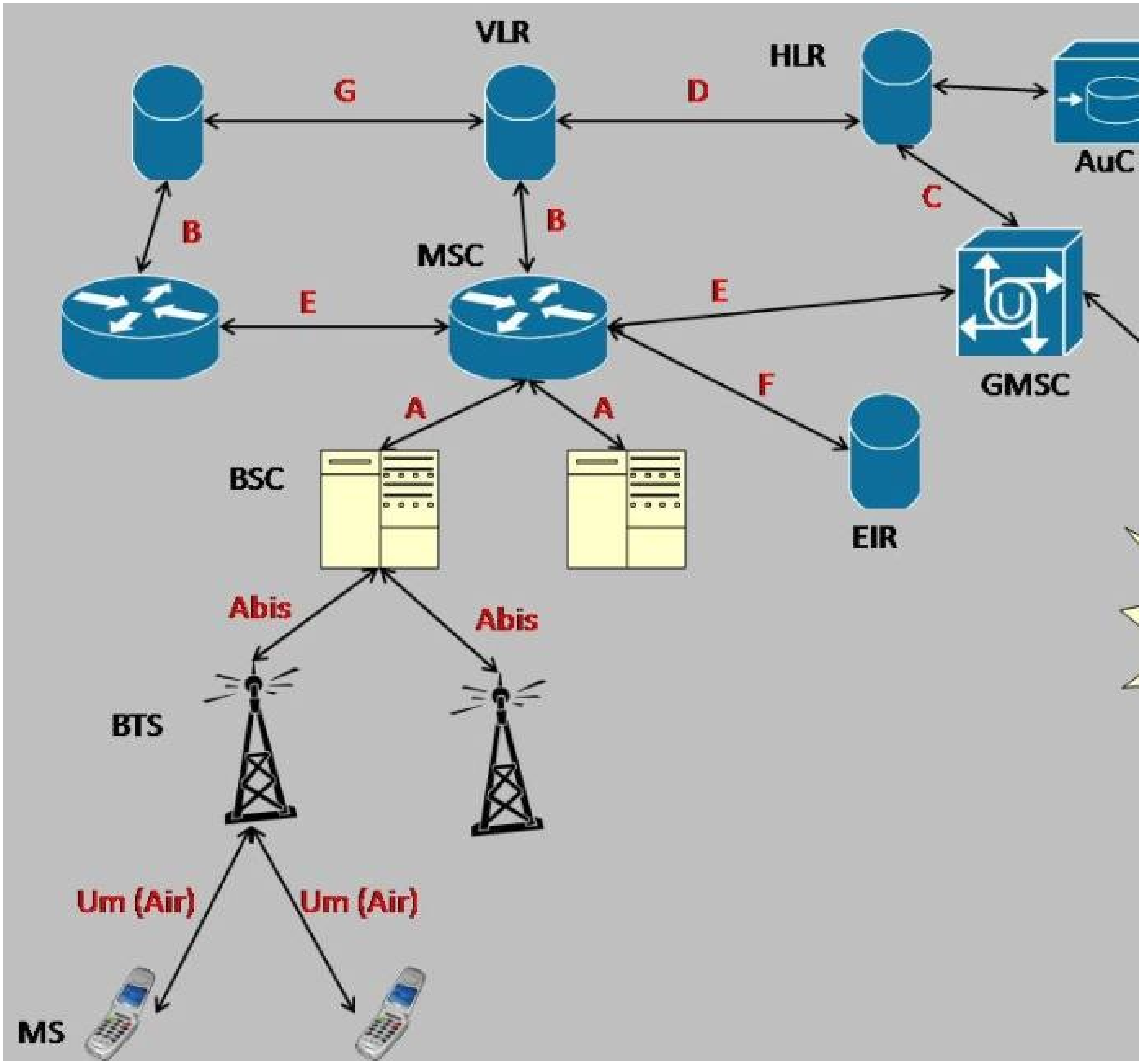
Authentication Center (Auc)

Authentication Center (AuC) - The AuC handles the authentication and encryption tasks for the network. The Auc stores the Ki for each IMSI on the network. It also generates cryptovariables such as the RAND, SRES, and Kc. Although it is not required, the Auc is normally physically collocated with the HLR.



Authentication Center

There is one last interface that we haven't discussed. The interface between the HLR and a GMSC is called the *C Interface*. You will see it in the full network diagram below.This completes the introduction to the network architecture of a GSM network. Below you will find a network diagram with all of the components as well as the names of all of the interfaces.



Full GSM Network

Mobile Station Base Transceiver Station Base Station Controller Mobile Switching Center
Gateway MSC
Home Location Register Visitor Location Register Equipment Identity Register Authentication Center

Introduction Architecture TDMA Logical Channels Authentication & Encryption Timing

Authentication & Encryption

Introduction Authentication Procedures Ciphering Procedures

Home

Introduction

Authentication - Whenever a MS requests access to a network, the network must authenticate the MS. Authentication verifies the identity and validity of the SIM card to the network and ensures that the subscriber is authorized access to the network.

Encryption - In GSM, encryption refers to the process of creating authentication and ciphering cryptovariables using a special key and an encryption algorithm.

Ciphering - Ciphering refers to the process of changing plaintext data into encrypted data using a special key and a special encryption algorithm. Transmissions between the MS and the BTS on the Um link, are enciphered.

Ki - The Ki is the individual subscriber authentication key. It is a 128-bit number that is paired with an IMSI when the SIM card is created. The Ki is only stored on the SIM card and at the Authentication Center (AuC). The Ki should never be transmitted across the network on any link.

RAND - The RAND is a random 128-bit number that is generated by the Auc when the network requests to authenticate a subscriber. The RAND is used to generate the Signed Response (SRES) and Kc cryptovariables.

Signed Response - The SRES is a 32-bit cryptovariable used in the authentication process. The MS is challenged by being given the RAND by the network, the SRES is the expected correct response. The SRES is never passed on the Um (Air) interface. It is kept at the MSC/VLR, which performs the authentication check.

A3 Algorithm - The A3 algorithm computes a 32-bit Signed Response (SRES). The Ki and RAND are inputted into the A3 algorithm and the result is the 32-bit SRES. The A3 algorithm resides on the SIM card and at the AuC.

A8 Algorithm - The A8 algorithm computes a 64-bit ciphering key (Kc). The Ki and the RAND are inputted into the A8 algorithm and the result is the 64-bit Kc. The A8 algorithm resides on the ISM card and at the AuC.

Kc - The Kc is the 64-bit ciphering key that is used in the A5 encryption algorithm to encipher and decipher the data that is being transmitted on the Um interface.

A5 - The A5 encryption algorithm is used to encipher and decipher the data that is being transmitted on the Um interface. The Kc and the plaintext data are inputted into the A5 algorithm and the output is enciphered data. The A5 algorithm is a function of the Mobile Equipment (ME) and not a function of the SIM card. The BTS also makes use of the A5 algorithm.

There are three versions of the A5 algorithm:

A5/1 - The current standard for U.S. and European networks. A5/1 is a stream cipher.<BR
A5/2 - The deliberately weakened version of A5/1 that is intended for export to non-western countries. A5/2 is a stream cipher.

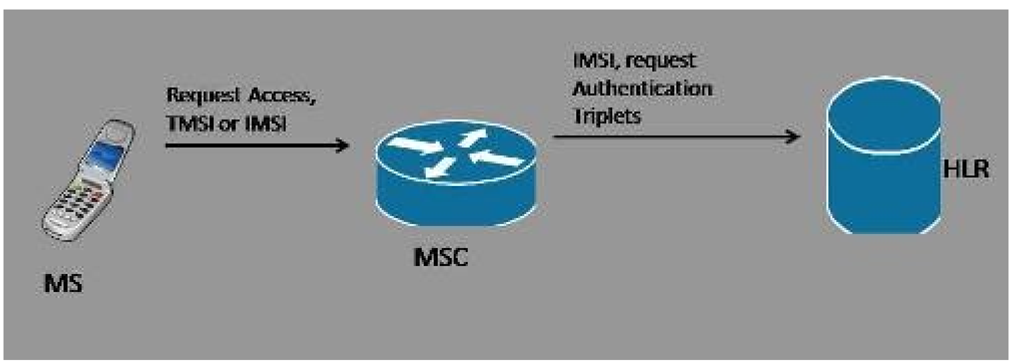
A5/3 - A newly developed algorithm not yet in full use. A5/3 is a block cipher.

Triplets - The RAND, SRES, and Kc together are known as the Triplets. The AuC will send these three cryptovariables to the requesting MSC/VLR so it can authenticate and encipher.

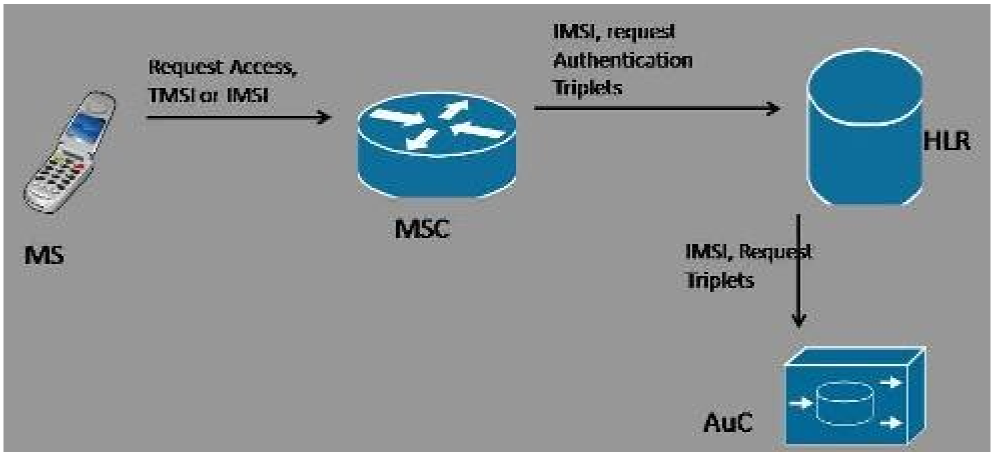
[Back to Top]

Authentication Procedures

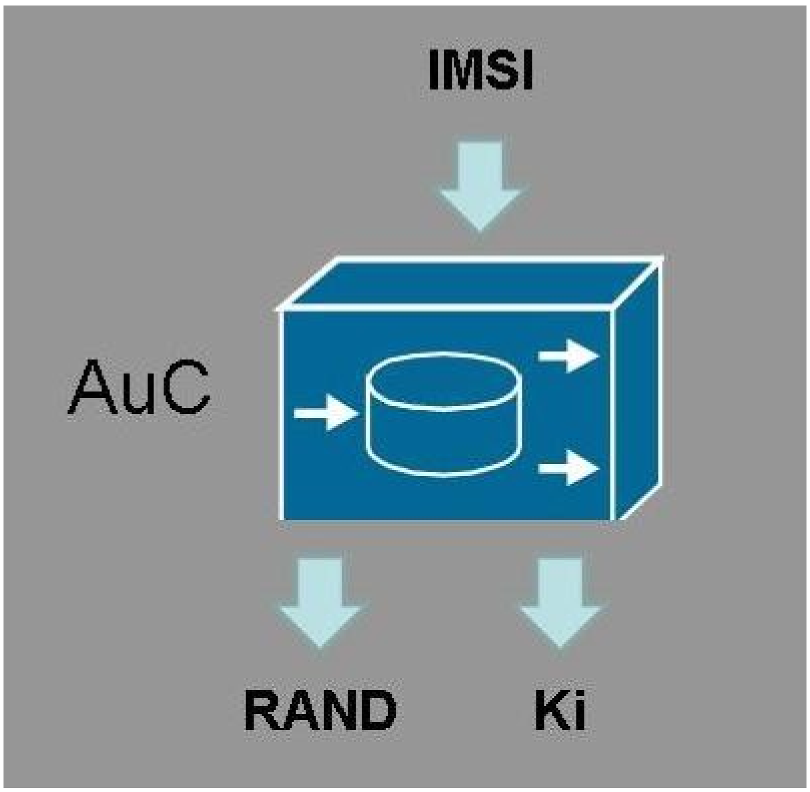
when a MS requests access to the network, the MSC/VLR will normally require the MS to *authenticate*. The MSC will forward the IMSI to the HLR and request authentication *Triplets*.



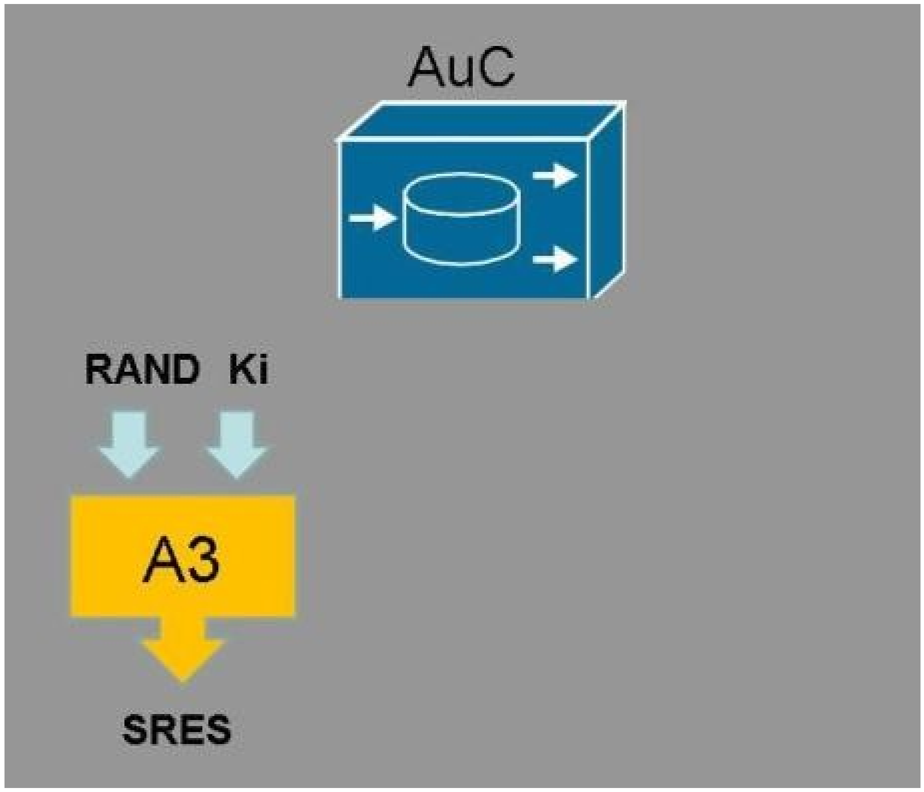
When the HLR receives the IMSI and the authentication request, it first checks its database to make sure the IMSI is valid and belongs to the network. Once it has accomplished this, it will forward the IMSI and authentication request to the *Authentication Center* (AuC).



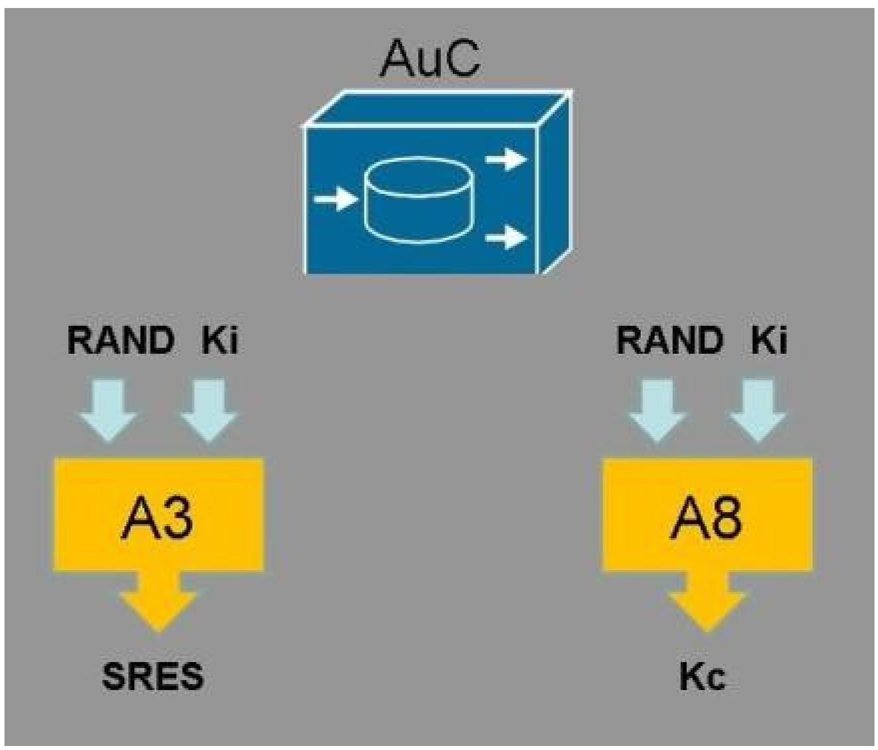
The AuC will use the IMSI to look up the Ki associated with that IMSI. The Ki is the individual subscriber authentication key. It is a 128-bit number that is paired with an IMSI when the SIM card is created. The Ki is only stored on the SIM card and at the AuC. The Auc will also generate a 128-bit random number called the RAND.



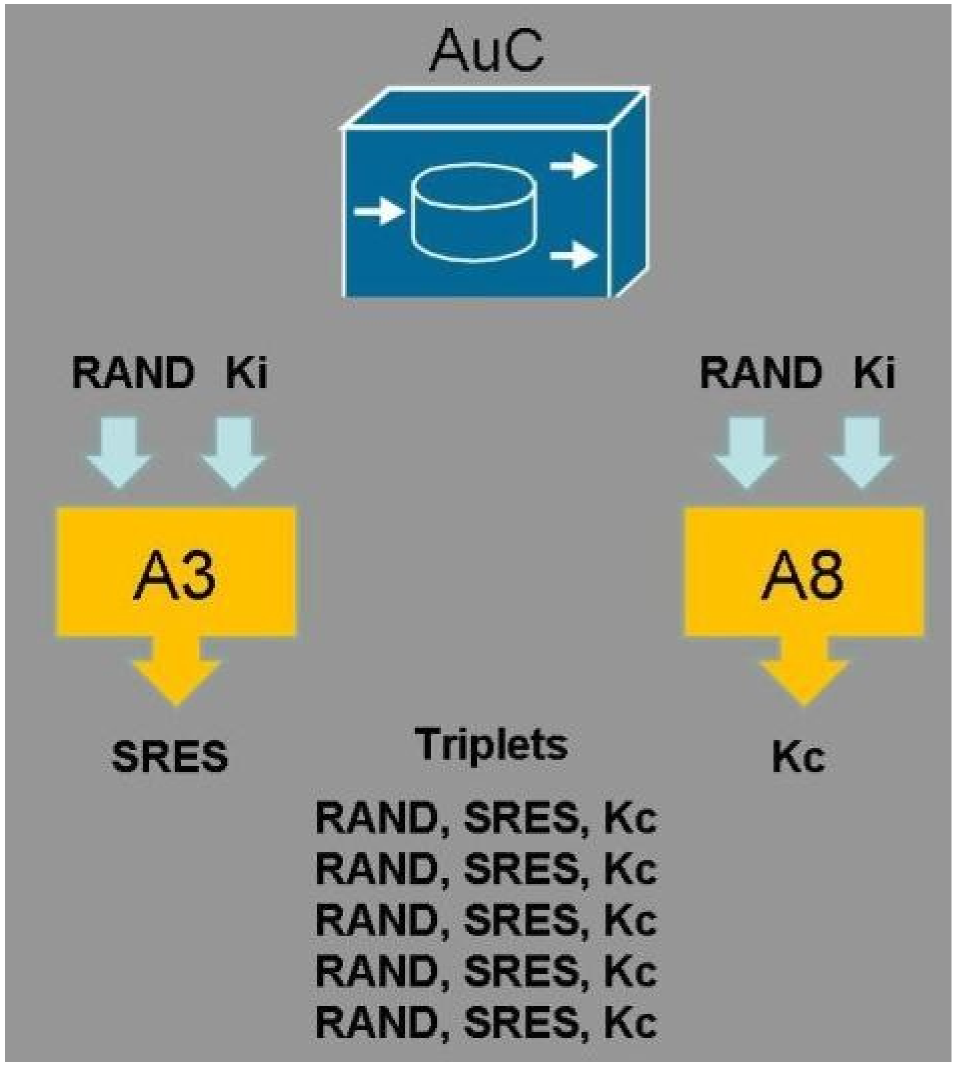
The RAND and the Ki are inputted into the A3 encryption algorithm. The output is the 32-bit *Signed Response* (SRES). The SRES is essentially the "challenge" sent to the MS when authentication is requested.



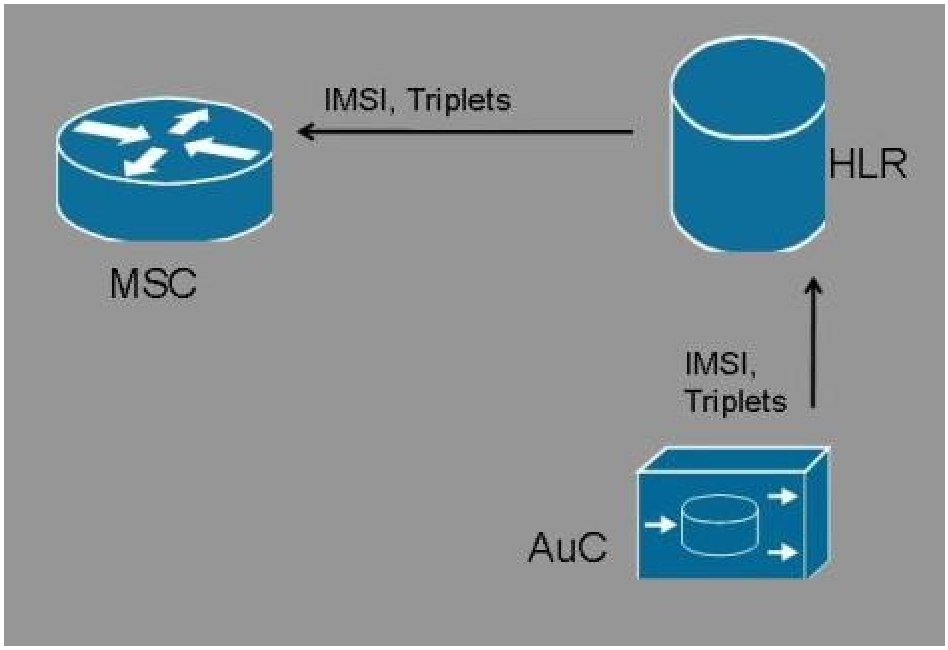
The RAND and Ki are input into the A8 encryption algorithm. The output is the 64-bit Kc. The Kc is the ciphering key that is used in the A5 encryption algorithm to encipher and decipher the data that is being transmitted on the Um interface.



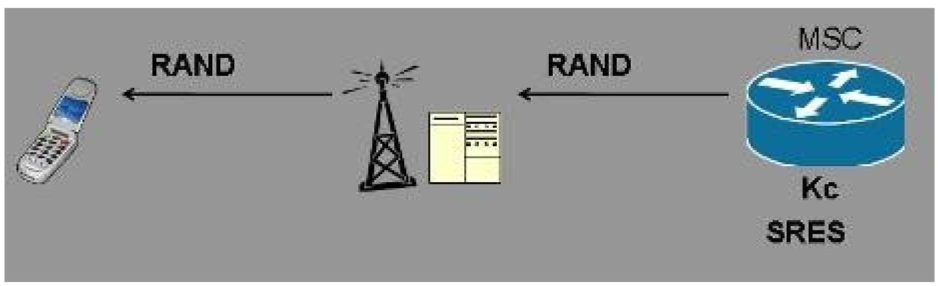
The RAND, SRES, and Kc are collectively known as the *Triplets*. The AuC may generate many sets of Triplets and send them to the requesting MSC/VLR. This is in order to reduce the signalling overhead that would result if the MSC/VLR requested one set of triplets every time it wanted to authenticate the. It should be noted that a set of triplets is unique to one IMSI, it can not be used with any other IMSI.



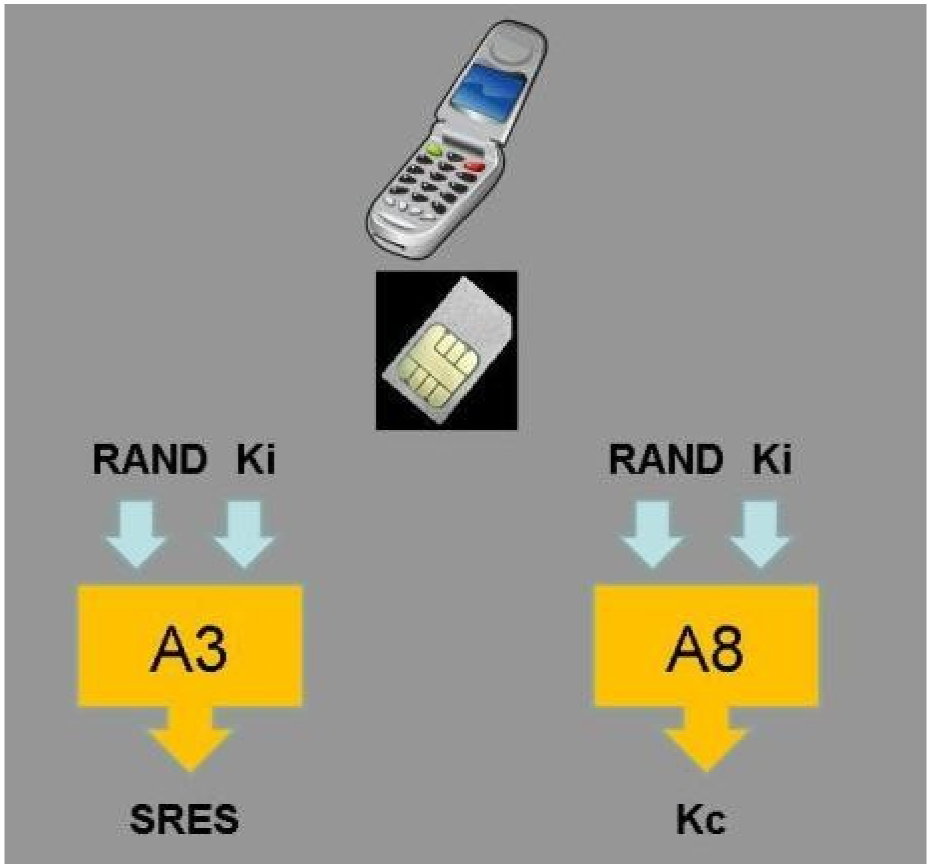
Once the AuC has generated the triplets (or sets of triplets), it forwards them to the HLR. The HLr subsequently sends them to the requesting MSC/VLR.



The MSC stores the Kc and the SRES but forwards the RAND to the MS and orders it to authenticate.



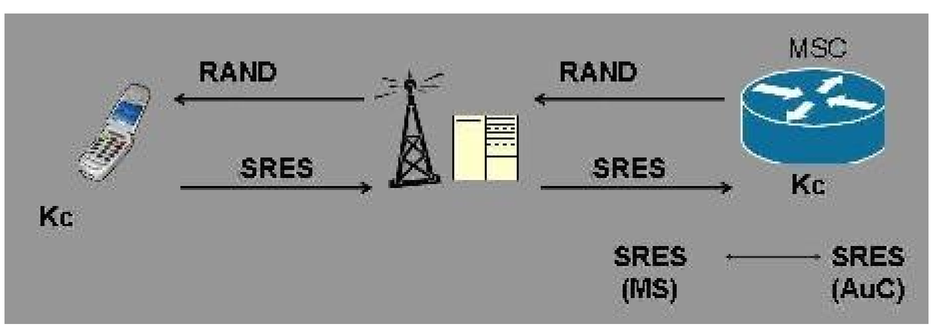
The MS has the Ki stored on the SIM card. The A3 and A8 algorithms also reside on the SIM card. The RAND and Ki are inputted into the A3 and A8 encryption algorithms to generate the SRES and the Kc respectively.



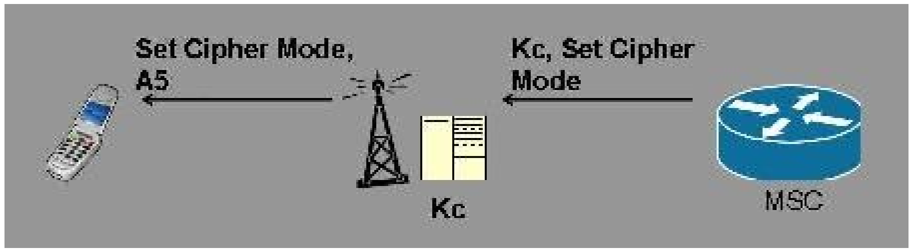
[Back to Top]

Ciphering Procedure

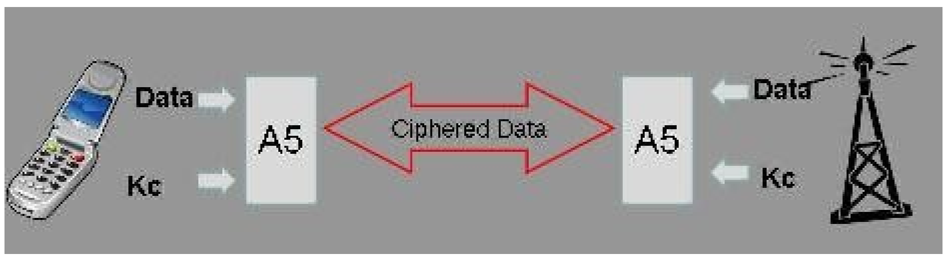
The MS stores the Kc on the SIM card and sends the generated SRES back to the network. The MSC recieves the MS generated SRES and compares it to the ARES generated by the AuC. if they match, then the MS is authenticated.



Once the MS is authenticated, it passes the Kc to the BSS (the BTS to be specific), and orders the BTS and MS to switch to *Cipher Mode*. The Kc should not be passed on the Um link, it will be stored at the BTS.



The BTS inputs the Kc and the data payload into the A5 encryption algorithm resulting in an enciphered data stream. The MS also inputs the Kc and the data payload into the A5 encryption algorithm resulting in an enciphered data stream. It should be noted that the A5 algorithm is a function of the Mobile Equipment (ME) and not the SIM card.



Introduction Authentication Procedures Ciphering Procedures

Introduction Architecture TDMA Logical Channels Authentication & Encryption Timing Advances Speech Encoding GSM Events
Updates Bulletin Board Sitemap Contact Me

Home

Time Division Multiple Access (TDMA)

Introduction Time Slots Data Rates Burst Structure Normal Burst Frequency Correction Burst Synchronization Burst
Access Burst Data Throughput Frame Structure TDMA Frame Multiframes Superframes Hyperframes

Time Division Multiple Access

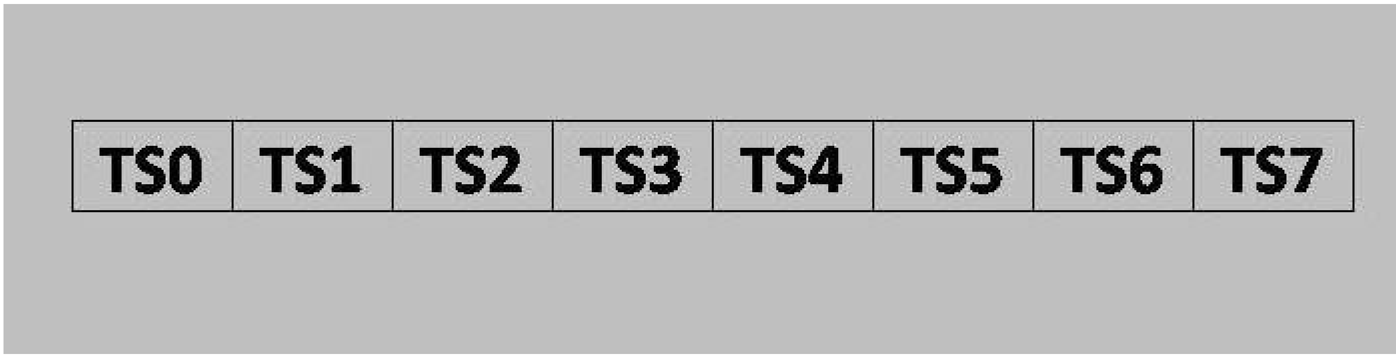
Introduction

GSM uses Time Division Multiple Acces (TDMA) as its access scheme. This is how the MS interfaces with the network. TDMA is the protocol used on the Air (Um) Link. GSM uses Gaussian Minimum-Shift Keying (GMSK) as its modulation methos.

Time Division means that the frequency is divided up into blocks of time and only certain *logical channels* are transmitted at certain times. Logical channels will be introduced in the next lesson.The time divisions in TDMA are known as **Time Slots**.

Time Slots

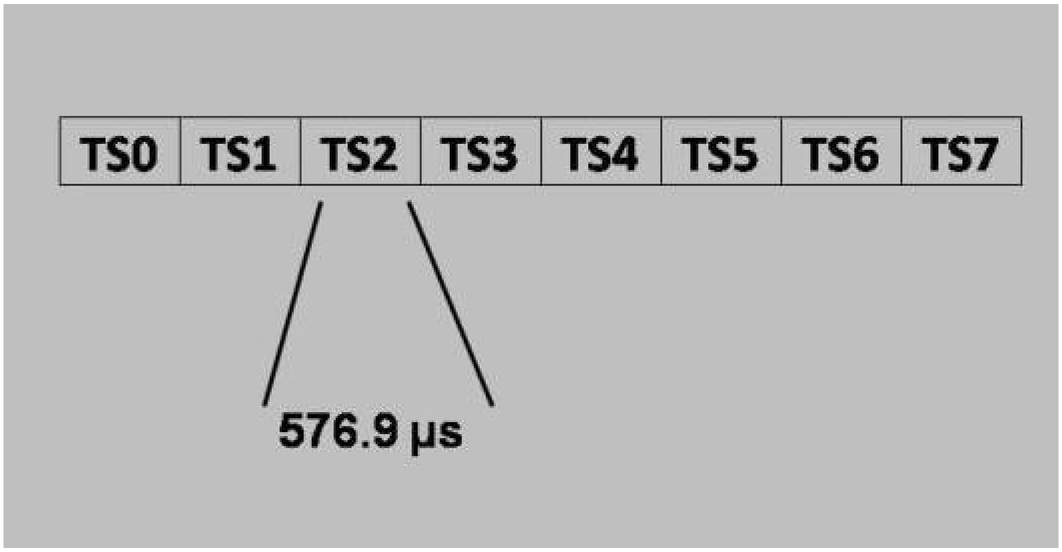
A frequency is divided up into 8 time slots, numbered 0 to 7.



Time Slots

On a side note, also remember that GSM carrier frequencies are separated by 200kHz and that GSM operates in duplex. A channel number assigned to a pair of frequencies, one uplink and one downlink, is known as an Absolute Radio Frequency Channel Number (ARFCN). For a review of the ARFCN go to the Introduction to GSM Tutorial.

Each time slot lasts 576.9 µs. A time slot is the basic radio resource used to facilitate communication between the MS and the BTS.



Time Slot Duration

[Back to Top]

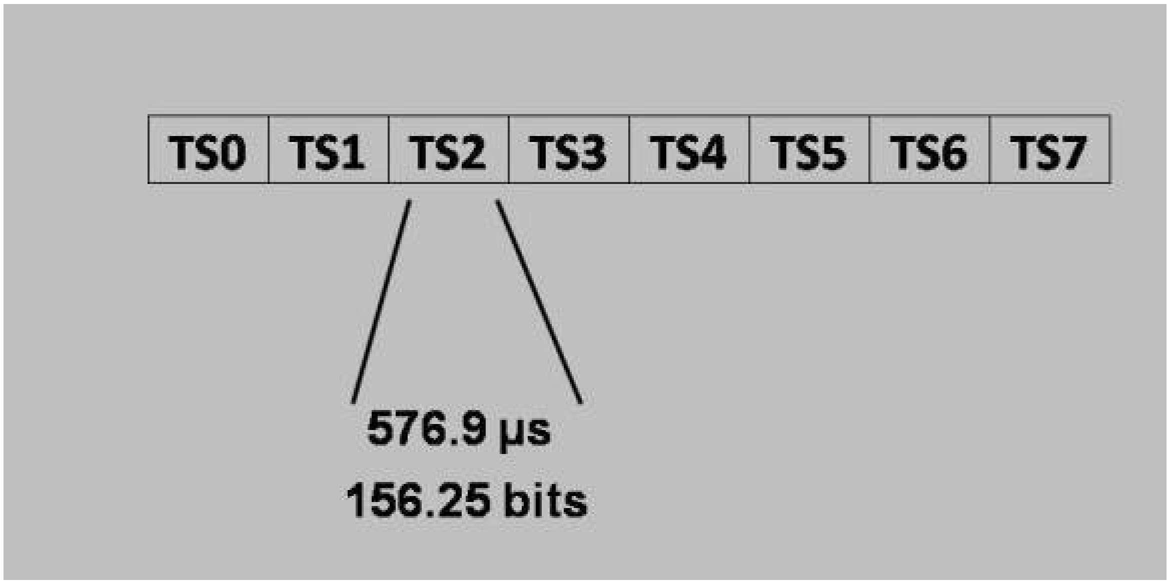
Data Rates

As stated earlier, GSM uses Gaussian Minimum-Shift Keying (GMSK) as its modulation method. GMSK provides a modulation rate of 270.833 kilobits per second (kb/s).

At that rate, a maximum of 156.25 bits can be transmitted in each time slot (576.9 µs).

Math:

270.833 kb/s × 1000 = 270,833 bits/sec (Converting from kilobits to bits)
270,833 b/sec ÷ 1,000,000 = .207833 b/µs (Calculating bits per miscrosecond)
.207833 b/µs × 576.9 µs = 156.25 bits (Calculating number of bits per time slot)
So, 156.25 bits can be transmitted in a single time slot



Bits per Time Slot

[Back to Top]

Data Burst

The data transmitted during a single time slot is known as a burst. Each burst allows 8.25 bits for *guard time* within a time slot. This is to prevent bursts from overlapping and interfering with transmissions in other time slots. Subtracting this from the 156.25 bits, there are 148 bits usable for each burst.

There are four main types of bursts in TDMA:

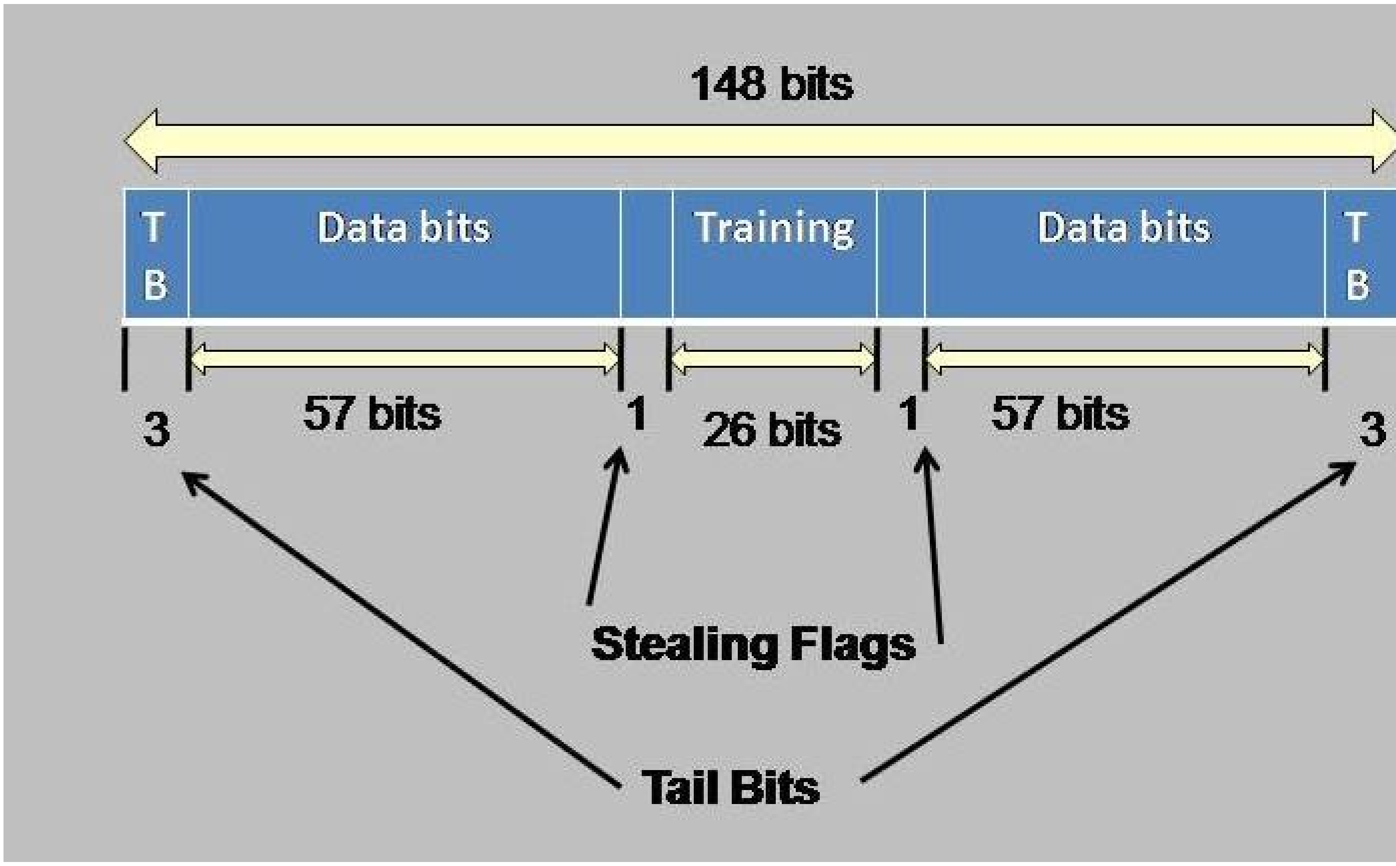
Normal Burst (NB)
Frequency Correction Burst (FB)
Synchronization Burst (SB)
Access Burst (AB)

Normal Burst

The data transmitted during a single time slot is known as a burst. Each burst allows 8.25 bits for *guard time*. This is to prevent bursts from overlapping and interfering with transmissions in other time slots.

Out of 156.25, this leaves 148 bits usable for each burst.

Here is the structure of a normal burst:



Burst

Tail Bits - Each burst leaves 3 bits on each end in which no data is transmitted. This is designed to compensate for the time it takes for the power to rise up to its peak during a transmission. The bits at the end compensate for the powering down at the end of the transmission.

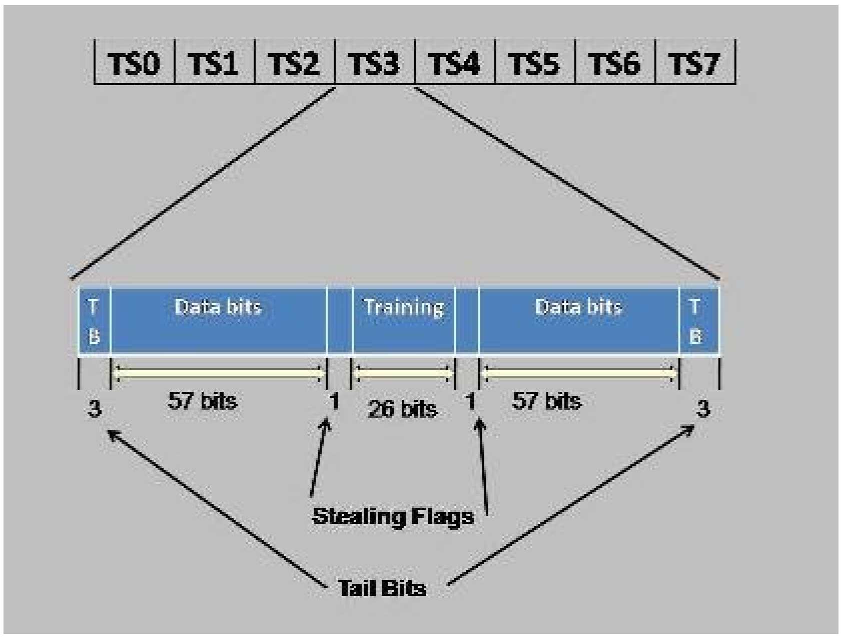
Data Bits - There are two data payloads of 57 bits each.

Stealing Flags - Indicates whether the burst is being used for voice/data (set to "0") or if the burst is being "stolen" by the *FACCH* to be used for singalling (set to "1"). *The FACCH is discussed in the Logical Channels Tutorial

Training Sequence - The training sequence bits are used to overcome multi-path fading and propagation effects through a method called *equalization*.

*Note: 3GPP TS 45.001 Standard does not describe stealing bits, and instead allows for two 58-bit data payloads in a burst. However, it is common practice in GSM networks to use 57-bit payloads and stealing bits.

This diagram illustrates a single burst inside a time slot. Remember that 8.25 bits are not used in order to allow for a guard time.



Burst within a Time Slot

Since each burst has two 57-bit data segments, we can see that a single burst has a data payload of 114 bits.

[Back to Top]

Frequency Correction Burst

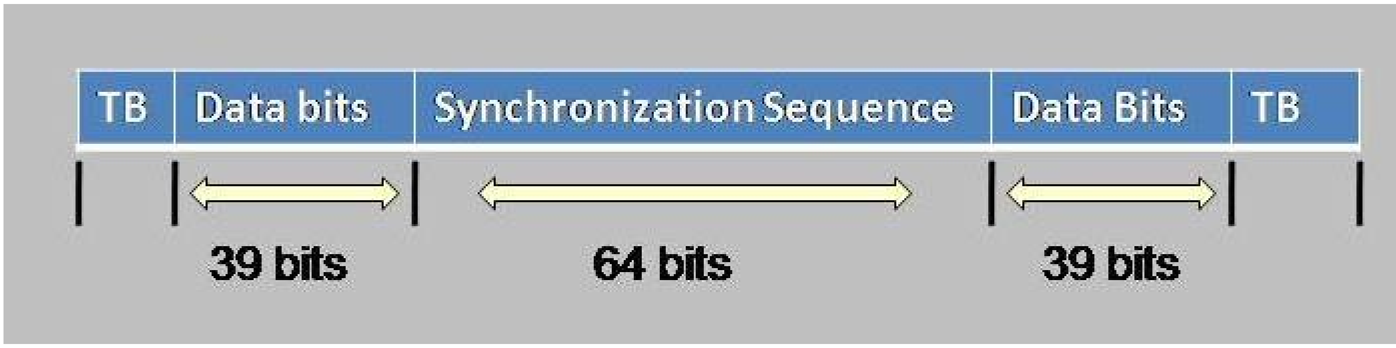
This burst is used for frequency synchronization of the mobile station. It is an unmodulated carrier that shifts in frequency. It has the same guard time as a normal bit (8.25 bits). The broadcast of the FB usually occurs on the logical channel *FCCH*.
*The FCCH is discussed in the Logical Channels Tutorial

Frequency Correction Burst

[Back to Top]

Synchronization Burst

This burst is used for time synchronization of the mobile. The data payload carries the TDMA *Frame Number (FN)* and the *Base Station Identity Code (BSIC)*. It is broadcast with the frequency correction burst. The Synchronization Burst is broadcast on the *Synchronization Channel (SCH)*.
*The SCH is discussed in the Logical Channels Tutorial



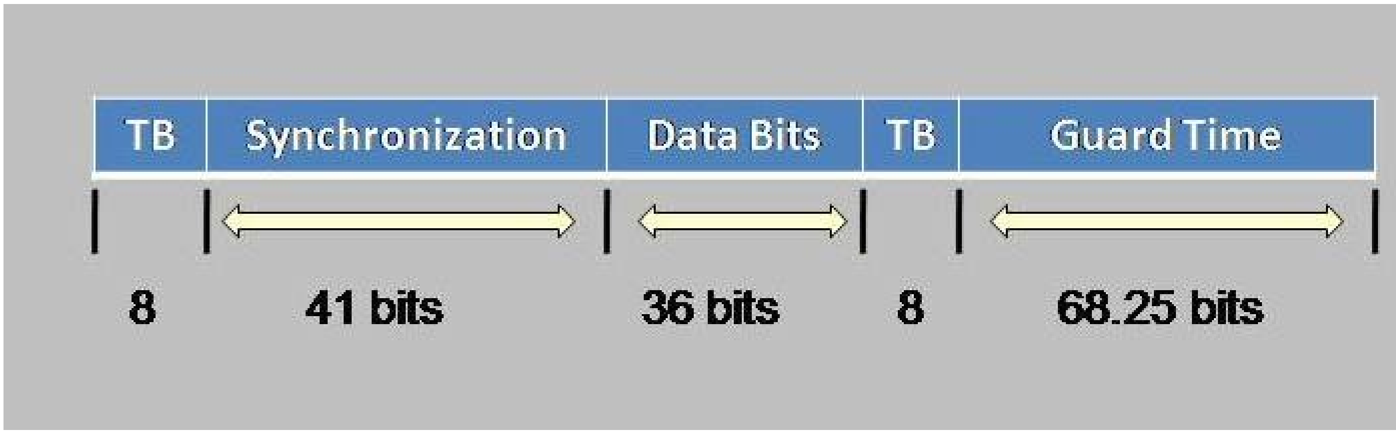
Synchronization Burst

[Back to Top]

Access Burst

This burst is used the by mobile station for random access. It has a much longer guard period (68.25 bits compared to the 8.25 bits in a normal burst). It is designed to compensate for the unknown distance of the mobile station from the tower, when the MS

wants access to a new BTS, it will not know the correct *Timing Advance*.
*The RACH is discussed in the Logical Channels Tutorial



Access Burst

[Back to Top]

Calculating the Data Throughput

Since each burst has two 57-bit data segments, we can see that a single burst has a data payload of 114 bits.

Each burst lasts 576.9 µs, so we can calculate the theoretical bit rate of a single time slot:

114 bits ÷ 576.9 µs = .1976 bits/µs   (Calculating bits per µs)

.1976 bits/µs × 1,000,000 = 197,607 bits/sec nbsp; (Converting µs to sec)

Since there are 8 time slots per carrier frequency, each time slot would only get 1/8 of this bit rate, so...

197,607 bits ÷ 8 = 24,700 bits   (Calculating bit rate for one of eight time slots.)

24,700 bits ÷ 1000 = 24.7 kbits/sec   (Converting bits to kilobits)

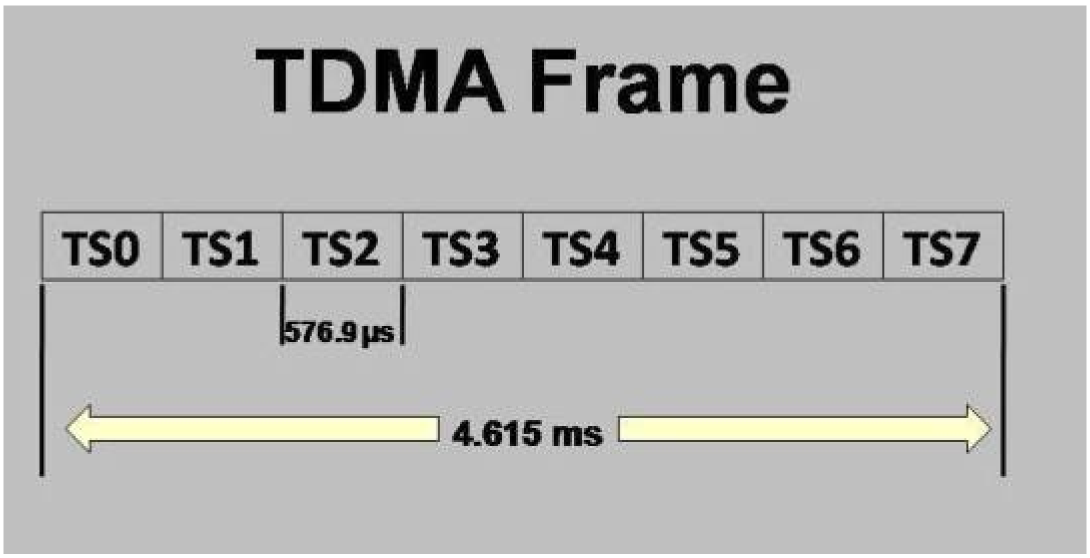
So, using GMSK modulation there is a maximum bit rate of 24.7 kb/s for a single time slot. Note that this bit rate does not account for any error correction bits. Any bits used for error correction would have to be stolen from the 114-bit data payload of each burst.

[Back to Top]

TDMA Frame Structure & Hierarchy

TDMA Frame

Each sequence of 8 time slots is known as a TDMA frame. The duration of a TDMA frame is 4.615 milliseconds (ms) (576.9 µs × 8).
* Remember that a TDMA frame is 8 time slots and that no one resource will be given an entire TDMA frame, the resources must share them.



A TDMA Frame

[Back to Top]

Multiframe

A Multiframe is composed of multiple TDMA frames.

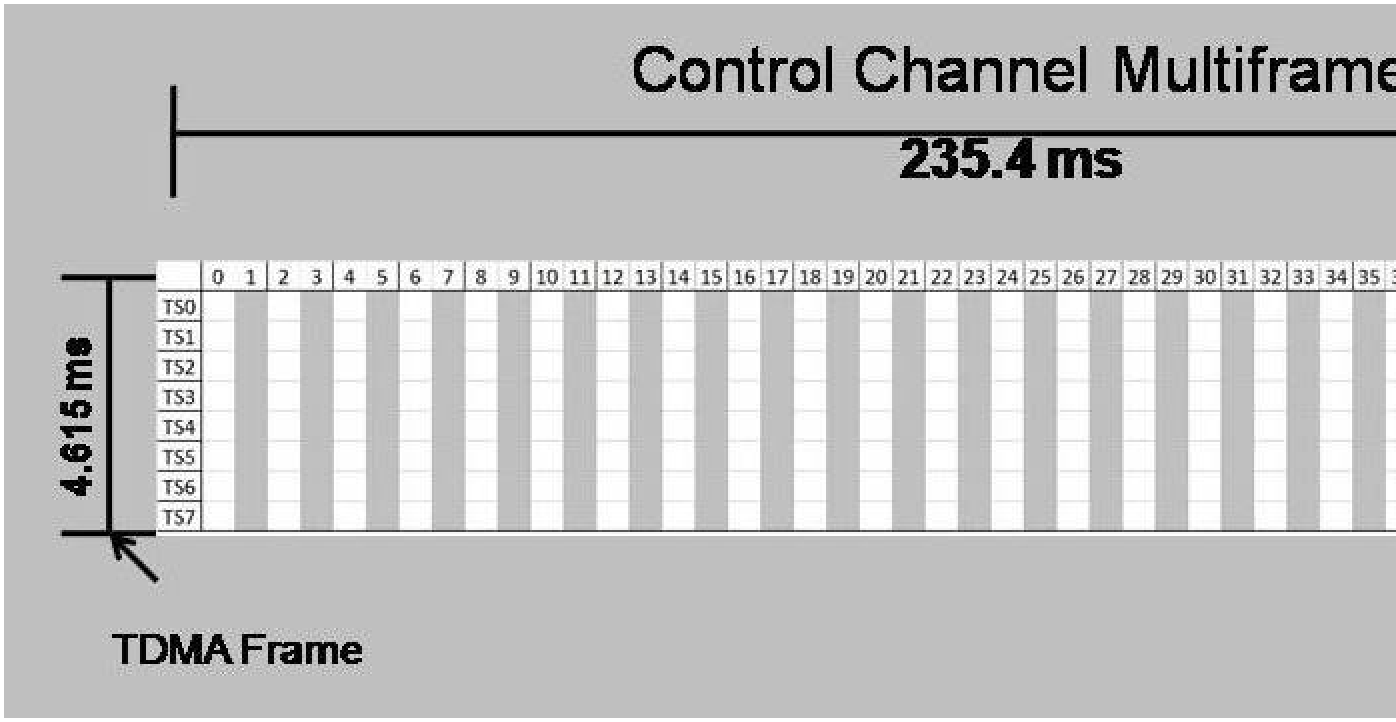
There are two types of multiframes:

Control Channel Multiframes
Traffic Channel Multiframes

*Control Channels and Traffic Channels are explained in Logical Channels Tutorial.

Control Channel Multiframe
composed of 51 TDMA frames

duration = 235.4 ms

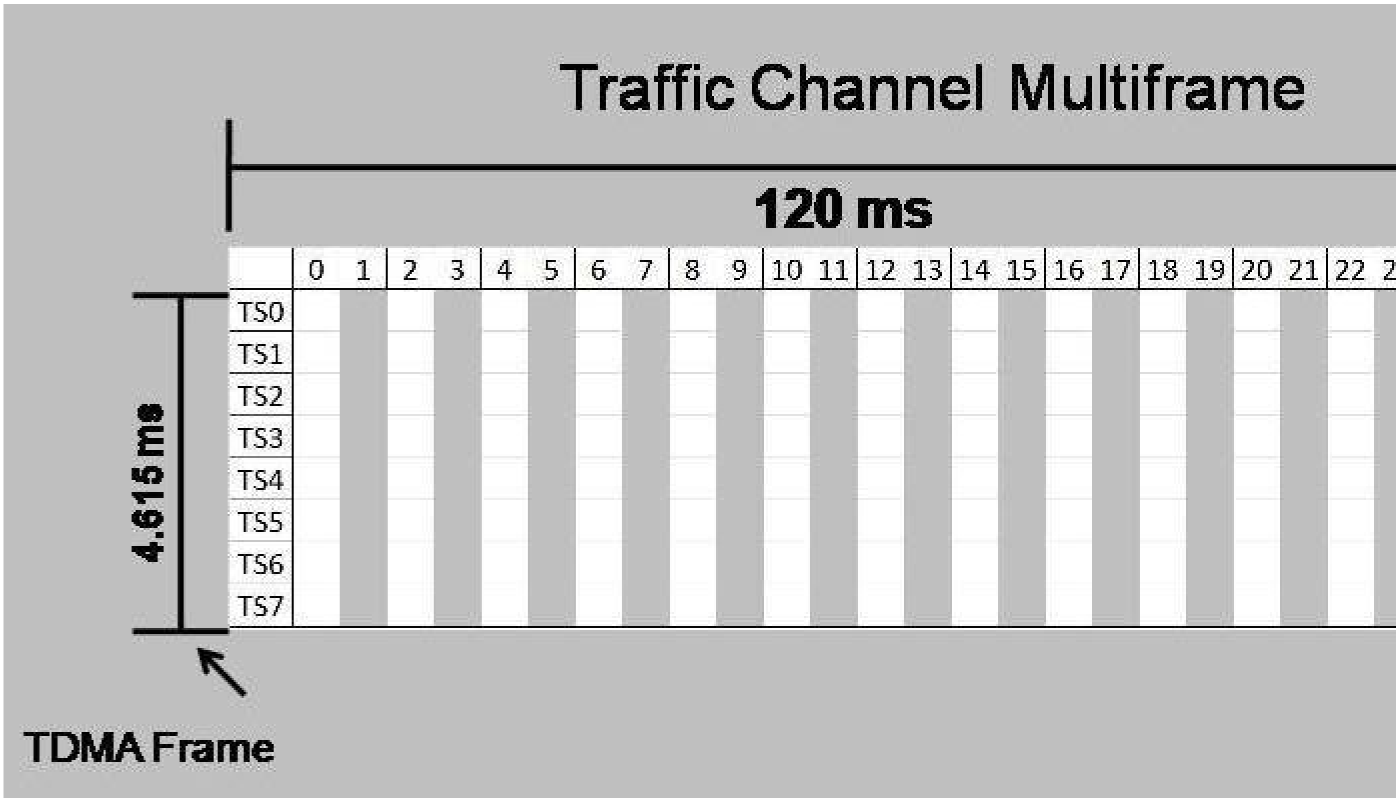


Control Channel Multiframe

Traffic Channel Multiframe

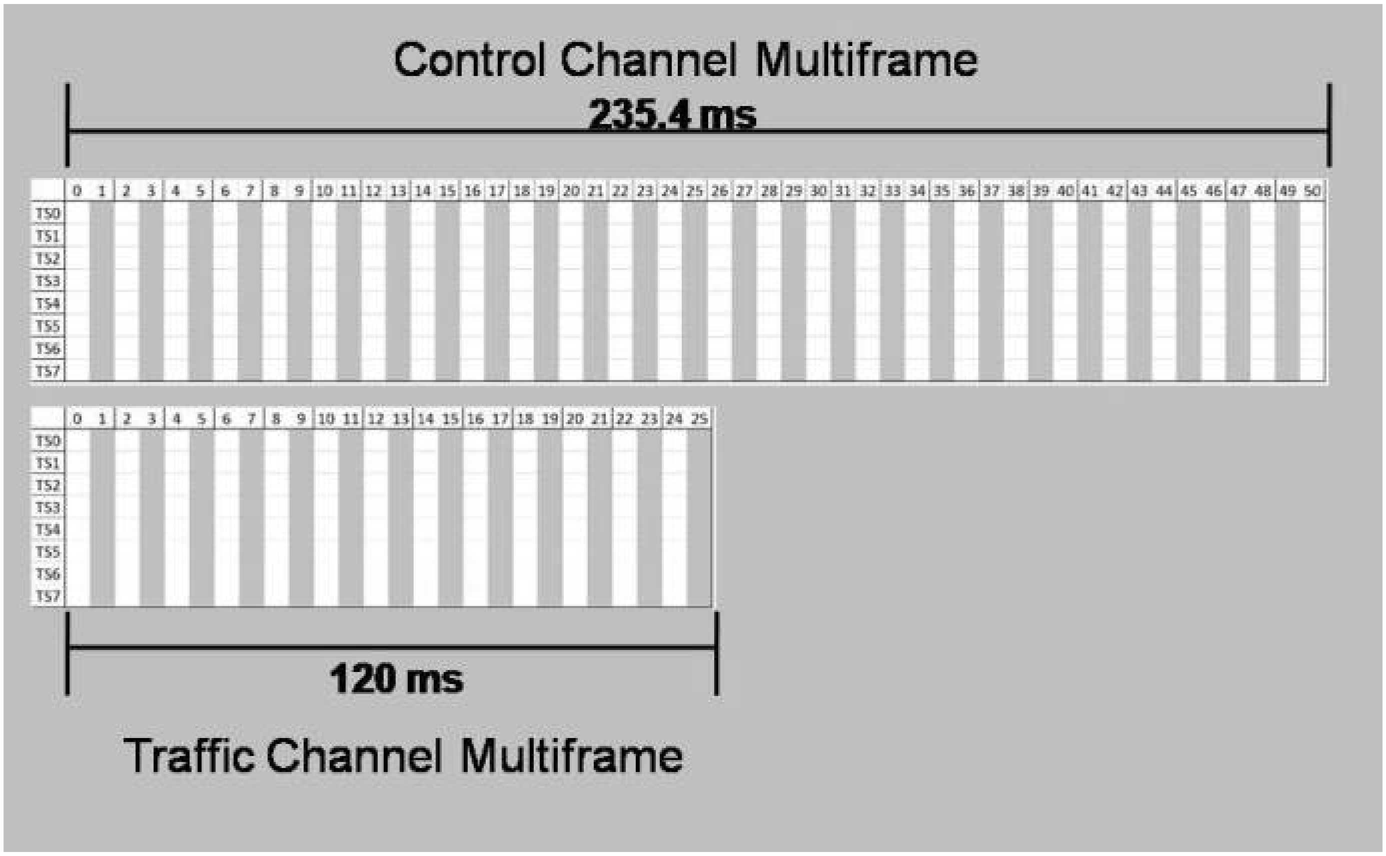
composed of 26 TDMA frames

duration = 120 ms



Traffic Channel Multiframe

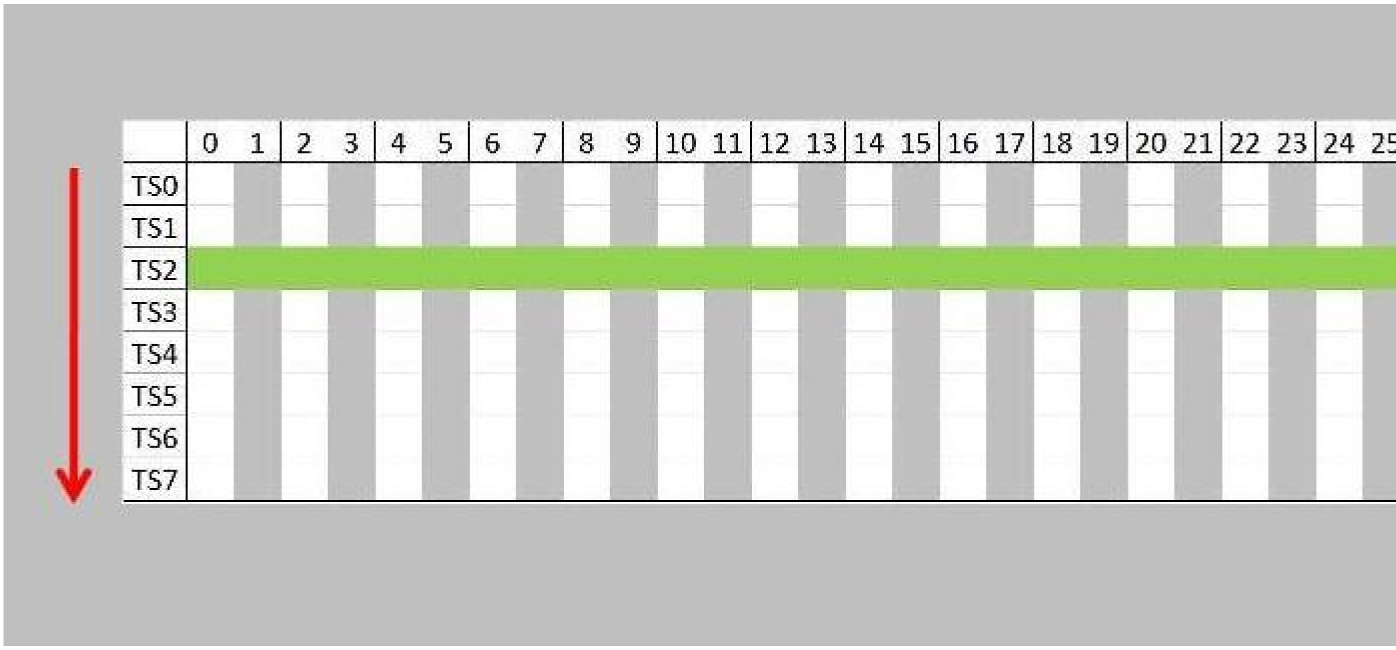
Here is a diagram comparing the Control Channel multiframe and a traffic channel multiframe.



Traffic Channel and Control Channel Multiframes

The next diagram shows a Traffic Channel (TCH) Multiframe with TS2 (green) being allocated to a Mobile Station (MS). The red arrow indicates the sequence of transmission. The sequence starts in TDMA frame 0 at TS0, proceeds through all eight time slots, then starts again with TDMA frame 1.

In this example, the MS has been allocated a Traffic Channel in TS2. Therefore the MS will only transmit/receive during TS2 of each TDMA frame.



Single Time Slot Allocated

[Back to Top]

Superframe

A Superframe is composed of multiple Multiframes.

Again, there is a superframe for Control Channels and one for Traffic Channels.

Control Channel Superframe
composed of 26 Control Channel (CCH) multiframes (each CCH multiframe has 51 TDMA frames)
duration = 6.12 seconds

Traffic Channel Superframe
composed of 51 Traffic Channel (TCH) multiframes (each TCH) multiframe has 26 TDMA frames)
duration = 6.12 seconds

Each superframe, whether it is a CCH or TCH frame, consists of 1326 TDMA frames (51 * 26)
*Note: The CCH and TCH frame sequences will synchronize every superframe.

[Back to Top]

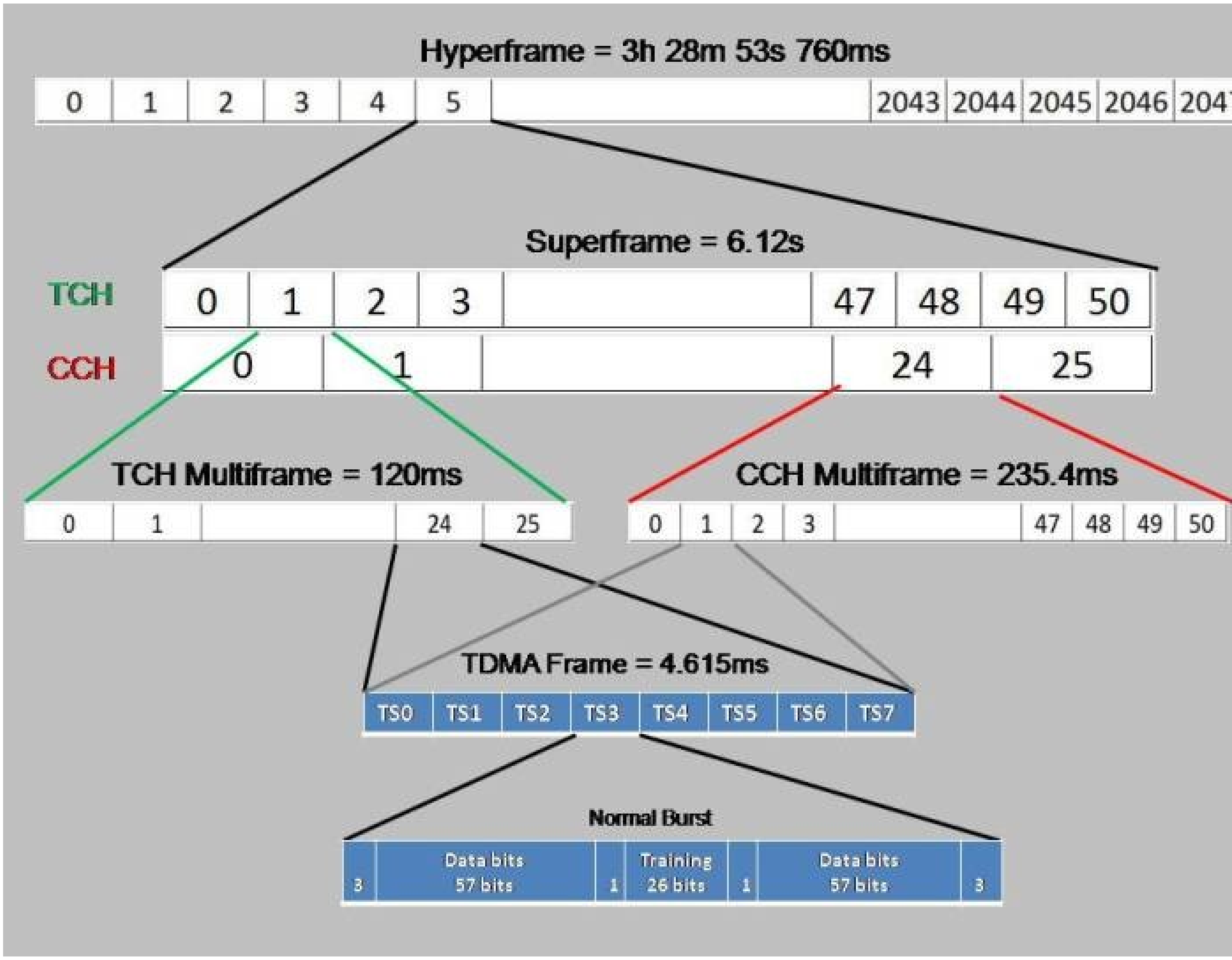
Hyperframe

A hyperframe is composed of 2048 superframes.
duration = 3h 28m 53s 76ms (12,533.76 seconds)
consists of 2,715,548 TDMA frames

Each TDMA frame is numbered according to its sequence within the hyperframe, starting from 0 and ending at 2,715,547.

The TDMA frame number within a hyperframe is abbreviated FN. The FN is one of the variables used in GSM encryption algorithms.

The following diagram shows the relationship between all of the various time segments introduced in this tutorial.



Relationship of All Time Segments

Introduction Time Slots Data Rates Burst Structure Normal Burst Frequency Correction Burst Synchronization Burst
Access Burst Data Throughput Frame Structure TDMA Frame Multiframes Superframes Hyperframes

Introduction Architecture TDMA Logical Channels Authentication & Encryption Timing Advances Speech Encoding GSM Events
Updates Bulletin Board Sitemap Contact Me

Home

Logical Channels

Signaling Channels   Broadcast Channels (BCCH FCCH SCH CBCH)   Common Control Channels (PCH RACH AGCH)
SDCCH   Associated Control Channels (FACCH SACCH)   Signal Channel Mapping

Traffic Channels   Encoded Speech   Data   Traffic Channel Mapping   ARFCN Mapping   Frequency Hopping

Home

Introduction

As you remember from the Introduction to TDMA tutorial. GSM divides up each ARFCN into 8 time slots.

These 8 timeslots are further broken up into logical channels.

Logical channels can be thought of as just different types of data that is transmitted only on certain frames in a certain timeslot.

Different time slots will carry different logical channels, depending on the structure the BSS uses.
There are two main categories of logical channels in GSM:

Signaling Channels
Traffic Channels (TCH)

Signaling Channels

These are the main types of signaling Channels:**Broadcast Channels (BCH)** - Transmitted by the BTS to the MS. This channel carries system parameters needed to identify the network, synchronize time and frequency with the network, and gain access to the network.

Common Control Channels (CCH) - Used for signaling between the BTS and the MS and to request and grant access to the network.

Standalone Dedicated Control Channels (SDCCH) - Used for call setup.

Associated Control Channels (ACCH) - Used for signaling associated with calls and call-setup. An ACCH is always allocated in conjunction with a TCH or a SDCCH.

*keep in mind, these are only categories of logical channels, they are not logical channels themselves.

The above categories can be divided into the following logical channels:

Broadcast Channels (BCH)
- Broadcast Control Channel (BCCH)
- Frequency Correction Channel (FCCH)
- Synchronization Channel (SCH)
- Cell Broadcast Channel (CBCH)

Common Control Channels (CCCH)
- Paging Channel (PCH)
- Random Access Channel (RACH)
- Access Grant Channel (AGCH)

Standalone Dedicated Control Channel (SDCCH)
- Associated Control Channel (ACCH)
- Fast Associated Control Channel (FACCH)
- Slow Associated Control Channel (SACCH)

[Back to Top]

Let's examine each type of logical channel individually.</A

Broadcast Channels (BCH)

Broadcast Control Channel (BCCH) - DOWNLINK - This channel contains system parameters needed to identify the network and gain access. These paramters include the Location Area Code (LAC), the Mobile Network Code (MNC), the frequencies of neighboring cells, and access parameters.

Frequency Correction Channel (FCCH) - DOWNLINK - This channel is used by the MS as a frequency reference. This channel contains frequency correction bursts.

Synchronization Channel (SCH) - DOWNLINK - This channel is used by the MS to learn the Base Station Information Code (BSIC) as well as the TDMA frame number (FN). This lets the MS know what TDMA frame they are on within the hyperframe.
*** The BSIC was covered in the Introduction to GSM Tutorial. You can also read about the numbering schemes used in GSM.**

Cell Broadcast Channel (CBCH) - DOWNLINK - This channel is not truly its own type of logical channel. The CBCH is for *point-to-omnipoint* messages. It is used to broadcast specific information to network subscribers; such as weather, traffic, sports, stocks, etc. Messages can be of any nature depending on what service is provided. Messages are normally public service type messages or announcements. The CBCH isnt allocated a slot for itself, it is assigned to an SDCCH. It only occurs on the downlink. The CBCH usually occupies the second subslot of the SDCCH. The mobile will not acknowledge any of the messages.

[Back to Top]

Common Control Channels (CCCH)

Paging Channel (PCH) - DOWNLINK - This channel is used to inform the MS that it has incoming traffic. The traffic could be a voice call, SMS, or some other form of traffic.

Random Access Channel (RACH) - UPLINK This channel is used by a MS to request an initial dedicated channel from the BTS. This would be the first transmission made by a MS to access the network and request radio resources. The MS sends an *Access Burst* on this channel in order to request access.

Access Grant Channel (AGCH) - DOWNLINK - This channel is used by a BTS to notify the MS of the assignement of an initial SDCCH for initial signaling.

[Back to Top]

Standalone Dedicated Control Channel (SDCCH) - UPLINK/DOWNLINK - This channel is used for signaling and call setup between the MS and the BTS.

Associated Control Channels (ACCH)

Fast Associated Control Channel (FACCH) - UPLINK/DOWNLINK - This channel is used for control requirements such as handoffs. There is no TS and frame allocation dedicated to a FAACH. The FAACH is a burst-stealing channel, it steals a Timeslot from a

Traffic Channel (TCH).

Slow Associated Control Channel (SACCH) - UPLINK/DOWNLINK - This channel is a continuous stream channel that is used for control and supervisory signals associated with the traffic channels.

[[Back to Top]]

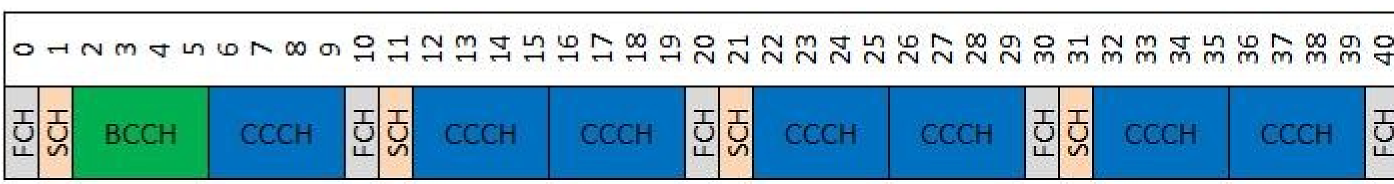
Signaling Channel Mapping

Normally the first two timeslots are allocated to signaling channels.

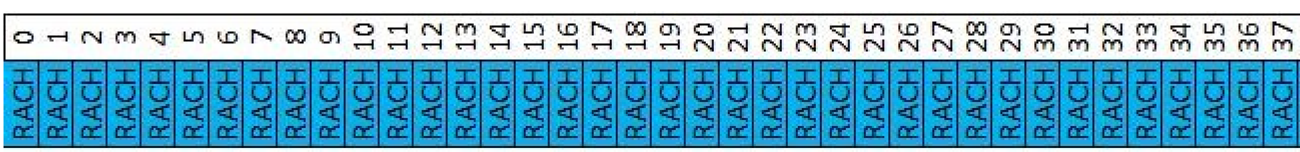
Remember that Control Channel (aka signaling channels) are composed of 51 TDMA frames. On a time slot Within the multiframe, the 51 TDMA frames are divided up and allocated to the various logical channels.

There are several channel combinations allowed in GSM. Some of the more common ones are:
FCCH + SCH + BCCH + CCCH
BCCH + CCCH
FCCH + SCH + BCCH + CCCH + SDCCH/4(0..3) + SACCH/C4(0..3)
SDCCH/8(0 .7) + SACCH/C8(0 . 7)

FCCH + SCH + BCCH + CCCH



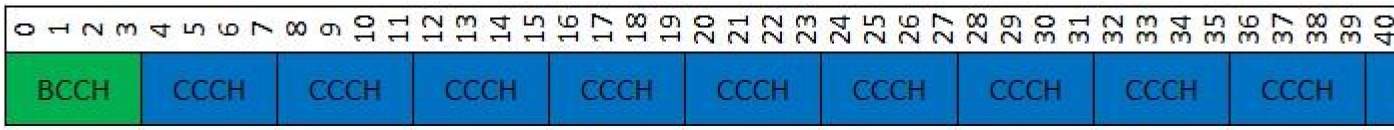
Downlink



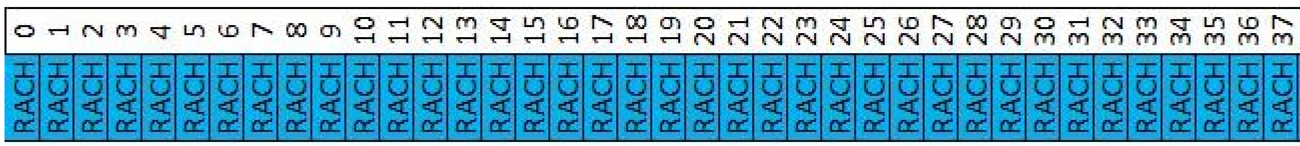
Uplink

[Back to Top]

BCCH + CCCH



Downlink

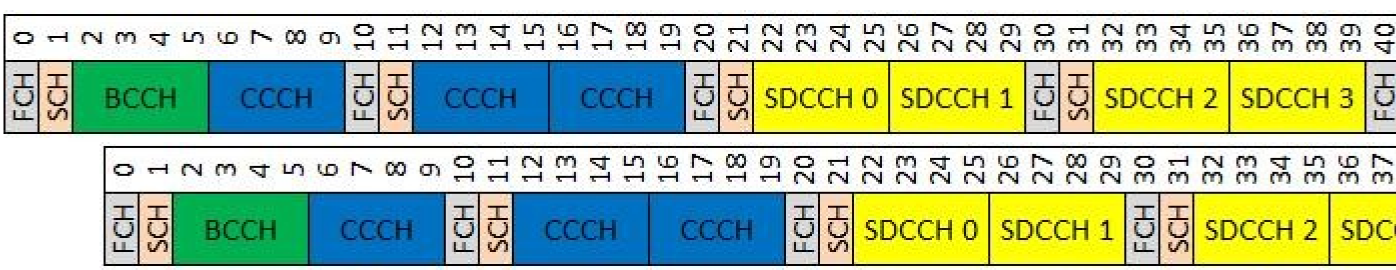


Uplink

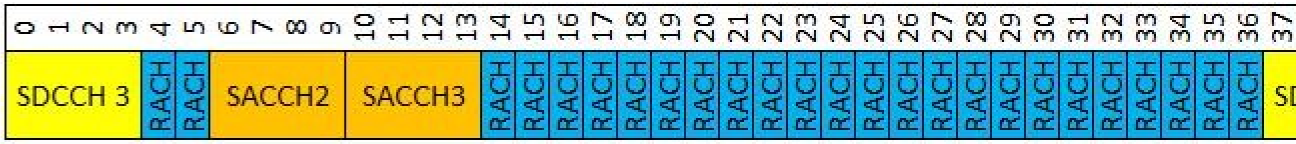
[Back to Top]

FCCH + SCH + BCCH + CCCH + SDCCH/4(0..3) + SACCH/C4(0..3)

The SACCH that is associated with each SDCCH is only transmitted every other multiframe. Each SACCH only gets half of the transmit time as the SDCCH that it is associated with. So, in one multiframe, SACCH0 and SACCH1 would be transmitted, and in the next multiframe, SACCH2 and SACCH3 would be transmitted. The two sequential multiframes would look like this:



Downlink



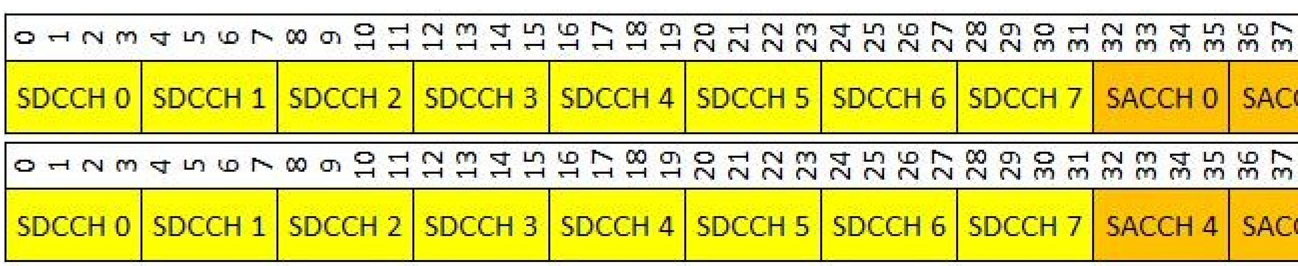
Uplink

You will also notice that the downlink and uplink multiframes do not align with each other. This is done so that if the BTS sends an information request to the MS, it does not have to wait an entire multiframes to receive the needed information. The uplink is transmitted 15 TDMA frames behind the downlink. For example, the BTS might send an authentication request to the MS on SDCCH0 (downlink) which corresponds to TDMA frames 22-25. The MS then has enough time to process the request and reply on SDCCH0 (uplink) which immediately follows it on TDMA frames 37-40.

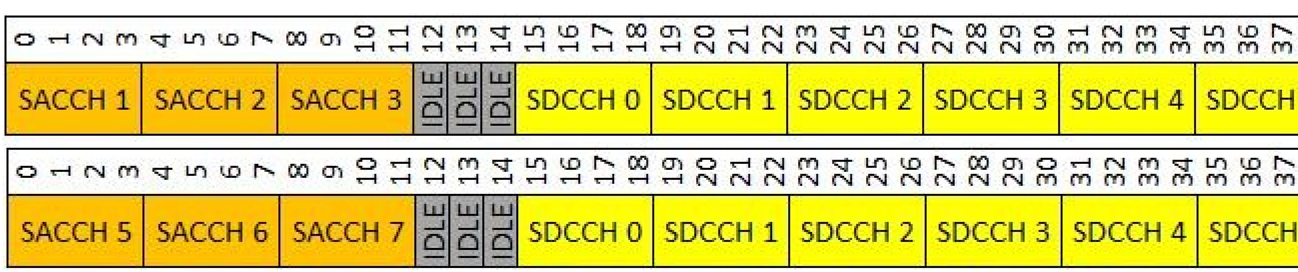
[Back to Top]

SDCCH/8(0 .7) + SACCH/C8(0 . 7)

Once again, the SACCH that is associated with an SDCCH is only transmitted every other multiframe. Two consecutive multiframes would look like this:



Downlink



Uplink

[Back to Top]

Traffic Channels (TCH)

Traffic Channels are used to carry two types of information to and from the user:

Encoded Speech
Data

There are two basic types of Encoded Speech channels:

Encoded Speech - Encoded speech is voice audio that is converted into digital form and compressed. See the Speech Encoding tutorial to see the process.
Full Rate Speech TCH (TCH/FS) - 13 kb/s
Half Rate Speech TCH (TCH/HS) - 5.6 kb/s

Data - Data refers to user data such as text messages, picture messages, internet browsing, etc. It includes pretty much everything except speech.

Full rate Data TCH (TCH/F14.1) - 14.4 kb/s
Full rate Data TCH (TCH/F9.6) - 9.6 kb/s
Full rate Data TCH (TCH/F4.8) - 4.8 kb/s
Half rate Data TCH (TCH/F4.8) - 4.8 kb/s
Full rate Data TCH (TCH/F2.4) - ≤2.4 kb/s
Half rate Data TCH (TCH/H2.4) - ≤2.4 kb/s

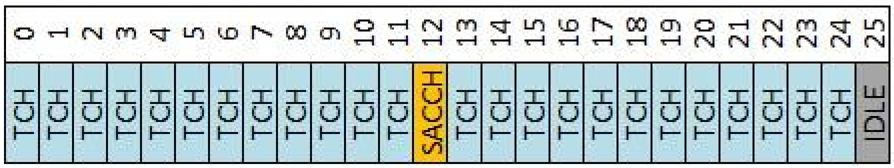
[Back to Top]

Traffic Channel Mapping

Time slots 2 through 7 are normally used for Traffic Channels (TCH)

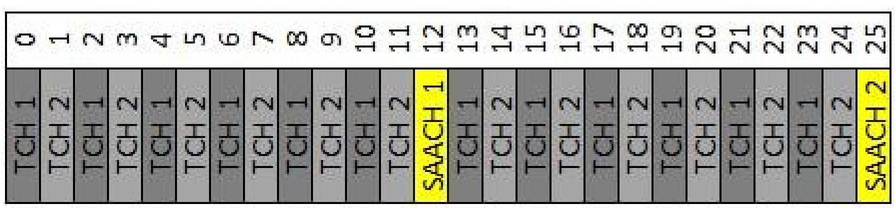
Traffic Channel Multiframes are composed of only 26 TDMA frames. On each multiframe, there are 24 frames for Traffic

Channels, 1 frame for a SACCH, and the last frame is Idle. Remember that a MS (or other device) only gets one time slot per TDMA frame to transmit, so in the following diagrams we are looking at a single time slot.



Full Rate Traffic Channel (TCH/FS)

When using Half-Rate Speech Encoding (TCH/HS), the speech encoding bit rate is 5.6 kb/s, so one time slot can handle two half-rate channels. In this case, one channel will transmit every other TDMA frame, and the other channel would be transmitted on the other frames. The final frame (25), which is normally used as an Idle frame, is now used as a SACCH for the second half-rate channel.

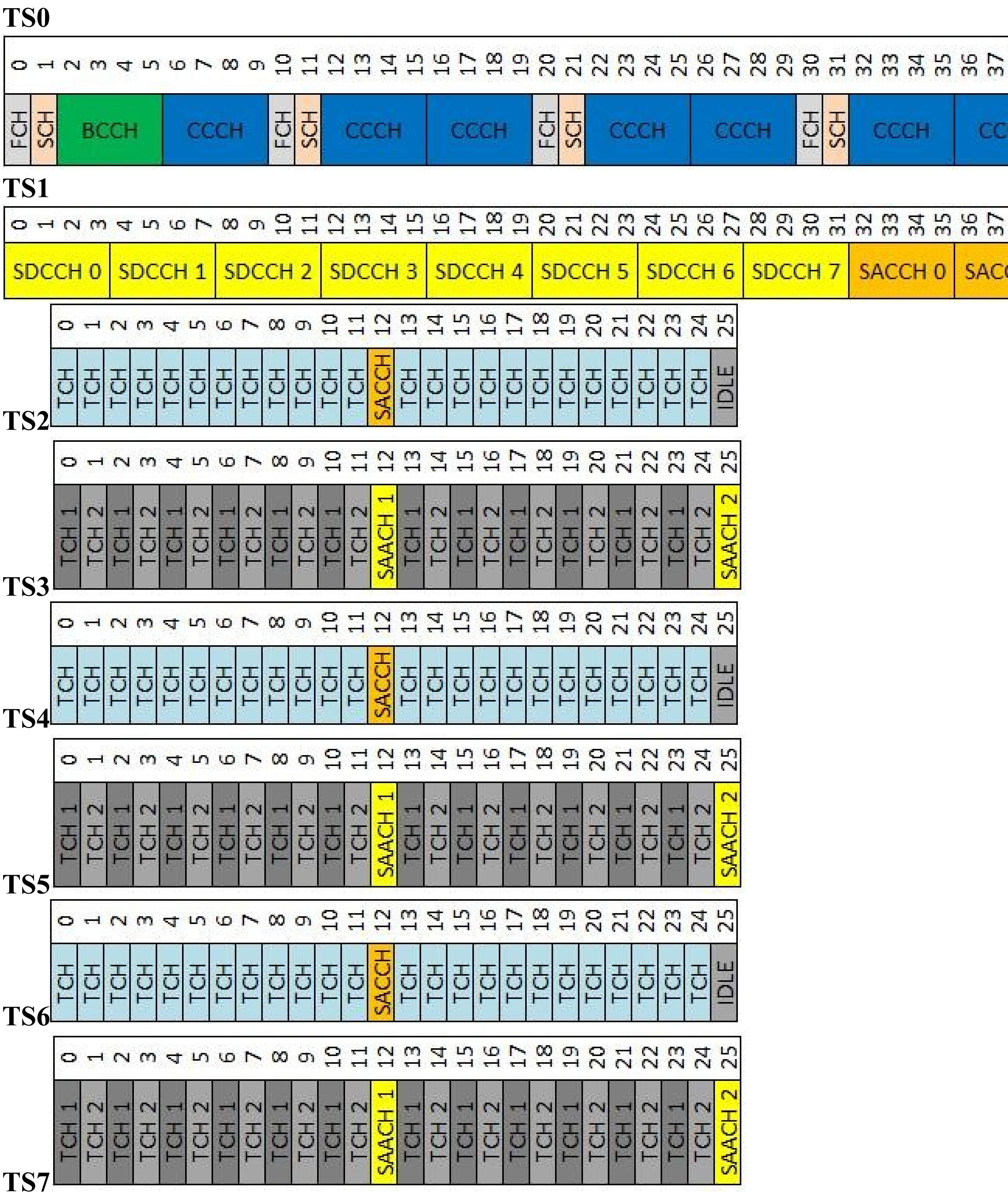


Half Rate Traffic Channel (TCH/HS)

[Back to Top]

ARFCN Mapping

This diagram shows a sample Multiframe with logical channels mapped to time slots and TDMA frames. This is just one possible configuration for an ARFCN.
***For illustrative purposes, half of the traffic channels are full-rate and the other half are half-rate**



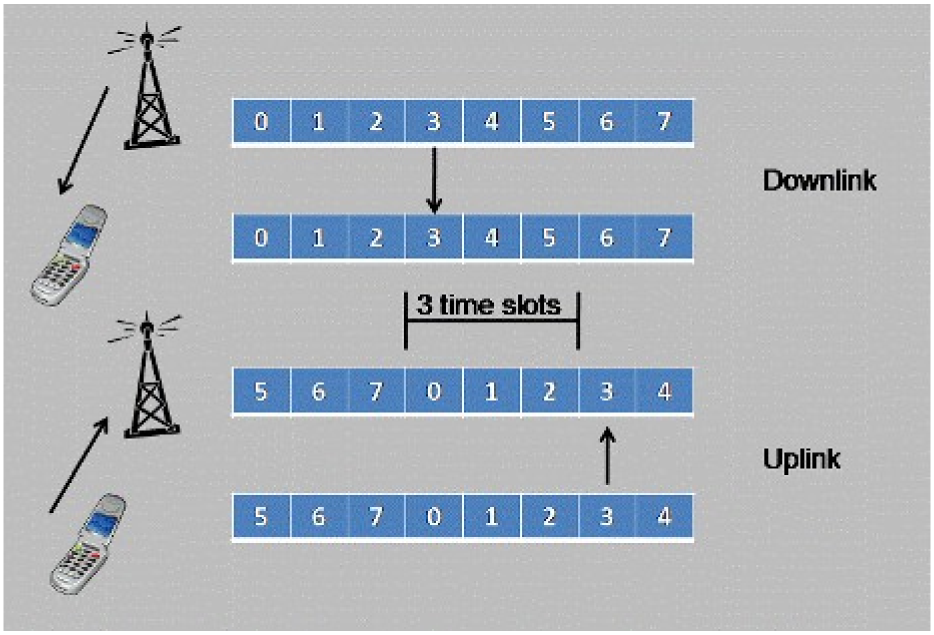
***Remember that CCH Multiframes have 51 frames and TCH Multiframes only have 26. Their sequences will synchronize every superframe.**

[Back to Top]

Offset

Even though GSM uses a full duplex radio channel, the MS and the BTS do not transmit at the exact same time. If a MS is assigned a given time slot, both the MS and the BTS will transmit during that given time slot, but their timing is offset. The uplink is exactly 3 time slots behind the downlink. For example, if the MS was allocated a TCH on TS3, the BTS would transmit when the downlink is on TS3 and the MS is set to receive on TS3. At this point, the uplink is only on TS0. Once the uplink reaches TS3, the MS would begin to transmit, and the BTS is set to receive on TS3. At this point, the downlink would be at TS6. When the MS is not transmitting or receiving, it switches frequencies to monitor the BCCH of adjacent cells.

<CENTER



[Back to Top]

Speech Data Throughput

When looking at a Time slot allocated to a TCH, you will notice that TCH does not occur on every single frame within a time slot. There is one

reserved for a SACCH and one that is Idle. So, in a TCH Multiframe, only 24 of the 26 frames are used for traffic (voice/data). This leaves us with a data throughput of 22.8 kb/s.

Here is the math:

1. Calculate bits per TCH Multiframe:
We know that there are 114 bits of data on a single burst, and we know that only 24 of the 26 frames in a TCH multiframe are used to send user data.
114 bits × 24 frames = 2736 bits per TCH multiframe

So, we know that on a single timeslot over the duration of one TCH multiframe, the data throughput is 2736 bits.

2. Calculate bits per millisecond (ms):
From step one above, we know that the throughput of a single TCH multiframe is 2736 bits. We also know that the duration of a TCH multiframe is 120ms.
2736 bits / 120 ms = 22.8 bits per millisecond

3. Convert milliseconds (ms) to seconds:
Now we need to put the value into terms of seconds. There are 1000 milliseconds in a second, so we simply multiply the value by 1000.
22.8 bits/millisecond × 1000 = 22,800 bits per second (22.8 kb/s)

4. Convert bits to kilobits:
Finally, we want to put it into terms of kilobits per second, wich is the most common term for referring to data throughput. We know a kilobit is 1000 bits, so we simply divide the term by 1000.
22,800 bits/s ÷ 1000 = 22.8 kb/s

So now we see why the data throughput of a single allocated timeslot is 22.8 kb/s.

There is an easier method to come to this number:

We know that only 24 of the 26 frames carry data, so we can say that the new throughput would be 24/26 of the original throughput. If we

convert this to decimal form:
24÷26 = .9231

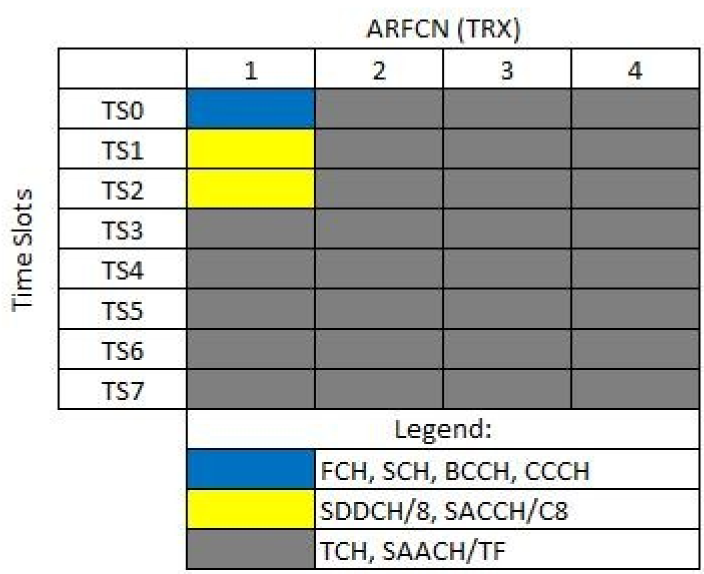
We know from the TDMA Tutorial that the data throughput of a single timeslot is 24.7 kb/s. Apply this 24/26 ratio to the 24.7 kb/s throughput:
24.7 × .9231 = 22.8 kb/s

You can see that we get the same answer as above.

A single BTS may have several Transceivers (TRX) assigned to it, each having its own ARFCN, each ARFCN having 8 time slots.

The logical channels that support signaling will normally only be on one ARFCN. All of the other ARFCNs assigned to a BTS will allocate all 8 time slots to Traffic Channels, to support multiple users.

The following diagram is an example of how a medium-sized cell might be set up with 4 TRX (ARFCNs).



Sample Medium-Size Cell

[Back to Top]

Frequency Hopping

Each radio frequency Channel (ARFCN) is influenced differently by propagation conditions. What affects channel 23 may not affect channel 78 at all. Within a given cell, some frequencies will have good propagation in a certain area and some will have poor propagation in that area. In order to take advantage of the good propagation and to defeat the poor propagation, GSM utilizes frequency hopping. Frequency hopping means that a transceiver hops from one frequency to another in a predetermined sequence. If a transceiver hops through all of the avilable frequencies in a cell then it will average out the propagation. GSM uses Slow Frequency Hopping (SFH). It is considered *slow* becuase the system hops relatively slow, compared with other frequency hopping systems. In GSM, the operating frequency is changed every TDMA frame.

The main reason for using slow frequency hopping is because the MS must also change its frequency often in order to monitor adjacent cells. The device in a transceiver that generates the frequency is called a *frequency synthesizer*. On a MS, a synthesizer must be able to change its frequency within the time frame of one time slot, which is equal to 577 µs. GSM does not require the BTS to utilize frequency hopping. However, a MS must be capable of utilizing frequency hopping when told to do so.

The frequency hopping and timing sequence is known as the *hopping algorithm*. There are two types of hopping algorithms available to a MS.

Cyclic Hopping - The transceiver hops through a predefined list of frequencies in sequential order.

Random Hopping - The transceiver hops through the list of frequencies in a random manner. The sequence *appears* random but it is actually a set order.

There are a total of 63 different hopping algorithms available in GSM. When the MS is told to switch to frequency hopping mode, the BTS will assign it a list of channels and the *Hopping Sequence Number* (HSN), which corresponds to the particular hopping algorithm that will be used.

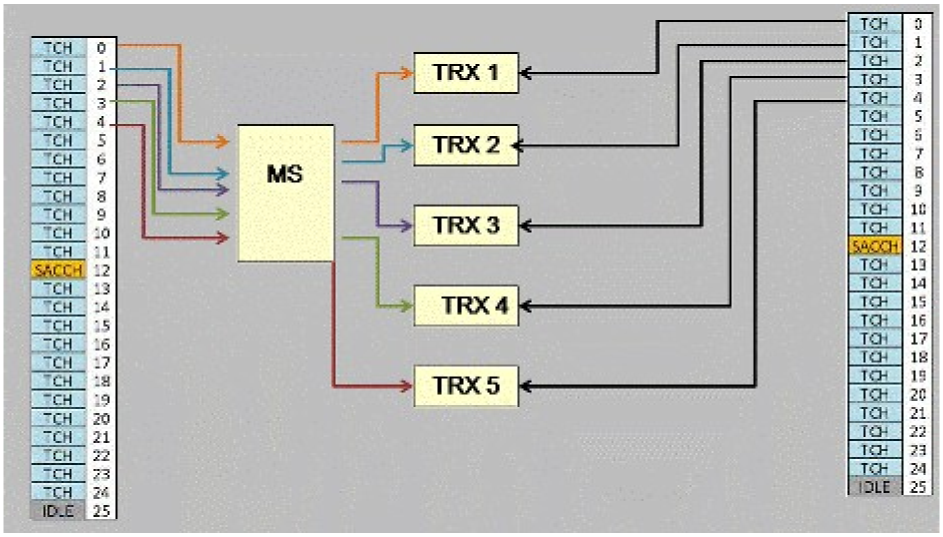
The base channel on the BTS does not frequency hop. This channel, located in time slot 0, holds the Broadcast Control Channels which the MS needs to monitor to determine strength measurements, determine access parameters, and synchronize with the system.

If a BTS uses multiple transceivers (TRX) then only one TRX will hold the the Broadcast Channels on time slot 0. All of the other TRXs may use time slot 0 for traffic or signaling and may take part in the frequency hopping.

There are two types of frequency hopping method available for the BTS: *synthesizer hopping* and *baseband hopping*.

Synthesizer Hopping - This requires the TRX itself to change frequencies according to the hopping sequence. So, one TRX would hop between multiple frequencies on the same sequence that the MS is required to.

Baseband Hopping - In this method there are several TRX and each one stays on a fixed frequency within the hopping frequency plan. Each TRX would be assigned a single time slot within a TDMA frame. For example, time slot 1 might be assigned to TRX 2 in one TDMA frame and in the next TDMA frame it would be assigned to TRX 3, and the next frame would be TRX 3. So, the data on each time slot would be sent on a different frequency each frame, but the TRXs on the BTS do not need to change frequency. The BTS simply routes the data to the appropriate TRX, and the MS knows which TRX to be on for any given TDMA frame.



Baseband Frequency Hopping

Signaling Channels Broadcast Channels (BCCH FCCH SCH CBCH) Common Control Channels (PCH RACH AGCH)
SDCCH Associated Control Channels (FACCH SACCH) Signal Channel Mapping

Traffic Channels Encoded Speech Data Traffic Channel Mapping ARFCN Mapping Frequency Hopping

Introduction Architecture TDMA Logical Channels Authentication & Encryption
Timing Advances Speech Encoding GSM Events
Updates Bulletin Board Sitemap Contact Me

Home

Timing Advances

Access Burst   Duration of a Bit   Propagation Delay   Max Cell Size   Determining a TA   Distance of a TA

Home

`

Introduction

A Timing Advance (TA) is used to compensate for the propagation delay as the signal travels between the Mobile Station (MS) and Base Transceiver Station (BTS). The Base Station System (BSS) assigns the TA to the MS based on how far away it perceives the MS to be. Determination of the TA is a normally a function of the Base Station Controller (BSC), bit this function can be handled anywhere in the BSS, depending on the manufacturer.

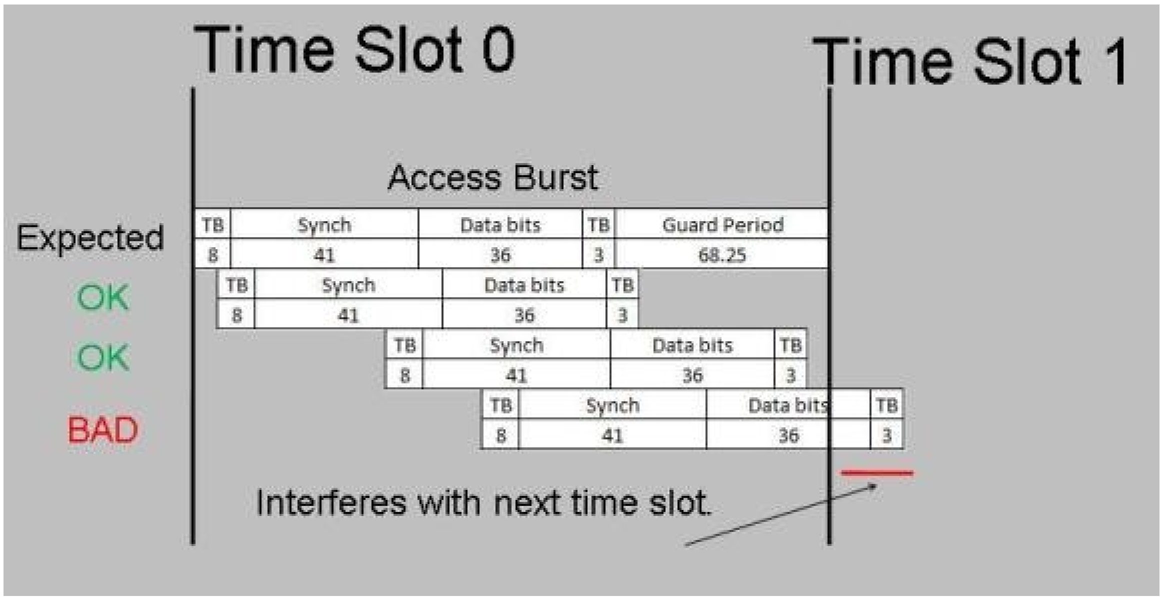
Time Division Multiple Access (TDMA) requires precise timing of both the MS and BTS systems. When a MS wants to gain access to the network, it sends an access burst on the RACH. The further away the MS is from the BTS, the longer it will take the access burst to arrive at the BTS, due to propagation delay. Eventually there comes a certain point where the access burst would arrive so late that it would occur outside its designated timeslot and would interfere with the next time slot.

Access Burst

As you recall from the TDMA Tutorial, an access burst has 68.25 guard bits at the end of it.

TB	Synch	Data bits	TB	Guard Period
8	41	36	3	68.25

This guard time is to compensate for propagation delay due to the unknown distance of the MS from the BTS. It allows an access burst to arrive up to 68.25 bits later than it is supposed to without interfering with the next time slot.



68.25 bits doesnt mean much to us in the sense of time, so we must convert 68.25 bits into a frame of time. To do this, it is necessary to calculate the duration of a single bit, the duration is the amount of time it would take to transmit a single bit.

[Back to Top]

Duration of a Single Bit

As you recall, GSM uses Gaussian Minimum Shift Keying (GMSK) as its modulation method, which has a data throughput of 270.833 kilobits/second (kb/s).

Calculate duration of a bit.

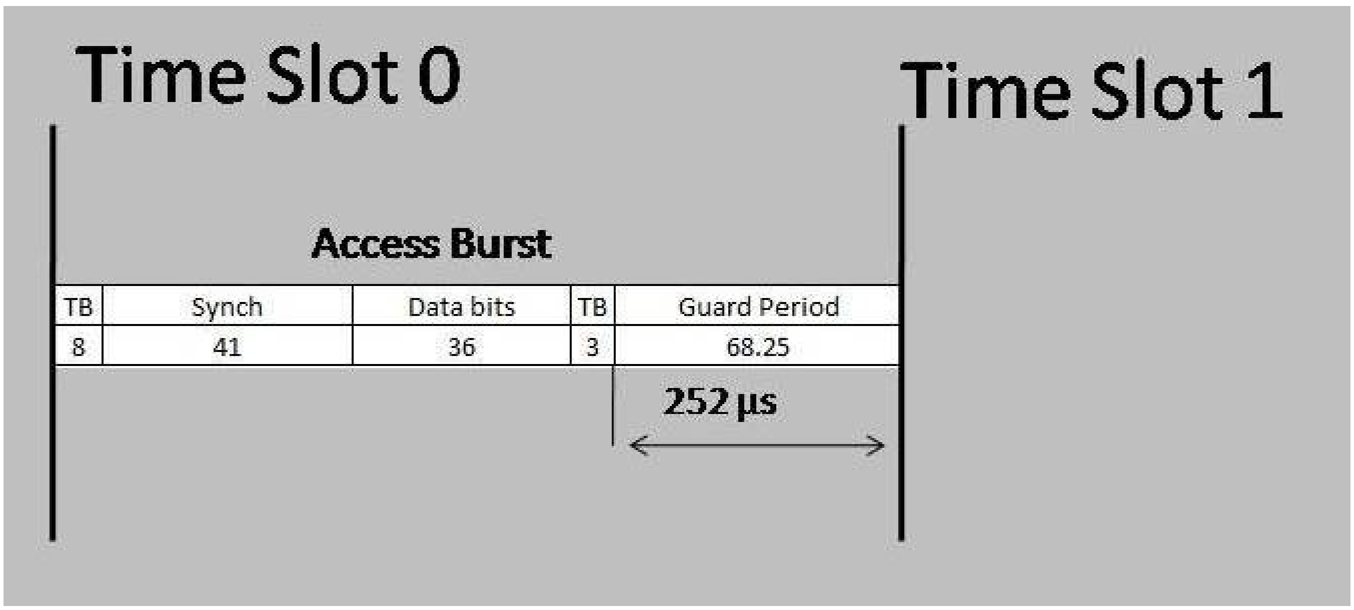
Description	Formula	Result
Convert kilobits to bits	270.833 kb × 1000	270,833 bits
Calculate seconds per bit	1 sec ÷ 270,833 bits	.00000369 seconds
Convert seconds to microseconds	.00000369 sec × 1,000,000	3.69 µs

So now we know that it takes 3.69µs to transmit a single bit.

[Back to Top]

Propagation Delay

Now, if an access burst has a guard period of 68.25 bits this results in a maximum delay time of approximately 252µs (3.69µs × 68.25 bits). This means that a signal from the MS could arrive up to 252µs after it is expected and it would not interfere with the next time slot.



The next step is to calculate how far away a mobile station would have to be for a radio wave to take 252µs to arrive at the BTS, this would be the theoretical maximum distance that a MS could transmit and still arrive within the correct time slot.

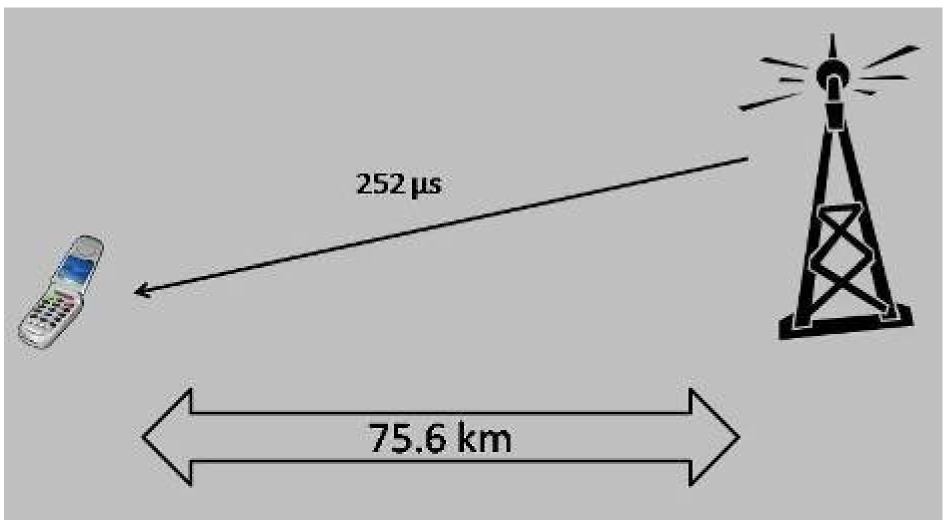
Using the speed of light, we can calculate the distance that a radio wave would travel in a given time frame. The speed of light (c) is 300,000 km/s.

Description	Formula	Result
Convert km to m	300,000km × 1000	300,000,000m
Convert m/s to m/µs	300,000,000 ÷ 1,000,000	300 m/µs
Calculate distance for 252µs	300 m/µs × 252µs	75600m
Convert m to km	75,600m ÷ 1000	75.6km

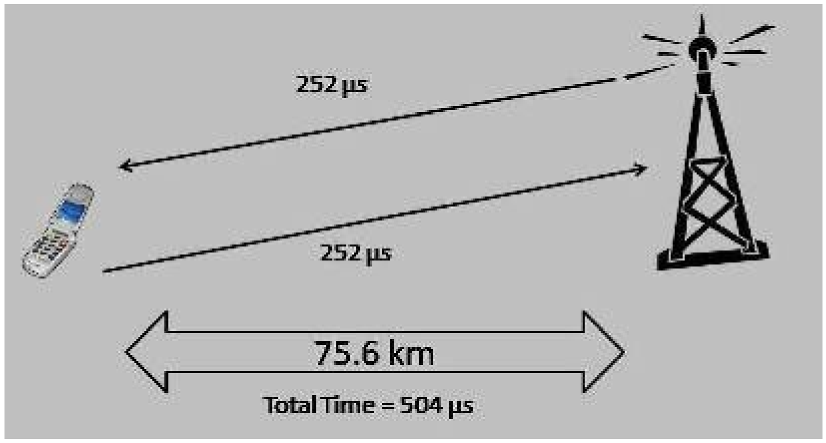
So, we can determine that a MS could theoretically be up to 75.6km away from a BTS when it transmits its access burst and still not interfere with the next time slot.

However, we must take into account that the MS synchronizes with the signal it receives from the BTS. We must account for the time it takes for the synchronization signal to travel from the BTS to the MS. When the MS receives the synchronization signal from the BTS, it has no way of determining how far away it is from the BTS. So, when the MS receives the syncronization signal on the SCH, it synchronizes its time with the timing of the system. However, by the time the signal arrives at the MS, the timing of the BTS has already progressed some. Therefore, the timing of the MS will now be behind the timing of the BTS for an amount of time equal to the travel time from the BTS to the MS.

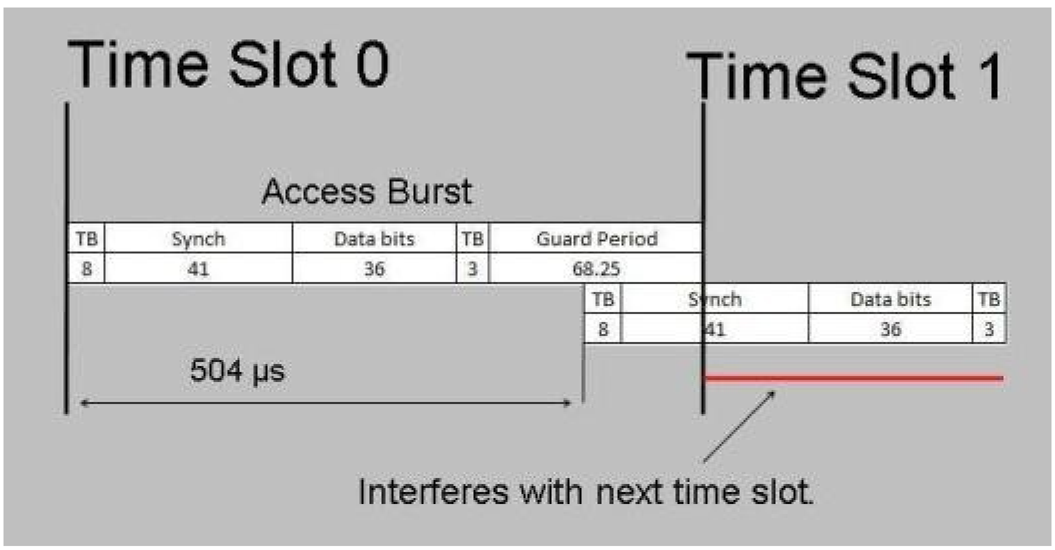
For example, if a MS were exactly 75.6km away from the BTS, then it would take 252µs for the signal to travel from the BTS to the MS.



The MS would then synchronize with this timing and send its access burst on the RACH. It would take 252µs for this signal to return to the BTS. The total round trip time would be 504µs. So, by the time the signal from the MS arrives at the BTS, it will be 504µs behind the timing of the BTS. 504µs equals about 136.5 bits.



The 68.25 bits of guard time would absorb some of the delay of 136.5 bits, but the access burst would still cut into the next time slot a whopping 68.25bits.



[Back to Top]

Maximum Size of a Cell

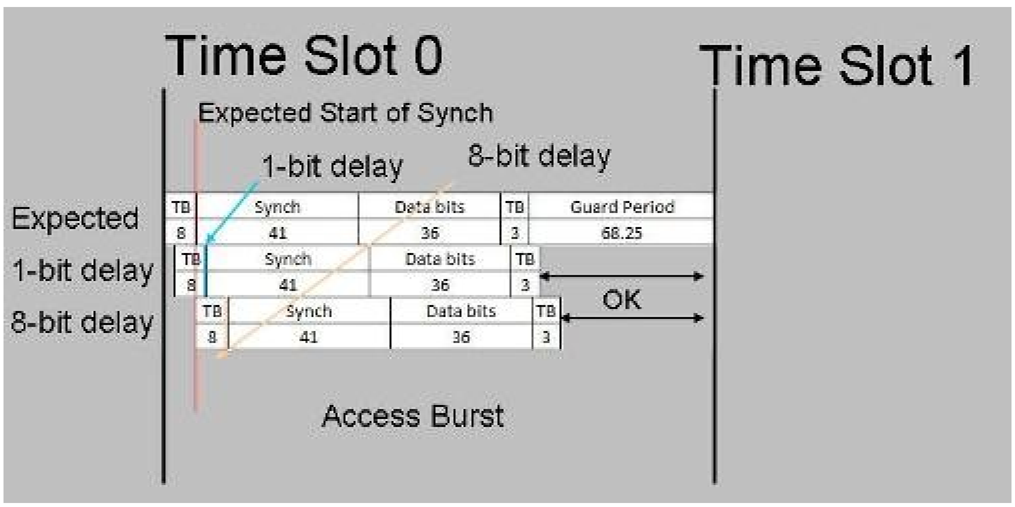
In order to compensate for the two-way trip of the radio link, we must divide the maximum delay distance in half. So, dividing 75.6km in half, we get approximately 37.8 km. If a MS is further out than 37.8km and transmits an access burst it will most likely interfere with the following time slot. Any distance less than 37.8km and the access burst should arrive within the guard time allowed for an access burst and it will not interfere with the next time slot.

In GSM, the maximum distance of a cell is standardized at 35km. This is due mainly to the number of timing advances allowed in GSM, which is explained below.

[Back to Top]

How a BSS Determines a Timing Advance

In order to determine the propagation delay between the MS and the BSS, the BSS uses the synchronization sequence within an access burst. The BSS examines the synchronization sequence and sees how long it arrived after the time that it expected it to arrive. As we learned from above, the duration of a single bit is approximately 3.69µs. So, if the BSS sees that the synchronization is late by a single bit, then it knows that the propagation delay is 3.69µs. This is how the BSS knows which TA to send to the MS.



For each 3.69µs of propagation delay, the TA will be incremented by 1. If the delay is less than 3.69µs, no adjustment is used and this is known as TA0. For every TA, the MS will start its transmission 3.69µs (or one bit) early. Each TA really corresponds to a range of propagation delay. Each TA is essentially equal to a 1-bit delay detected in the synchronization sequence.

TA	From	To
0	0µs	3.69µs
1	3.69µs	7.38µs
2	7.38µs	11.07µs
3	11.07µs	14.76µs
...	...	...
63	232.47µs	236.16µs

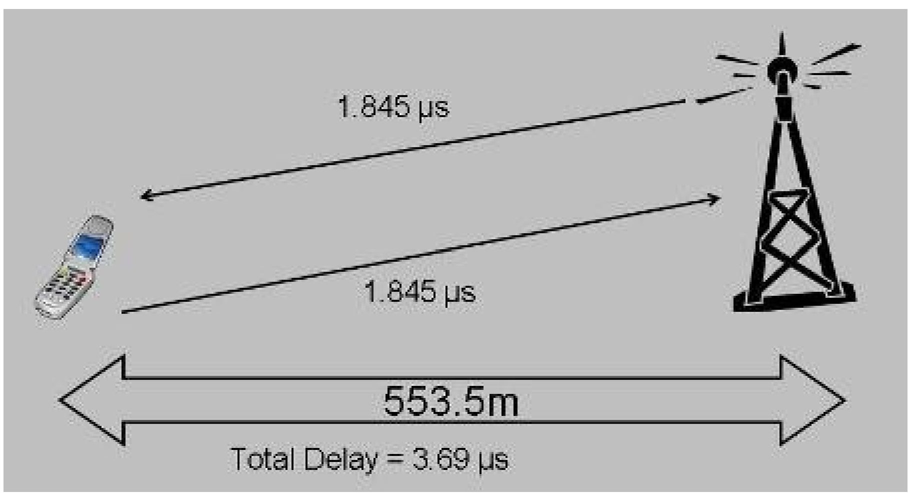
[Back to Top]

The Distance of a Timing Advance

When calculating the distances involved for each TA, we must remember that the total propagation delay accounts for a two-way trip of the radio wave. The first leg is the synchronization signal traveling from the BTS to the MS, and the second leg is the access burst traveling from the MS to the BTS. If we want to know the true distance of the MS from the BTS, we must divide the total propagation delay in half.

For example, if the BSS determines the total propagation delay to be 3.69µs, we can determine the distance of the MS from the BTS.

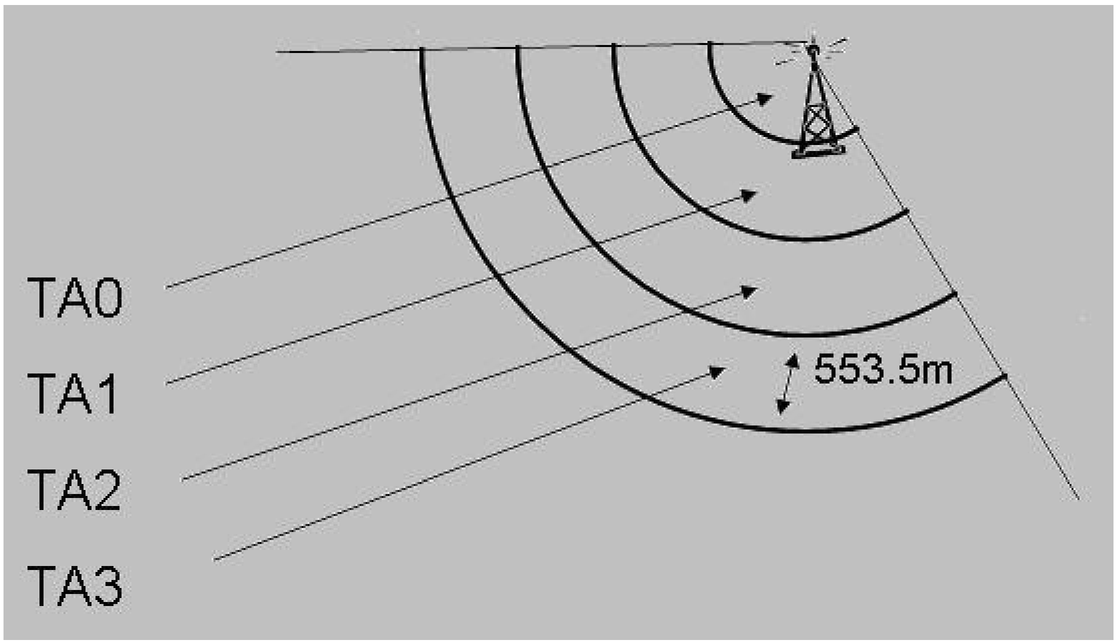
Description	Formula	Result
Determine one-way propagation time	3.69µs ÷ 2	1.845µs
Calculate distance (using speed of light.)	300 m/µs × 1.845µs	553.5m



We determined earlier that for each propagation delay of 3.69µs the TA is inceremented by one. We just learned that a propagation delay of 3.69µs equals a one-way distance of 553.5 meters. So, we see that each TA is equal to a distance of 553.5 meters from the tower. Starting from the BTS (0 meters) a new TA will start every 553.5m.

TA Ring	Start	End
0	0	553.5m

1	553.5m	1107m
2	1107m	1660.5m
3	1660.5m	2214m
...	...	...
63	34.87km	35.42km



The TA becomes very important when the MS switches over to using a normal burst in order to transmit data. The normal burst does not have the 68.25 bits of guard time. The normal burst only has 8.25 bits of guard time, so the MS must transmit with more precise timing. With a guard time of 8.25 bits, the normal burst can only be received up to 30.44µs late and not interfere with the next time slot. Because of the two-way trip of the radio signal, if the MS transmits more than 15.22µs after it is supposed to then it will interfere with the next time slot.

GSM Events

IMSI Attach IMSI Detach Location Update Mobile-Originated Call Mobile-Terminated Call

Home

Whenever a Mobile Station (MS) needs some kind of service from the network, a series of messages are sent across different links in order to facilitate this service. Some examples include Location Update, IMSI Attach, IMSI Detach, and placing and receiving calls. These tutorials illustrate some of the different tasks that are needed to facilitate service and the messages that are exchanged in order to complete those tasks. Choose one of the events from the menu above to view how it works.

Authentication and encryption are not considered an "event" since it is required every time the MS requests access to the network. Authentication and encryption is covered in detail here.

*Note: For all GSM events, only the signaling messages for the Air (Um) Interface are specified on this website. In the future, messages for all interfaces will be included on the website.

IMSI Attach IMSI Detach Location Update Mobile-Originated Call Mobile-Terminated Call

Introduction Architecture TDMA Logical Channels Authentication & Encryption Timing Advances Speech Encoding GSM Events
Updates Bulletin Board Sitemap Contact Me

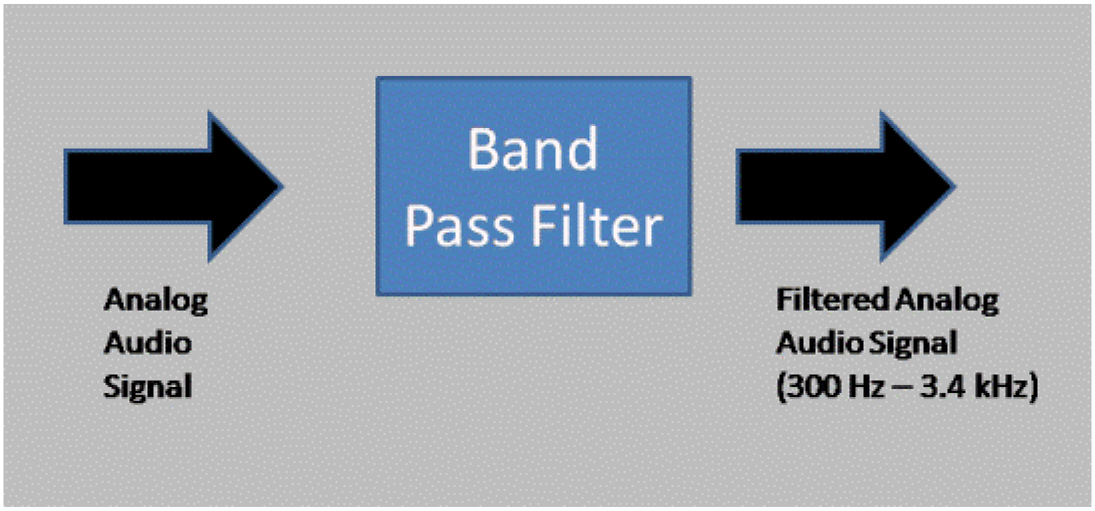
Home

Speech Coding

Analog to Digital Conversion

In order to fully understand speech and channel coding it is easier to start from the very beginning of the process. The first step in speech coding is to transform the sound waves of our voices (and other ambient noise) into an electrical signal. This is done by a *microphone*. A microphone consists of a diaphragm, a magnet, and a coil of wire. When you speak into it, sound waves created by your voice vibrate the diaphragm which is connected to the magnet which is inside the coil of wire. These vibrations cause the magnet to move inside the coil at the same frequency as your voice. A magnet moving in a coil of wire creates an electric current. This current which is at the same frequency as the sound waves is carried by wires to whereever you wish it to go like an amplifier, transmitter, etc. Once it gets to its destination the process is reversed and it comes out as sound. Speakers basically being the opposite of microphones. The signal created by a microphone is an analog signal. Since GSM is an all digital system, this analog signal is not suitable for use on a GSM network. The analog signal must be converted into digital form. This is done by using an Analog to Digital Converter (ADC).

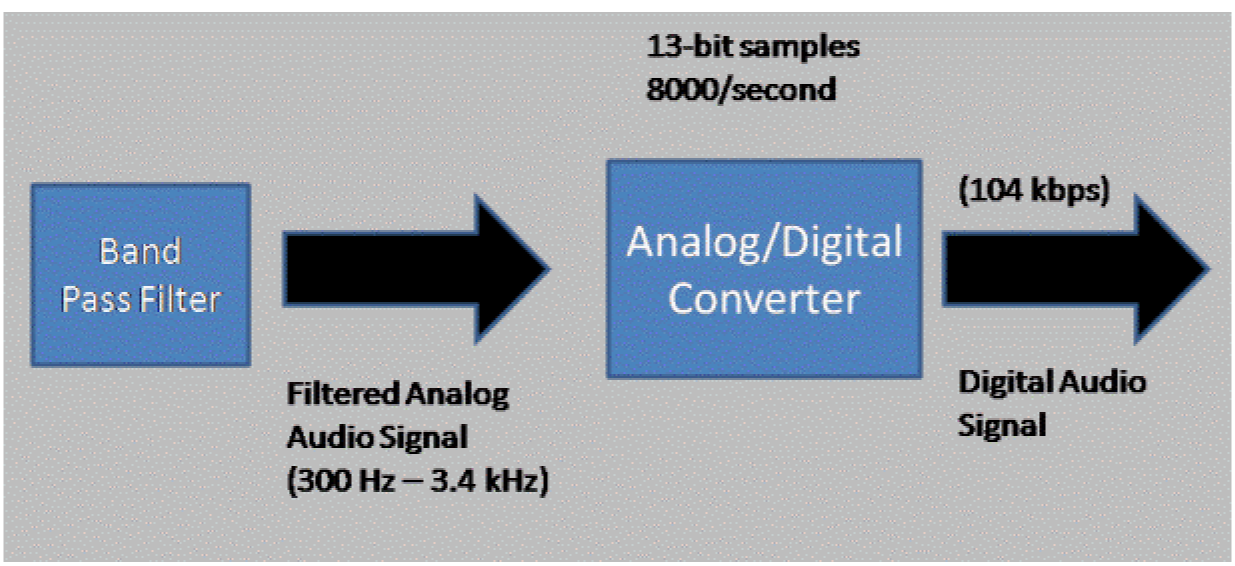
In order to reduce the amount of data needed to represent the sound wave, the analog signal is first inputted into a *band pass filter*. Band pass means that the filter only allows signal that fall within a certain frequency range to pass through it, and all other signals are cut off, or *attenuated*. The BP filter only allows frequencies between 300Hz and 3.4 kHz to pass through it. This limits the amount of data that the Analog/Digital Converter is required to process.



Band Pass Filter

The filtered signal is inputted into the analog/digital converter. The analog/digital converter performs two tasks. It converts an analog signal into a digital signal and it does the opposite, converts a digital signal into an analog signal.

In the case of a cell phone, the analog signal created by a microphone is passed to the analog/digital converter. The A/D converter measures the analog signal, or *samples* it 8000 times per second. This means that the ADC takes a sample of the analog signal every .125 sec (125 µs). Each sample is quantified with a 13-bit data block. If we calculate 13 bits per sample at 8000 samples per second, we determine a data rate of 104,000 bits per second, or 104 kb/s.



Analog/Digital Converter

A data rate of 104 kbps is far too large to be economically handled by a radio transmitter. In order to reduce the bitrate, the signal is inputted into a speech encoder.A speech encoder is a device that compresses the data of a speech signal. There are many types of speech encoding schemes available. The speech encoder used in GSM is called Linear Predictive Coding (LPC) and Regular Pulse Excitation (RPE). LPC is a very complicated and math-heavy process, so it will only be summarized here.

[Back to Top]

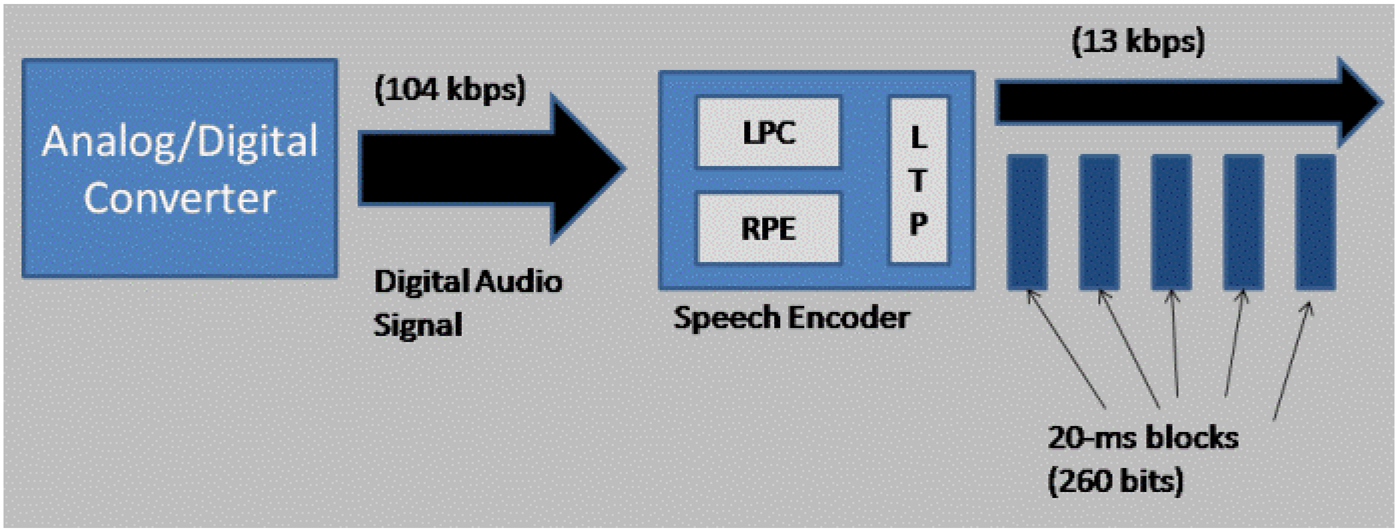
Linear Predictive Coding (LPC)

Remember that the ADC quantifies each audio sample with a 13-bit "word". In LPC, 160 of the 13-bit samples from the converter are saved up and stored into short-term memory. Remember that a sample is taken every 125 µs, so 160 samples covers an audio block of 20ms. This 20ms audio block consists of 2080 bits. LPC-RPE analyzes each 20ms set of data and determines 8 coefficients used for filtering as well as an excitation signal. LPC basically identifies specific bits that correspond to specific aspects of human voice, such as vocal modifiers (teeth, tongue, etc.) and assigns coefficients to them. The excitation signal represents things like pitch and loudness. LPC identifies a number of correlations of human voice and redundancies in human speech and removes them.

The LPC/RPE sequence is then fed into the Long-Term Prediction (LTP) Analysis function. The LTP function compares the sequence it receives with earlier sequences stored in its memory and selects the sequence that most resembles the current sequence. The LTP function then calculates the difference between the two sequences. Now the LTP function only has to translate the difference value as well as a pointer indicating which earlier sequence it used for comparison. By doing this is prevents encoding redundant data.

You can envision this by thinking about the sounds we make when we talk. When we pronounce a syllable, each little sound has a specific duration that seems short when we are talking but often lasts longer than 20ms. So, one sound might be represented by several 20ms-block of exactly the same data. Rather than transmit redundant data, LPC only includes data that tells the receiving which data is redundant so that it can be created on the receiving end.

Using LPC/RPE and LTP, the speech encoder reduces the 20ms block from 2,080 bits to to 260 bits. Note that this is a reduction by eight times. 260 bits every 20ms gives us a net data rate of 13 kilobits per second (kbps).



Speech Encoding

This bitrate of 13kbps is known as Full Rate Speech (FS). There is another method for encoding speech called Half Rate Speech (HS), which results in a bit rate of approximately 5.6kbps. The explanations in the remainder of this tutorial are based on a full-rate speech bitrate (13kbps).

Calculate the net data rate:

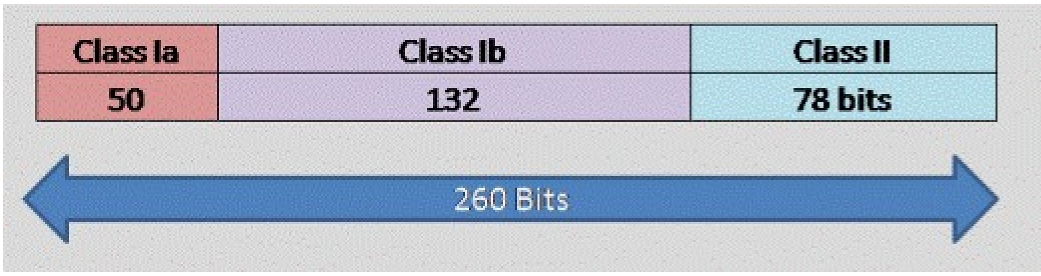
Description	Formula	Result
Convert ms to sec	20 ms ÷ 1000	.02 seconds
Calculate bits per second	260 bits ÷ .02 seconds	13,000 bits per second (bps)
Convert bits to kilobits	13,000 bps ÷ 1000	13 kilobits per sec (kbps)

As we all know, the audio signal must be transmitted across a radio link from the handset to the Base Station Transceiver (BTS). The signal on this radio link is subject to atmospherics and fading which results in a large amount of data loss and degrades the audio. In order to prevent degradation of audio, the data stream is put through a series of error detection and error correction procedures called *channel coding*. The first phase of channel coding is called *block coding*.

[Back to Top]

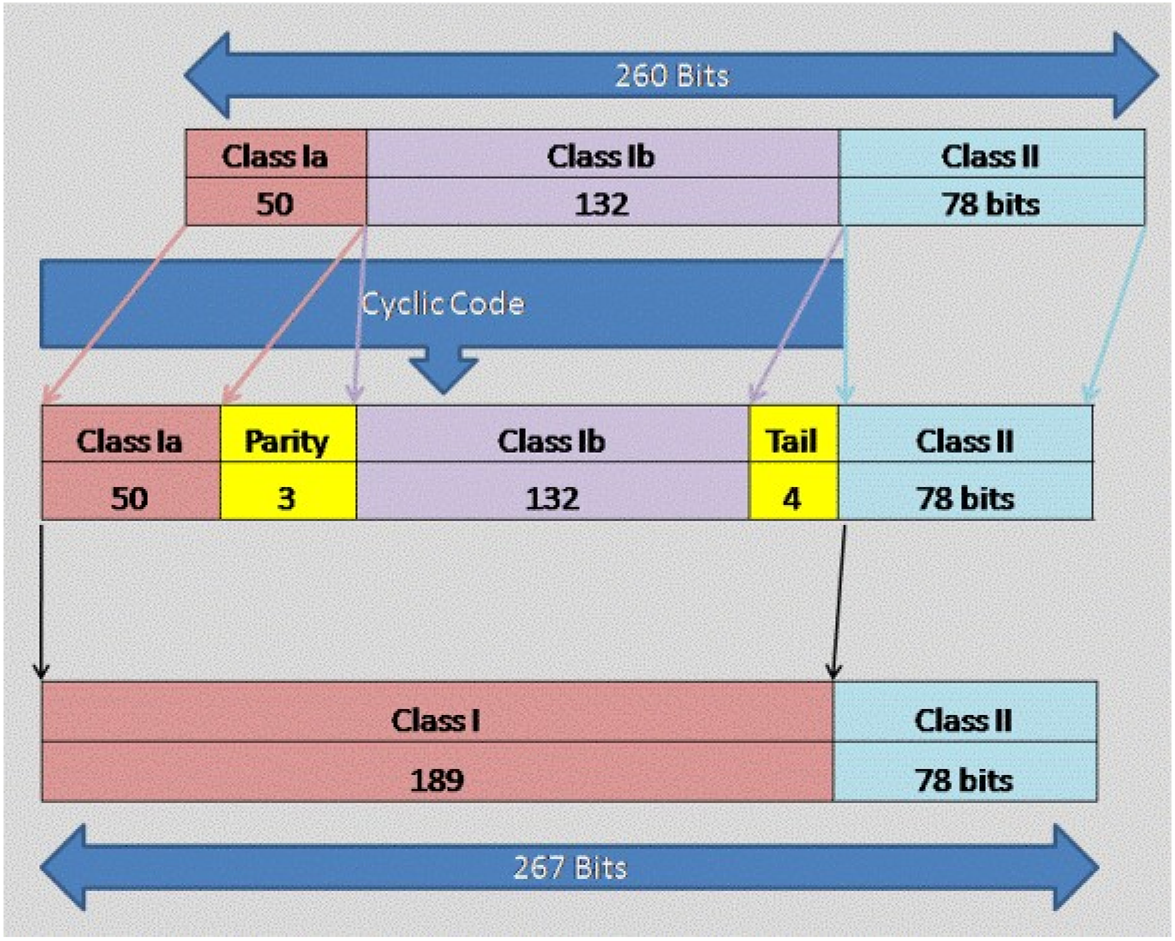
Block Coding

A single 260-bit (20ms) audio block is delivered to the block-coder. The 260 bits are divided up into classes according to their importance in reconstructing the audio. Class I are the bits that are most important in reconstructing the audio. The class II bits are the less important bits. Class I bits are further divided into two categories, Ia and Ib.



Classes of Bits

The class Ia bits are protected by a cyclic code. The cyclic code is run on the 50 Ia bits and calculates 3 parity bits which are then appended to the end of the Ia bits. Only the class Ia bits are protected by this cyclic code. The Ia and Ib bits are then combined and an additional 4 bits are added to the tail of the class I bits (Ia and Ib together). All four bits are zeros (0000) and are needed for the next step which is "convolutional coding". There is no protection for class II bits. As you can see, block coding adds seven bits to the audio block, 3 parity bits and 4 tail bits, therefore, a 260-bit block becomes a 267-bit block.



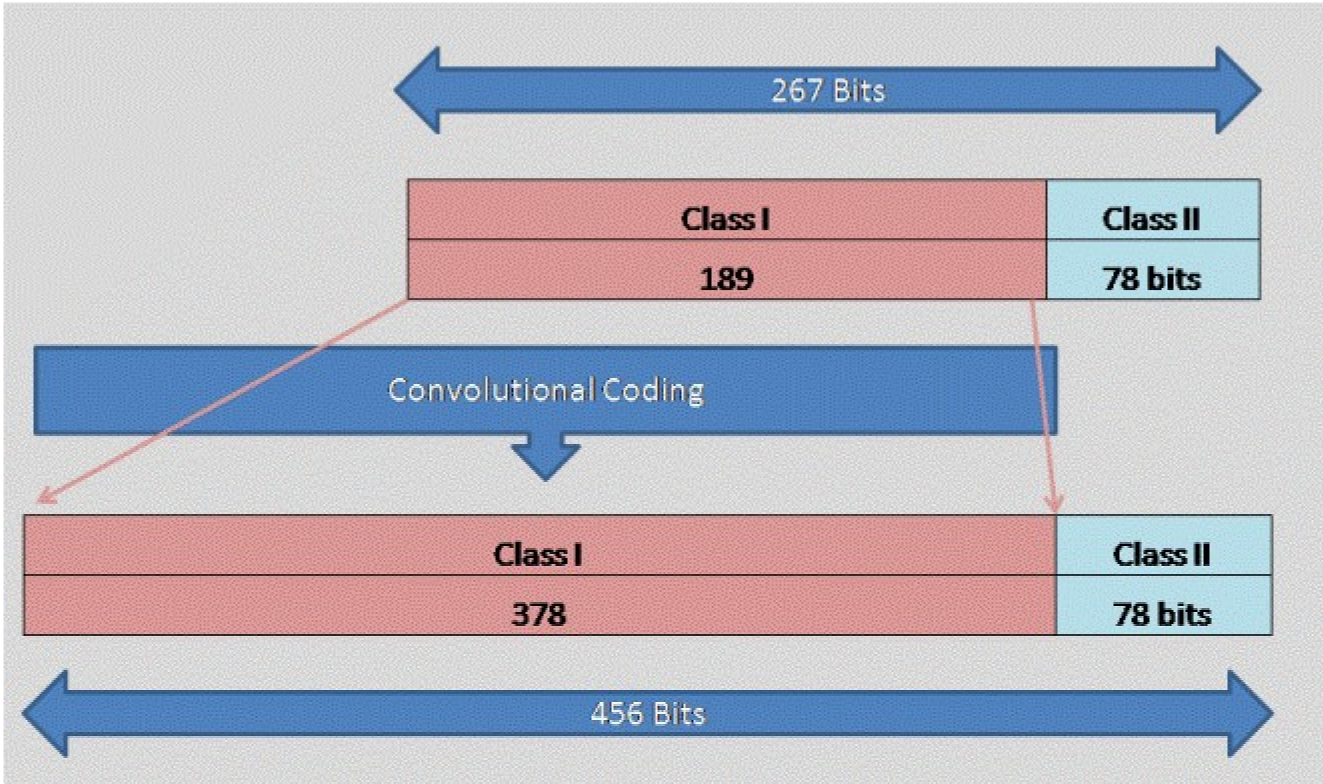
Block Coding

[Back to Top]

Convolutional Coding

This 267-bit block is then inputted into a convolutional code. Convolutional coding allows errors to be detected and to be corrected to a limited degree. The class I "protected" bits are inputted into a complex convolutional code that outputs 2 bits for every bit that enters it. The second bit that is produced is known as a redundancy bit. The number of class I bits is doubled from 189 to 378.

This coding uses 5 consecutive bits to calculate the redundancy bit, this is why there are 4 bits added to the class I bits when the cyclic code was calculated. When the last data bit enters the register, it uses the remaining four bits to calculate the redundancy bit for the last data bit. The class II bits are not run through the convolutional code. After convolutional coding, the audio block is 456 bits



Convolutional Coding

[Back to Top]

Reordering, Partitioning, and Interleaving

Now, one problem remains. All of this error detection and error correction coding will not do any good if the entire 456-bit block is lost or garbled. In order to alleviate this, the bits are reordered and partioned onto eight separate sub-blocks. If one sub-block is lost then only one-eighth of the data for each audio block is lost and those bits can be recovered using the convolutional code on the receiving end. This is known as *interleaving*.

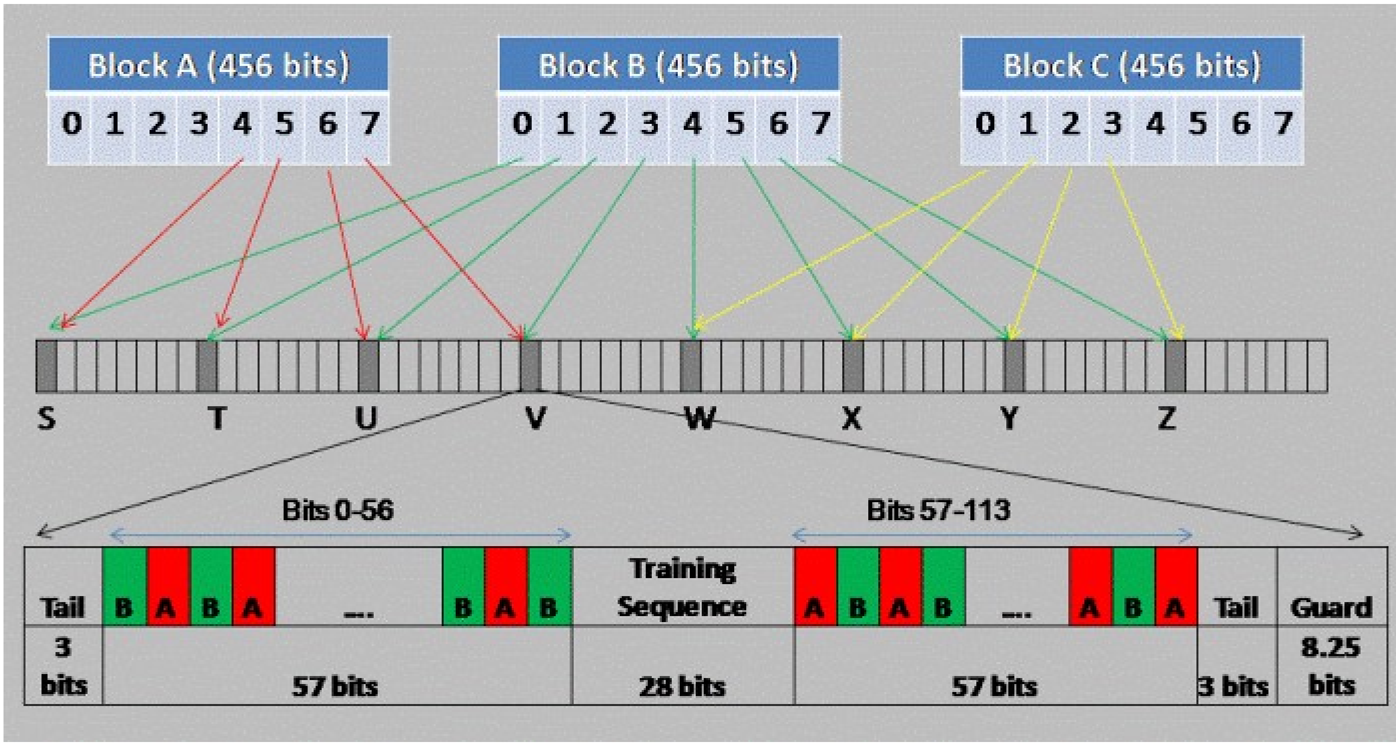
Each 456-bit block is reordered and partitioned into 8 sub-blocks of 57 bits each. Click Here to see the ordering sequence.

These eight 57-bit sub-blocks are then interleaved onto 8 separate bursts. As you remember from the TDMA Tutorial, each burst is composed of two 57-bit data blocks, for a total data payload of 114 bits.

The first four sub-blocks (0 through 3) are mapped onto the even bits of four consecutive bursts. The last four sub-blocks (4 through 7) are mapped onto the odd bits of the next 4 consecutive bursts. So, the entire block is spread out across 8 separate bursts.

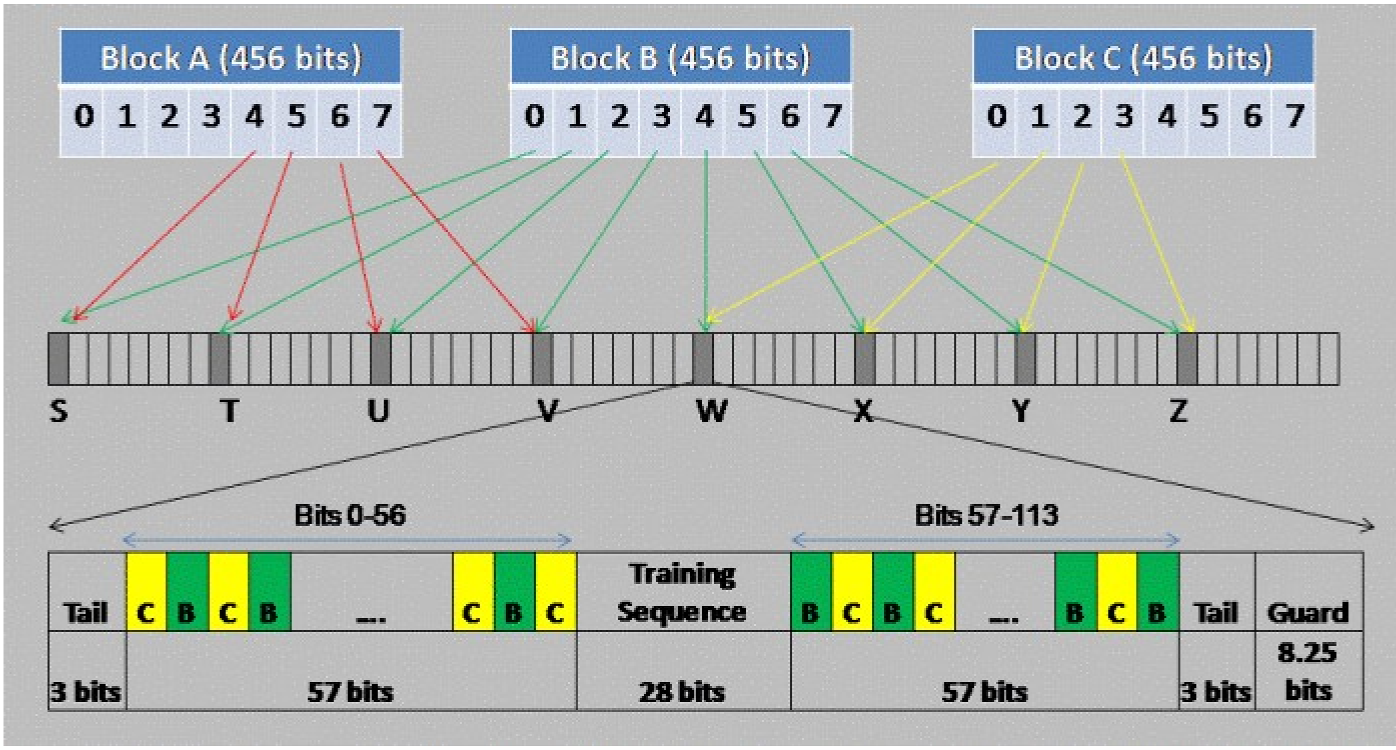
Taking a look at the diagram below we see three 456-bit blocks, labeled A, B, and C. Each block is sub-divided into eight sub-blocks numbered 0-7. Let's take a look at Block B. We can see that each sub-block is mapped to a burst on a single time-slot. Block B is mapped onto 8 separate bursts or time-slots. For illustrative purposes, the time-slots are labeled S through Z.

Let's expand time-slot V for a close-up view. We can see how the bits are mapped onto a burst. The bits from Block B, sub-block 3 (B3) are mapped onto the even numbered bits of the burst (bits 0,2,4....108,110,112). You will also notice that the odd bits are being mapped from data from block A, sub-block 7 (bits 1,3,5....109,111,113). Each burst contains 57 bits of data from two separate 456-bit blocks. This process is known as *interleaving*.



Reordering, Partitioning, and Interleaving

In the following diagram, we examine time-slot W. We see that bits from B4 are mapped onto the odd-number bits (bits 1,3,5....109,111,113) and we would see bits from C1 mapped onto the even number bits (bits 0,2,4....108,110,112). This process continues indefinitely as data is transmitted. Time-slots W, X, Y, and Z would all be mapped identically. The next time-slot would have data from Block C and Block D mapped onto it. This process continues for as long as there is data being generated.



Interleaving

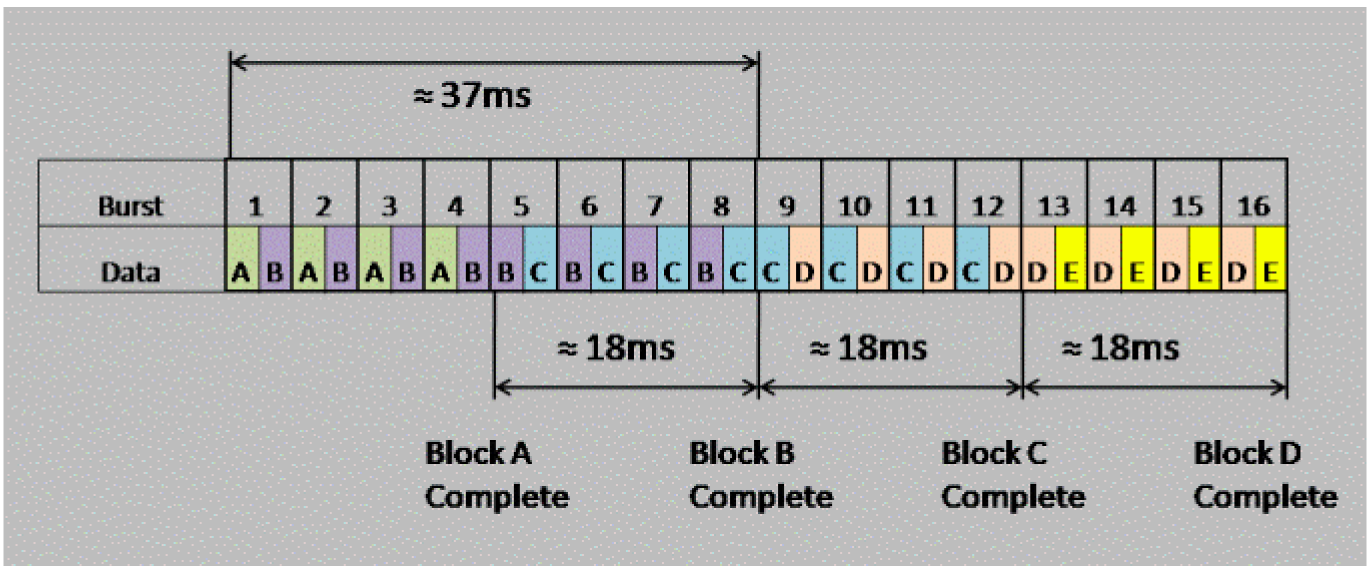
The process of interleaving effectively distributes a single 456 bit audio block over 8 separate bursts. If one burst is lost, only 1/8 of the data is lost, and the missing bits can be recovered using the convolutional code.

Now, you might notice that the data it takes to represent a 20ms (456-bits) audio block is spread out across 8 timeslots. If you remember that each TDMA frame is approximately 4.615ms, we can determine that it takes about 37ms to transmit one single 456-bit block. It seems like transmitting 20ms worth of audio over a period of 37ms would not work. However, this is not what is truly happening. If you look at a series of blocks as they are mapped onto time-slots you will notice that one sub-block ends every four time-slots, which is approximately 18ms. The only effect this has is that the audio stream is effectively delayed by 20ms, which is truly negligible.

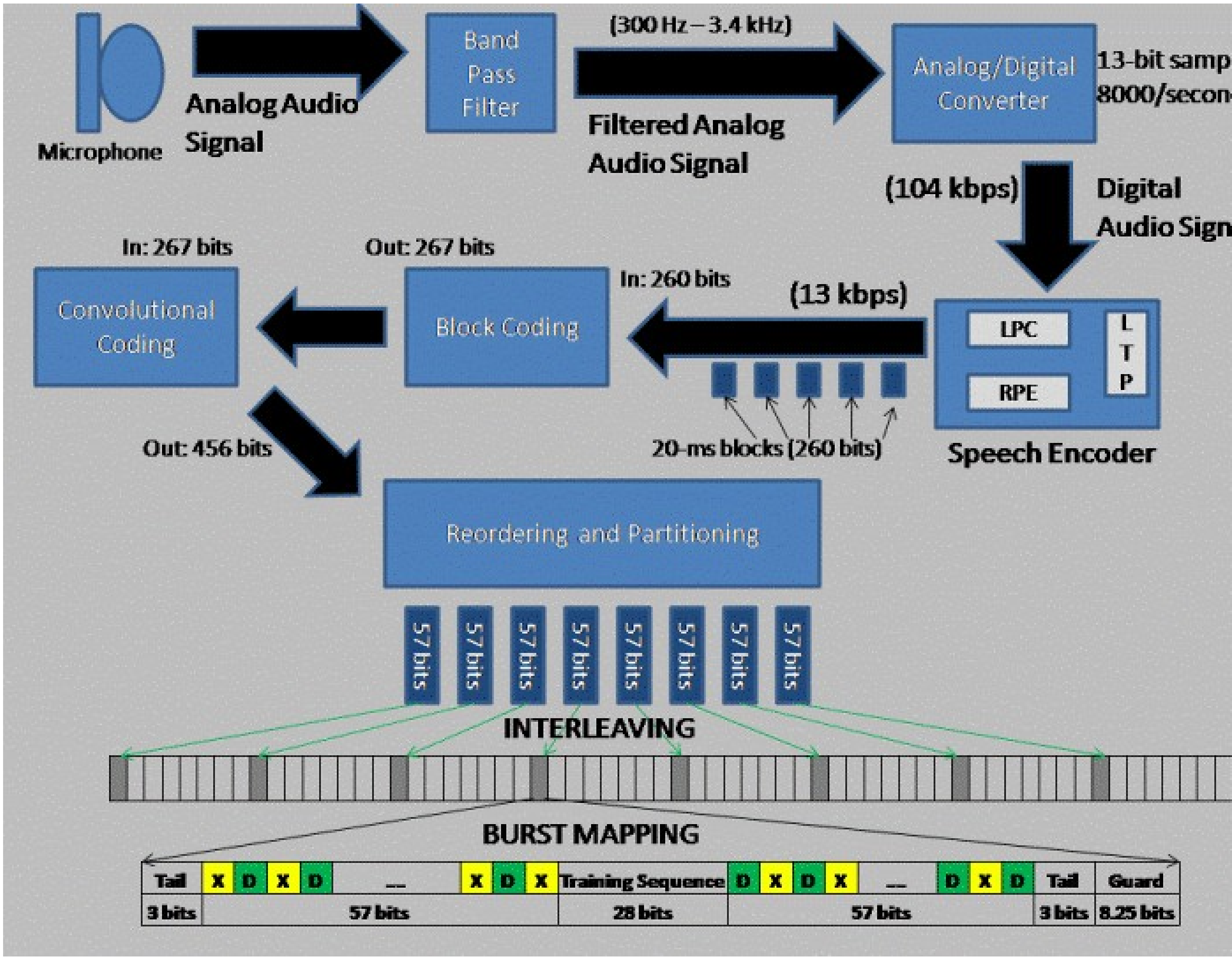
In the diagram below, we can see how this works. The diagram shows 16 bursts. Remember that a burst occurs on a single time-slot and the the duration of a time-slot is 577 µs. Eight time-slots make up a TDMA frame, which is 4.615ms. Since a single resource is only given one time-slot in which to transmit, we only get to transmit once every TDMA frame. Therefore, we only get to transmit one burst every 4.615ms.
* If this is not clear, please review the TDMA Tutorial.

During each time-slot, a burst is transmitted that carries data from two different 456-bit blocks. In the diagram below, Burst 1 carries data from A and B, burst 5 has B and C, burst 9 has C and D, etc. Looking at the diagram, we can see that it does take approximately 37ms for Block B to transmit all of its data, (bursts 1-8). However, in bursts 5-8, data from block C is also being transmitted. Once block B has finished transmitting all of its data (burst 8), block C has already transmitted half of its data and only requires 4 more bursts to complete its data.

Block A completes transmitting its data at the end of the fourth burst. Block B finishes in the eighth, block C, in the 12th, and block D in the 16th. Viewing it this way shows us that every fourth burst comepletes the data for one block, which takes approximately 18ms.



The following diagram illustrates the entire process, from audio sampling to partitioning and interleaving.



Data and signalling messages will be covered in a future tutorial.

[Analog/Digital Conversion](#) [Speech Coding](#) [Block Coding](#) [Convolutional Coding](#) [Reordering & Partioning](#)

[Introduction](#) [Architecture](#) [TDMA](#) [Logical Channels](#) [Authentication & Encryption](#) [Timing Advances](#) [Speech Encoding](#) [GSM Events](#) [Updates](#) [Bulletin Board](#) [Sitemap](#) [Contact Me](#)

[Home](#)

sd