**GSM**

Table of Contents

[Chapter 2 – GSM Network Structure 3](#_Toc63693109)

[Mobile Stations 3](#_Toc63693110)

[Base Transceiver Stations 4](#_Toc63693111)

[Base Station Controllers 4](#_Toc63693112)

[Mobile Switching Centres 4](#_Toc63693113)

[General Architecture 5](#_Toc63693114)

[Authentication Process 6](#_Toc63693115)

[Chapter 4: Radio Coverage 9](#_Toc63693116)

[Spectrum Allocation 9](#_Toc63693117)

[Frequency Reuse 11](#_Toc63693118)

[Chapter 5: Radio Problems and Digital Information 12](#_Toc63693119)

[GSM Transmission Process 12](#_Toc63693120)

[Chapter 6: Air Interference 18](#_Toc63693121)

[Physical Channels 18](#_Toc63693122)

[Logical Channels 18](#_Toc63693123)

[Chapter 7: Traffic Cases 23](#_Toc63693124)

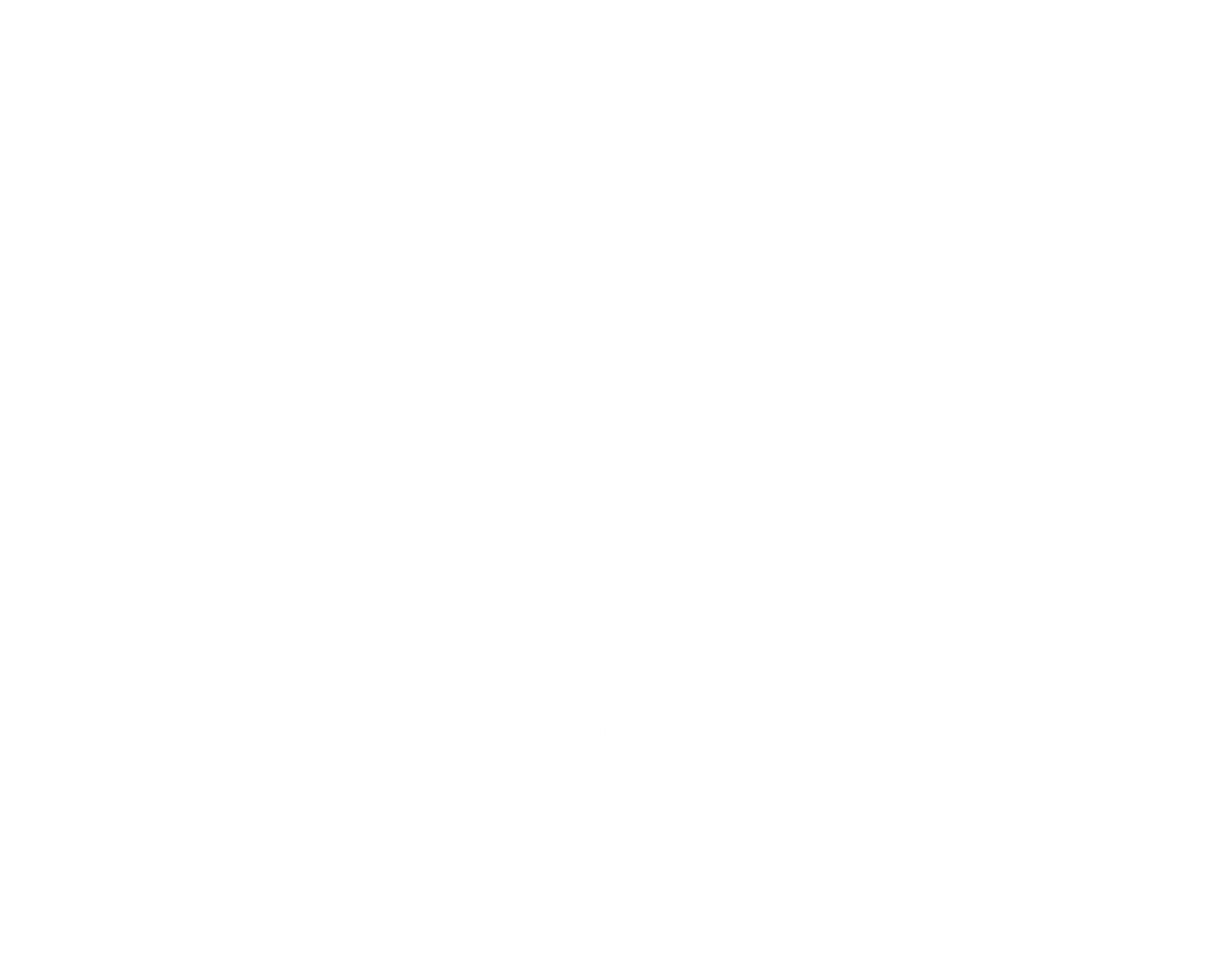
[Location Updates 23](#_Toc63693125)

[Handover 26](#_Toc63693126)

[Call from an MST 29](#_Toc63693127)

[Calls to an MST 30](#_Toc63693128)

## Chapter 2 – GSM Network Structure



The only interaction end users (also called mobile stations (MST)) have with a cellular network is with the base transceiver station (BTS). Several BTS towers are in turn controlled by a base station controller (BSC). Those in turn communicate with a mobile switching centre (MSC).

### Mobile Stations

An MST refers to any mobile device that has a Subscriber Identity Module (SIM) card. The SIM card contains a processor and memory that stores the International Mobile Subscriber Identity (IMSI) and the authentication and ciphering keys.

### Base Transceiver Stations

A BTS consists of the radio transmitters, receivers and the antenna system required to provide coverage to a particular cell. It converts the GSM radio signals into a format that can be understood by the BSC. It also records and passes the signal strength measurements to the BSC. Ciphering and encryption on the network end is also performed by the BTS.

### Base Station Controllers

A BSC manages the radio communication with the mobile stations over the air. It controls the handover of calls in progress between different BTSs and supervises the transmission network and operation of each BTS.

### Mobile Switching Centres

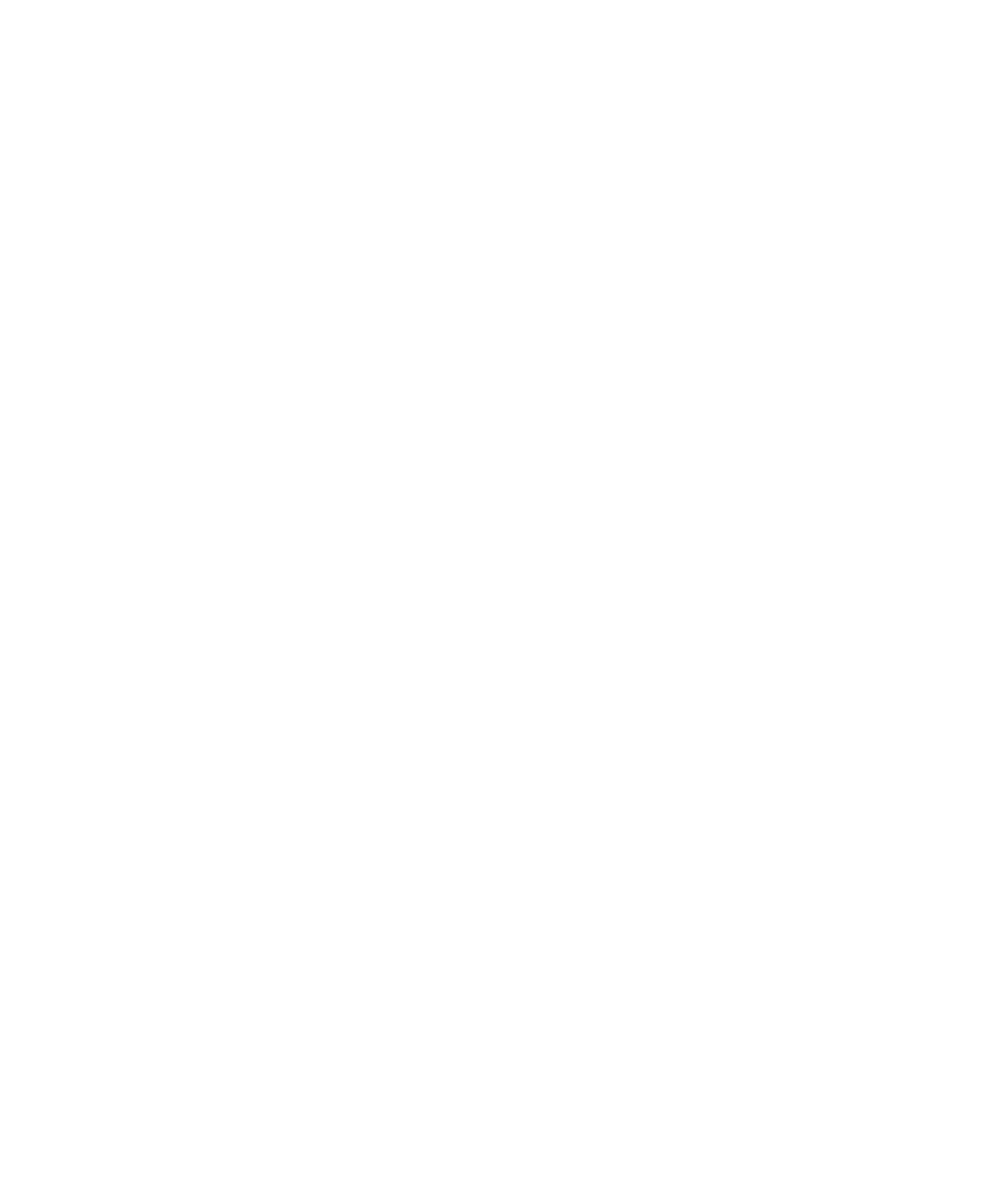
An MSC is in charge of administering the BSCs under its control. It switches calls to and from different subscribers, records charging and accounting details and provides gateways to other networks.

The MSC is supported by three major databases:

* **Home Location Register (HLR)** – This database contains the data of all the users of the network provider, such as what service they are using, their location, authentication data etc.
* **Visitor Location Register (VLR)** – This database holds a partial copy of the data of just the users served by a specific MSC, as well as any data for roaming users, i.e. users from other networks who are using roaming services.
* **Authentication Centre (AUC)** – This provides authentication services in order to verify that all users requesting services are valid users, as well as encryption services to encrypt user data.

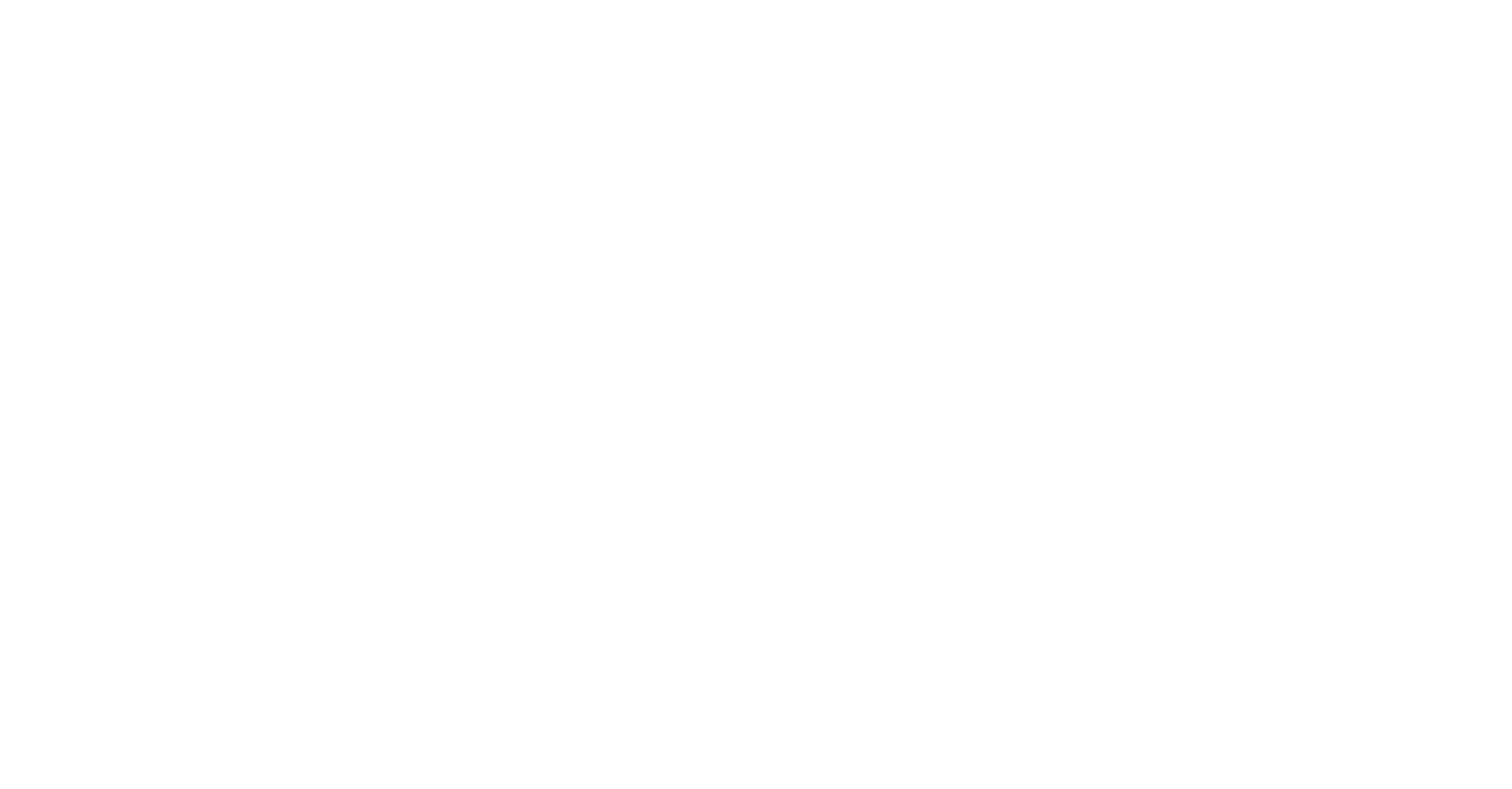
MSCs are in turn connected to other switching nodes, including other MSCs, through public networks like PSTN and ISDN.

### General Architecture



The diagram above shows the same configuration of the Global System for Mobile Communications (GSM) network structure. It shows that MSTs, BTSs and BSCs can be put into one subgroup, called the Base Station Subsystem, MSCs and their support databases can be put into another subgroup, called the Network Switching Subsystem, and the public networks are a third subgroup. There is another subgroup called the Operation Support Subsystem (OSS), which is essentially in charge of monitoring the network to help diagnose and troubleshoot problems.

Between each subsystem, there is an interface.

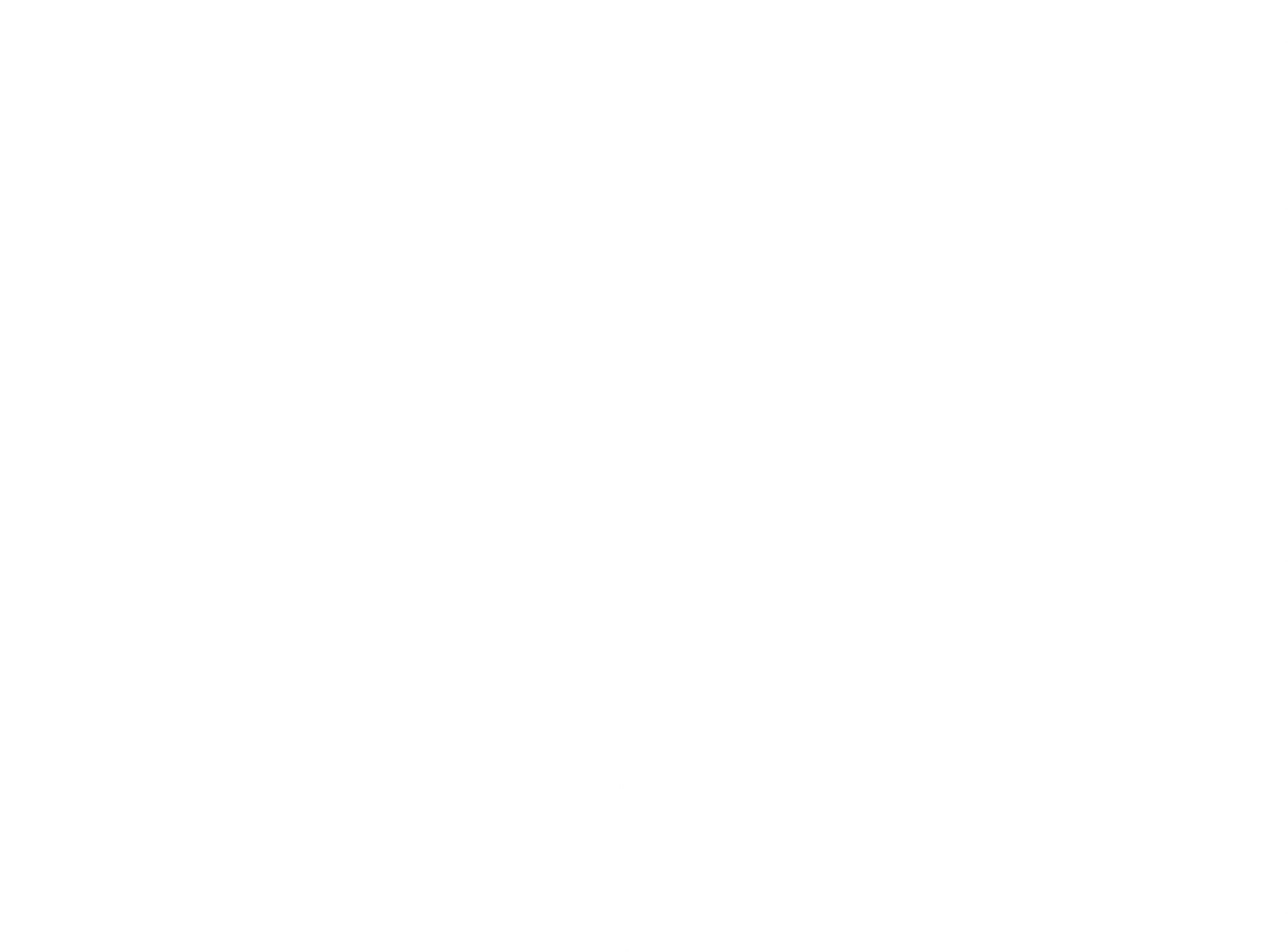


### Authentication Process

Any encryption or decryption algorithm requires two things, a key and some data. An encryption algorithm would take plain text and use the key to produce some cipher text while a decryption algorithm would do the opposite.

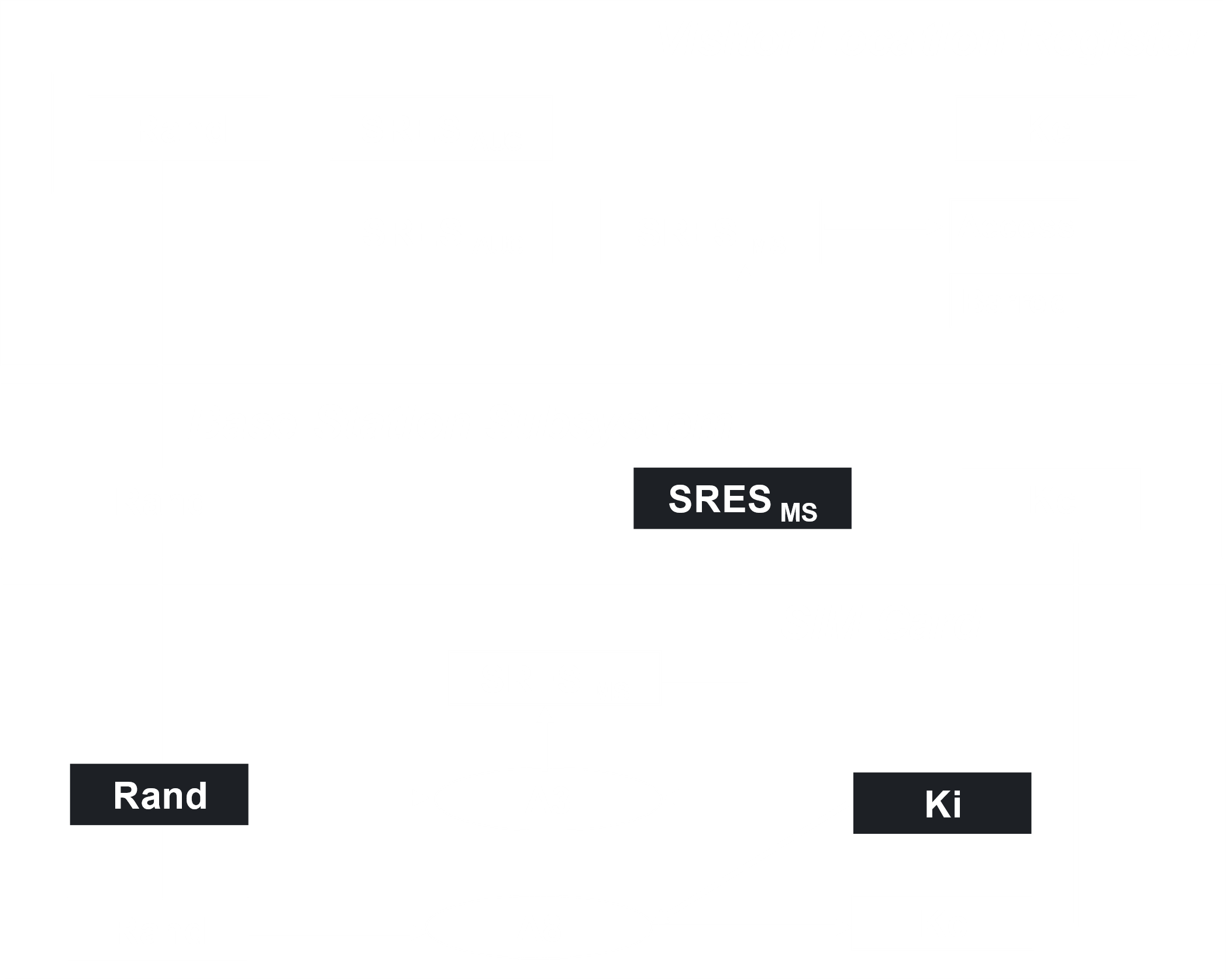
Encryption and decryption algorithms can be of two types. If a single key is used to encrypt and decrypt the data, such algorithms are called Symmetric Key or Shared Key or Private Key Cryptography algorithms. The most common Symmetric Key Cryptography algorithm is Caesar’s Cipher. If different keys are used to encrypt and decrypt the data, such algorithms are called Asymmetric or Public Key Cryptography.

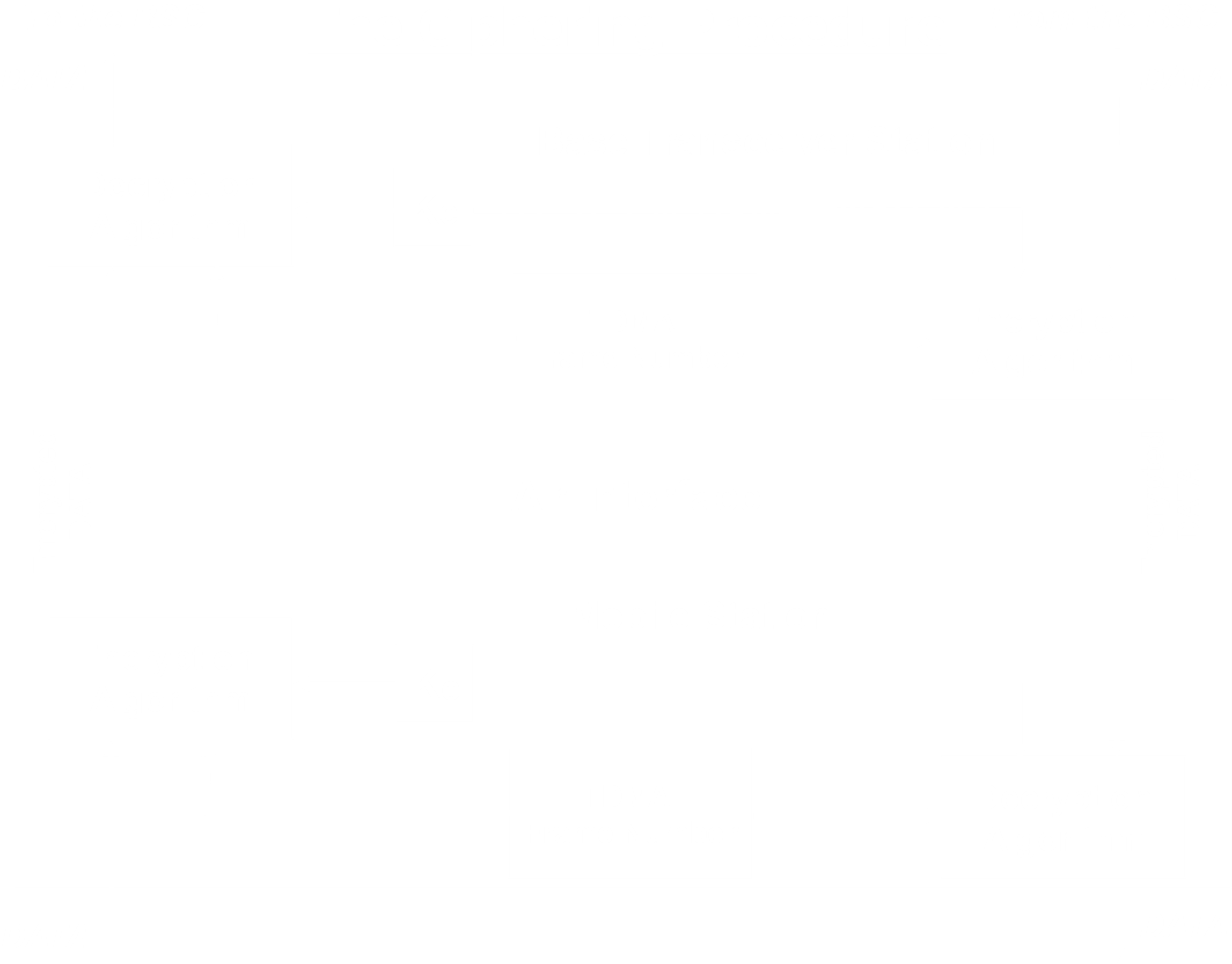
In GSM, encryption and decryption is handled by algorithms called A5 and A8 while authentication is handled by an algorithm called A3. We do not need to know the details of these algorithms for now.



When a user wants access to the network, the VLR produces a random number, which the BST sends to the user. Every SIM card has a key. On the MST, the random number and the key from the SIM is used by the A3 algorithm to produce a Short Response (SRES). This SRES is sent to the BST, which forwards it to the VLR. The VLR already has an SRES for the user, and it matches the new SRES with this value. If they match, the user is granted access.

Next, the same random number that was originally sent is used along with the same key from the SIM card, this time by the A8 algorithm. This algorithm generates a new key, . This key is used to encrypt the user’s data during communication.

’



In the last diagram, there is an extra object called the TDMA Frame Number. This provides an extra layer of security. Again, we will not be getting into the details of this.

## Chapter 4: Radio Coverage

This section mostly covers topics like the need for hexagonal cells and details about frequency reuse. We have already discussed all of that, so we will be skipping over those parts. The only thing we need to cover here is Spectrum Allocation.

### Spectrum Allocation

The original GSM was called GSM 900, because each BST was allocated frequencies in the range. More specifically, the range from to was used as an uplink, and the range from to was used as a downlink. Thus, there were each for the uplink and downlink.

Every channel was allocated , so there could be channels in total. There also needed to be some guard bands, so in reality only channels could be used. This is called the Absolute Radio Frequency Channel Number (ARFCN).

These channels are essentially under frequency division. Additionally, each channel also underwent time division, with users using a channel. Thus, the spectrum could handle users simultaneously. If we take into consideration that some channels were control channels, then this number will go down.

Every channel used the same cell from the uplink and downlink, meaning a channel that used a range starting at as its uplink would use the range starting at as its downlink. In this way, every channel had a constant difference in frequency. For GSM 900, this difference is (. This is called the duplex distance.

Overtime, this capacity of GSM 900 became insufficient, so GSM 1800 was introduced. This has an uplink range from to and a downlink range from to . Thus, both the uplink and the downlink are of each, and the duplex distance is .

There are a few other versions of GSM that use different uplink and downlink frequencies and different duplex distances, but they all use the same carrier separation. Thus, the size of the uplink and downlink determines how many channels are supported by each.

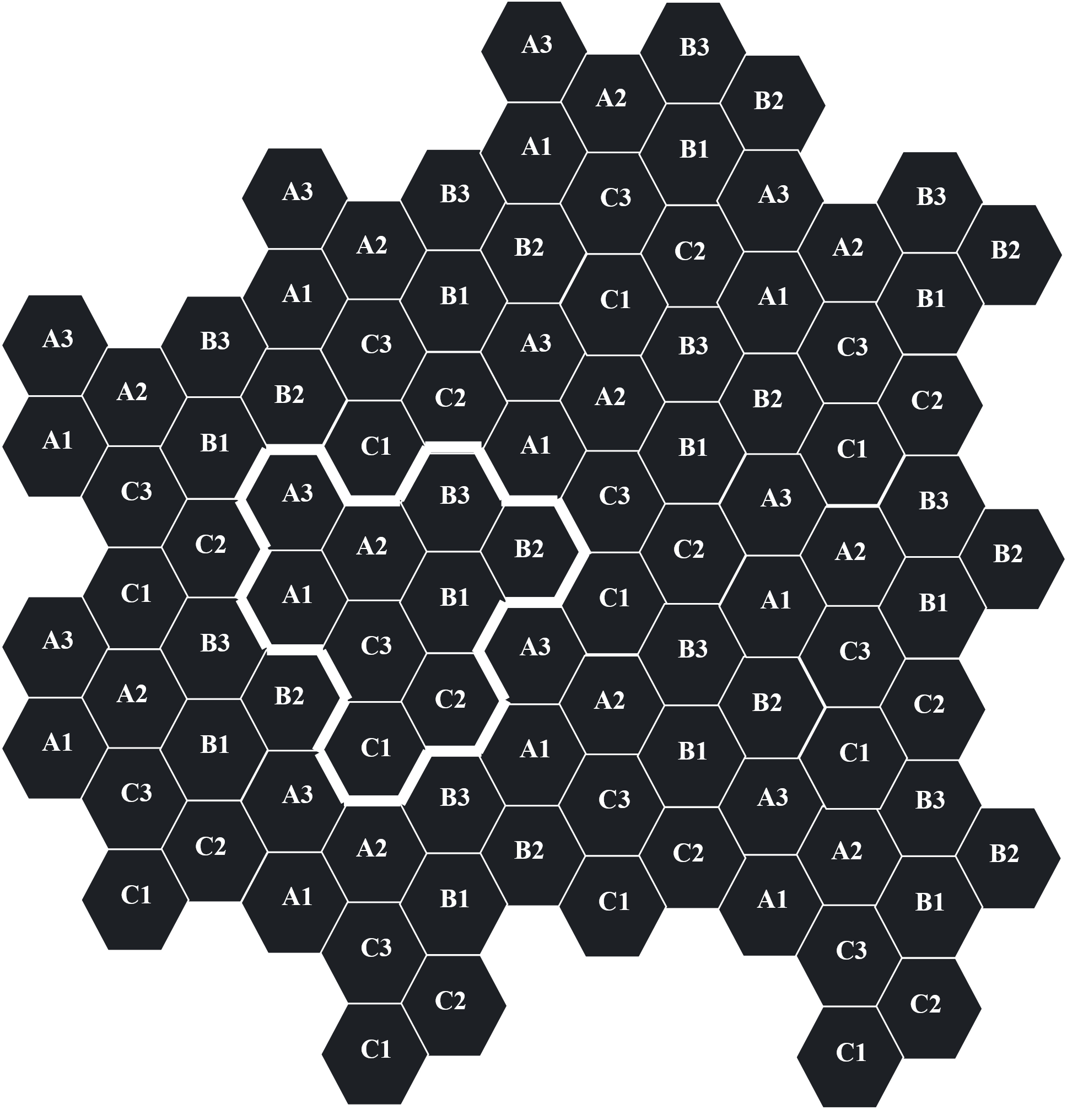
|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| System | | GSM 800 | P-GSM 900 | E-GSM 900 | GSM 1800 | GSM 1900 |
| Frequencies | |  |  |  |  |  |
|  | Uplink |  |  |  |  |  |
|  | Downlink |  |  |  |  |  |
| Wavelength | |  |  |  |  |  |
| Bandwidth | |  |  |  |  |  |
| Duplex Distance | |  |  |  |  |  |
| Carrier Separation | |  |  |  |  |  |
| Radio Channels | |  |  |  |  |  |
| Transmission Rate | |  |  |  |  |  |

Depending on the number of users we need to support in a cell, we can decide which version of GSM we should use. Ones that use larger bandwidths are more costly to obtain and to maintain, so it would be unwise to get unnecessarily large ones.

### Frequency Reuse

We have already discussed frequency reuse thoroughly, so we will not be going into details again here. One thing that is slightly different in GSM is how clusters are divided. There are a few different forms.

Firstly, consider the image below:



This is called a 3/9 cluster, where the available frequencies are divided into 9 cells, and the 9 cells are in turns divided into 3 ‘sites’. We will not be discussing what sites are here.

Similarly, we can have 4/12 clusters, where 12 cells form a cluster and they are divided into 4 sites, or 7/21 clusters, where 21 cells form a cluster and they are divided into 7 sites.

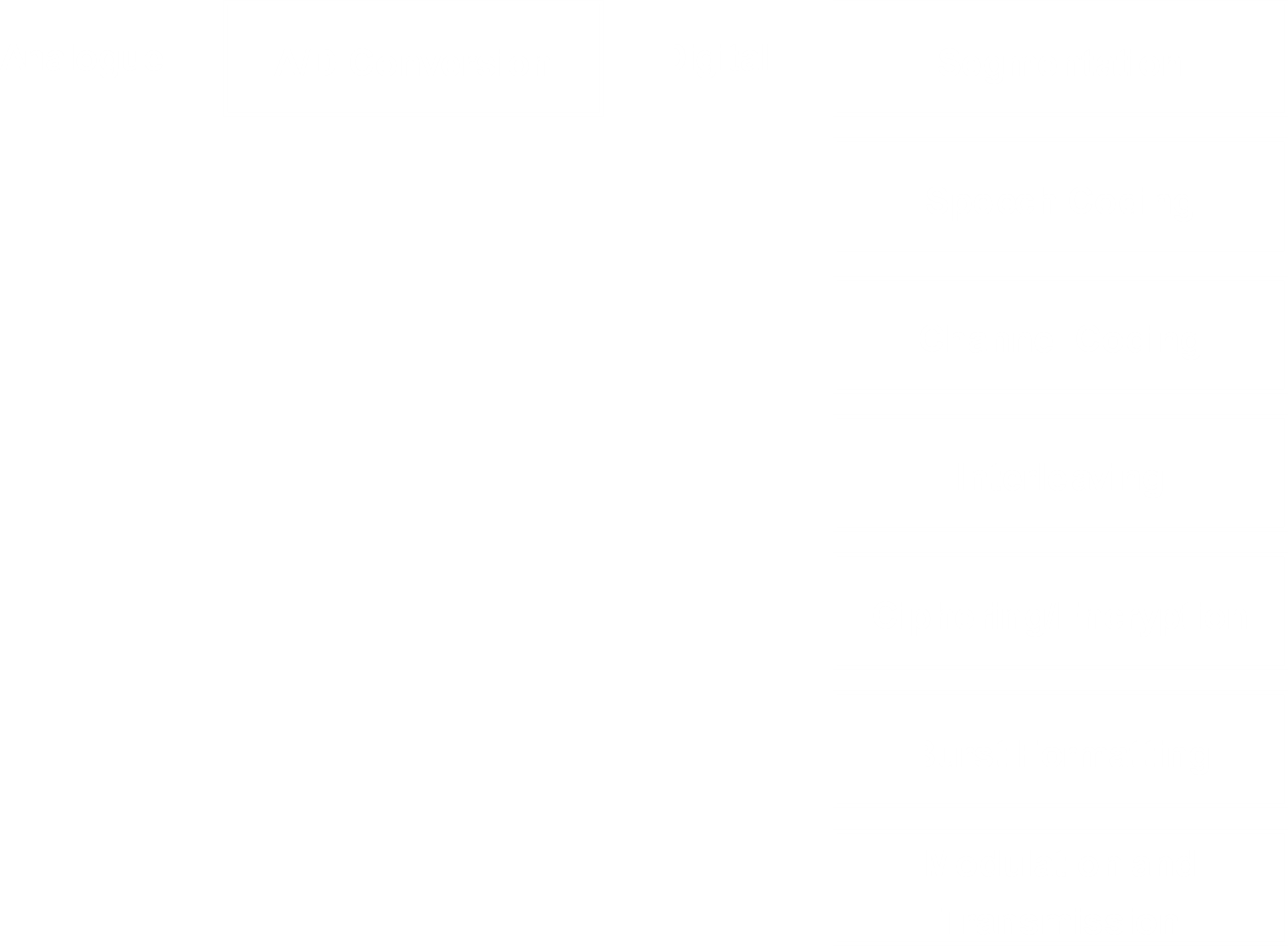
Of course, if we have more cells per cluster, there will be less reuse, which means capacity decreases. However, there is also less interference. Thus, we need to balance these factors.

## Chapter 5: Radio Problems and Digital Information

The first topic under this section is about fading. Fading is essentially the process in which signals get reflected, refracted or diffracted due to obstacles in the environment, which in turn causes interference issues. There are many details about these problems and how to solve them, but we will be skipping over all of that for now.

Instead, we will be looking into another topic from this section, which looks at how GSM processes and transmits signals, GSM Transmission Process.

### GSM Transmission Process



The entire process is outlined above.

#### Analogue to Digital Conversion

The first thing that happens is the analogue signal of the human voice is converted to a digital signal using Analogue to Digital conversion. We have already looked into details about how this works, using Pulse Code Modulation (PCM).

#### Segmentation

The second step is segmentation. We essentially take partitions of the signal and take samples from it. Keep in mind that this is different from the process that occurred in PCM. In PCM, we took samples of analogue data. Each sample had bits of data. The result of the PCM process was some digital data. This digital data is again being sampled by the segmentation process. This time, we take samples every , which forms a single segment.

#### Speech Coding

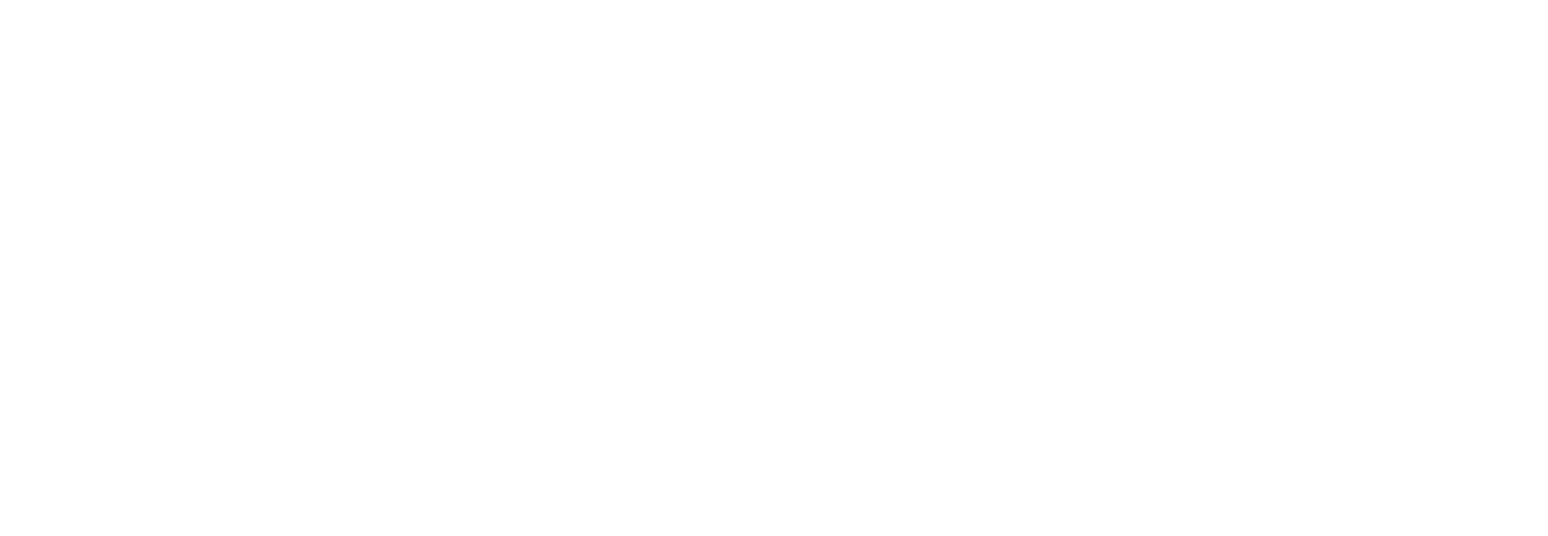
The speech coder will in turn take the segments, and for each segment, it will generate bits of data. Thus, the data rate is . This is the acceptable speech quality in mobile telephony.

#### Channel Coding

The bits of data is then given to the channel coder. The channel coder divides the data into three parts:

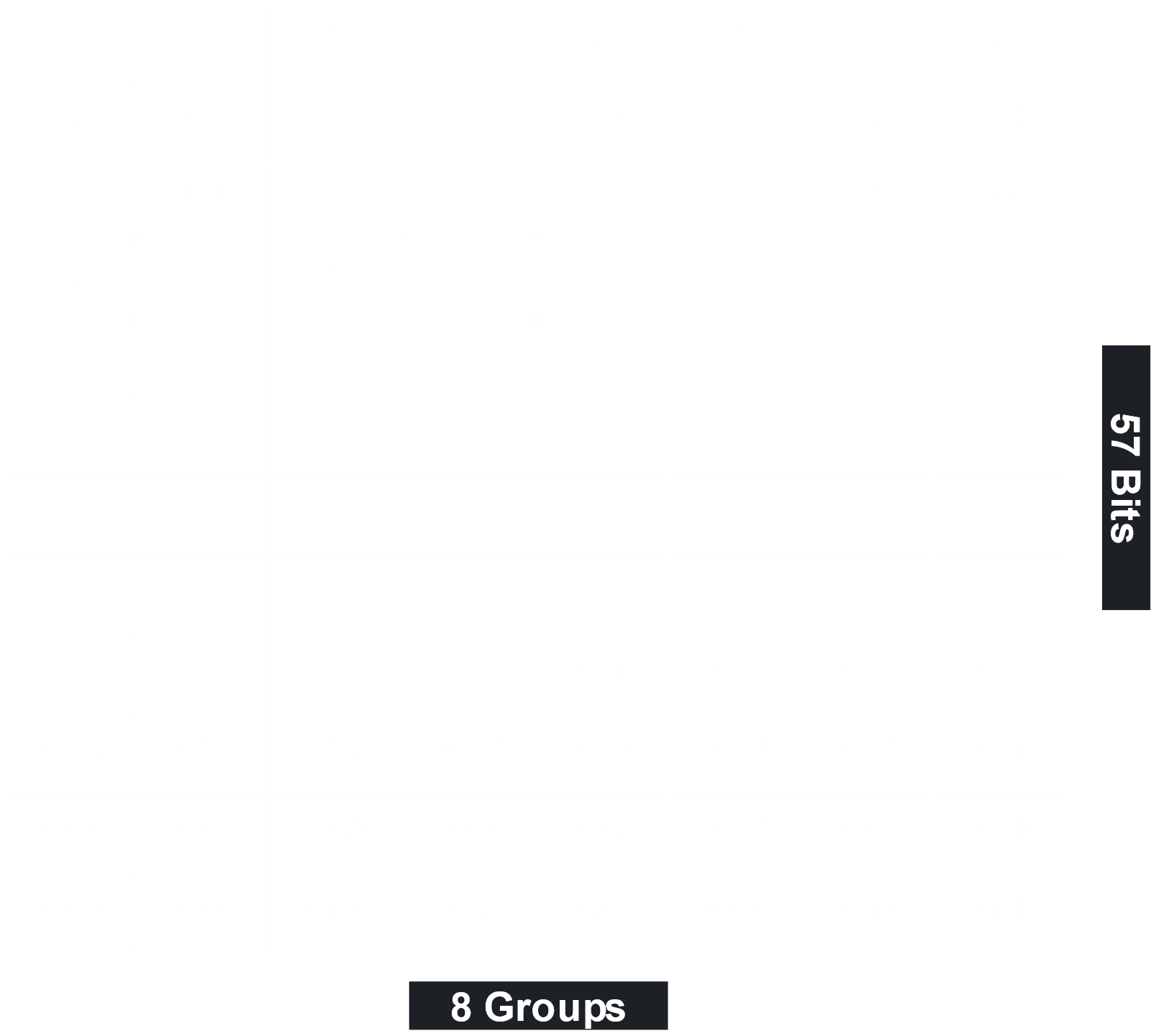
* bits that are very important
* bits that are important
* bits that are not so important

The channel coder puts the very important bits into a block coder, where bits are added. This, along with the important bits and other tail bits are taken to a Convolutional Coder, which adds redundant bits to double the number of bits. Thus, we have bits. This, along with the not so important bits is the output of the channel coder, which is of bits.



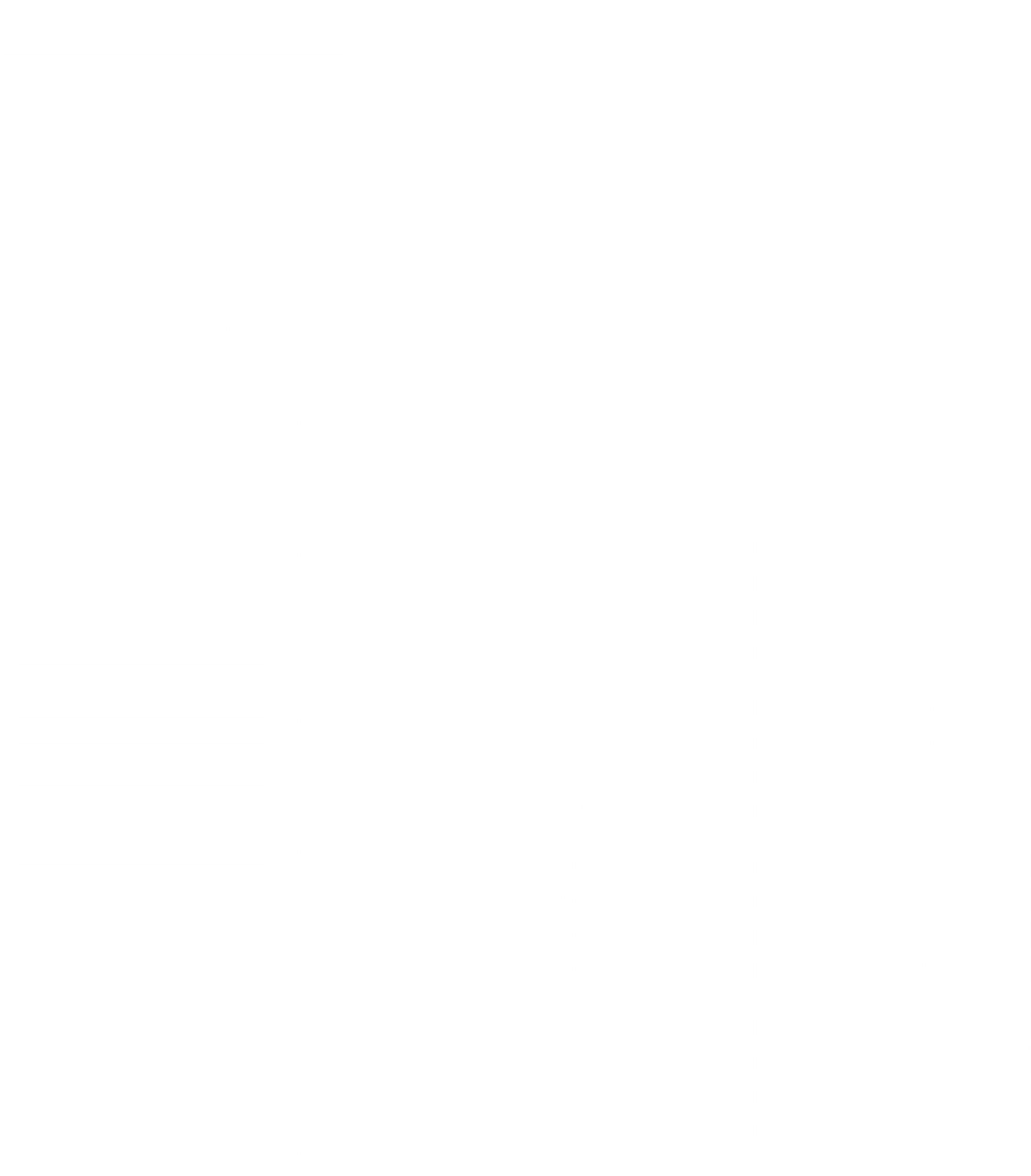
#### Interleaving

Next, the interleaving stage. Instead of sending data consecutively, we divide them into groups and send the groups instead. Essentially, the bits are divided into rows of bits each, and instead of sending the data row by row, we send it column by column.

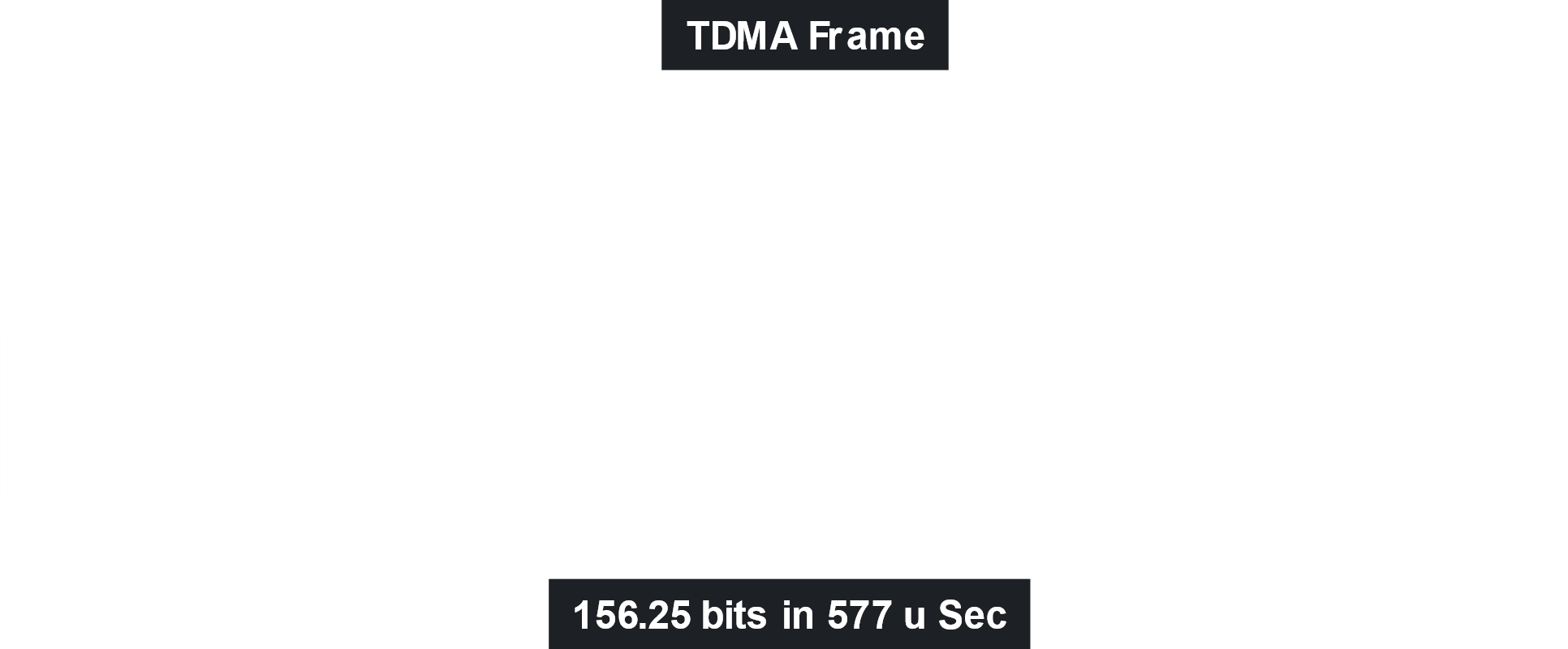


The first group consists of the 1st bit, the 9th bit, the 17th bit and so on. In this way, we are not sending consecutive data at the same time. Even if we lose an entire column, we will not have lost consecutive data and we can make up for it. This is better than losing bits of consecutive data. Think of this like losing in every of a audio clip, as opposed to losing consecutively, which would be a much more noticeable problem.

The above process is first level interleaving. We also have second level interleaving after this. Notice that in first level interleaving, there are groups. We take segments, with a total of groups, and mix these together. The bits in groups from a single segment is placed in a frame along with bits from group from another segment.



Notice how the frames are set up. The bits from each group have a space between them, marked . This space contains the training sequency bits. This has to do with how frames are set up later on in the process.



The two groups of bits are separated by bits of training sequence, which are used for control and error detection and correction purposes. There is bit as a guard bit between the training sequence and each of the groups of user data. Additionally, there are tail bits on either end. This makes up a single frame.

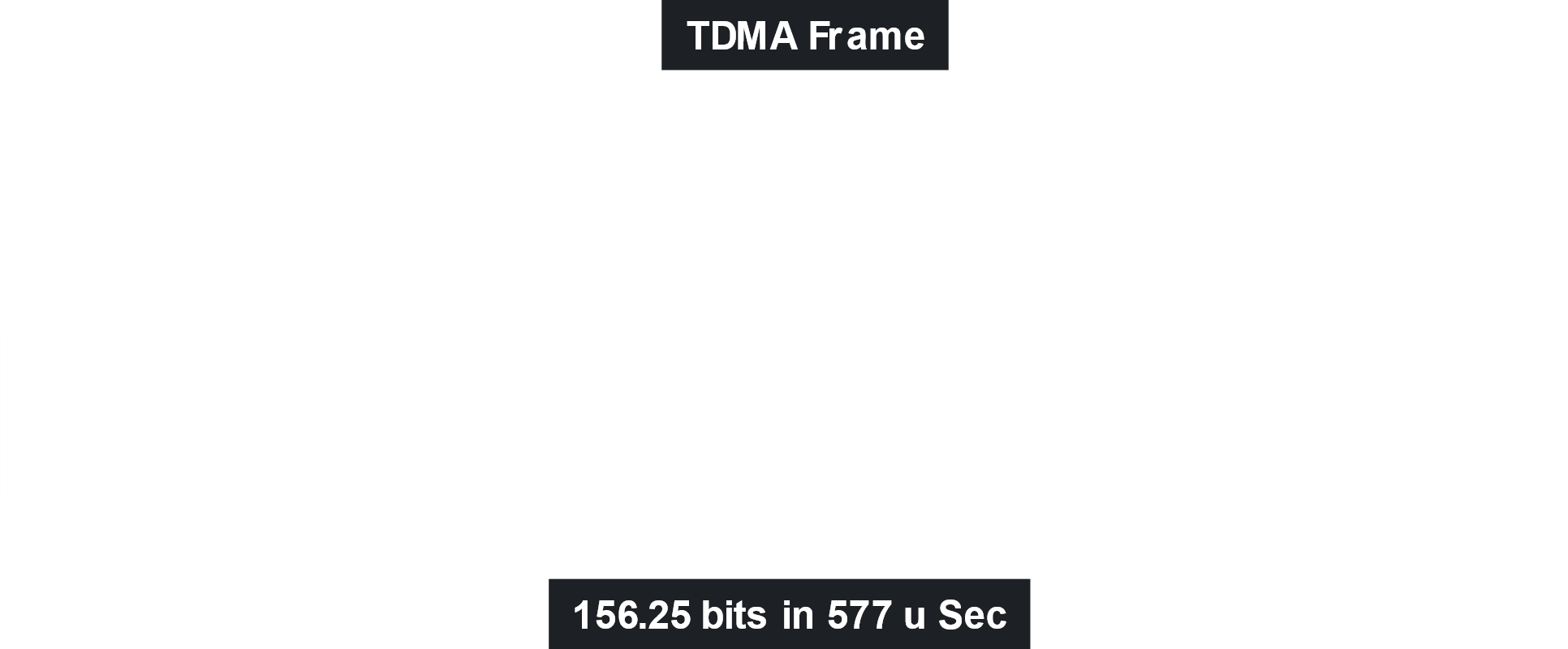
This frame creation is something we will look into more detail later on.

#### Ciphering and Encryption

We will not be looking into details about how data is encrypted. All we need to know is that the Ciphering and Encryption process uses the A5 algorithm. It does not add any extra data. The output is still of bits.

#### Burst Formatting

This is the stage where the frame we saw earlier is actually formed. The bits of encrypted data from a single segment are taken and bits extra are added for control purposes. This brings the total to bits. These bits will be sent in four ‘bursts’, or frames, each containing sets of bit encrypted user data, and other bits of data, as seen in the frame.



A single burst seemingly has bits, but of course, it is only sending bits. The remaining time in which bits could have been sent is left as a guard period. During this time, the MST ramps up and down, meaning it either gets power from the battery to send data or lets go of power to ensure it does not transmit during time slots dedicated to other users. GSM frames undergo time division, so the bits were for just one user of the frame. There can be users per frame.

## Chapter 6: Air Interference

### Physical Channels

Physical channels refer to the actual bandwidth allocated to the users. In GSM, the total bandwidth can be divided into groups of , which results in a total of channels. Using TDMA, each of these channels is further divided among users in time slots. These time slots are the physical channels.

### Logical Channels

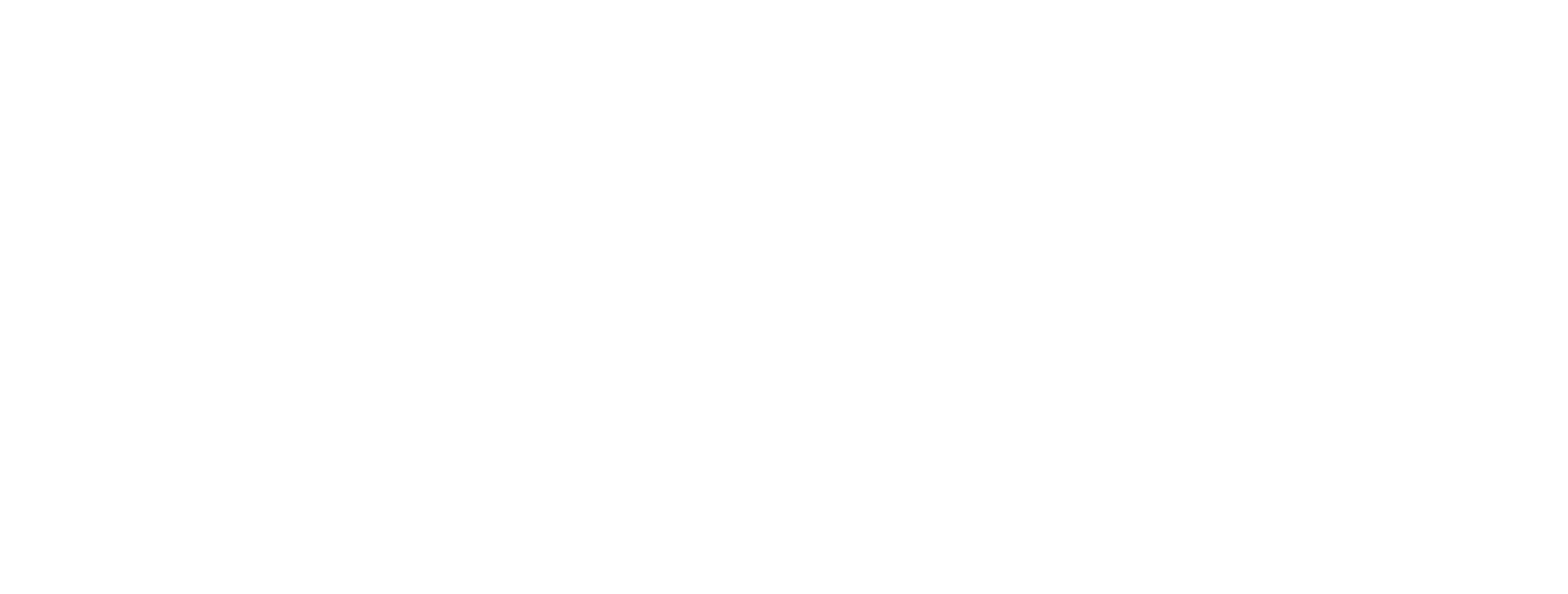
The actual physical channels are occupied by different things at different times. We can have either traffic channels, which carry actual user data, or control channels, which help us manage the network. Both of these are called logical channels.

Control channels can be of many types and are divided into three categories

* Broadcast Channels – These are broadcasted by the BTS tower. They help connect devices to the network.
* Common Channels – These channels are used by end users when making a call, for example to request the BTS to assign a traffic channel to them.
* Dedicated Channels – These channels are what are used to actually establish the call. When a user makes a request using a common channel, another common channel is used to respond. The response sent is a dedicated channel, which will allow the user to make the call.

Keep in mind that the above categories are generalizations of the channels. We will be learning the details of the different types of channels in each category shortly.

The breakdown for the different types of logical channels is given below:



#### Traffic Channels

The only thing we need to know about traffic channels is that they are used to actually send and receive the user data during a call. A full rate traffic channel has a data rate of and a half rate traffic channel has a data rate of .

#### Broadcast Channels

All the broadcast channels are downlink channels, meaning data comes from the BTS to subscribers. The details of the different channels are outlined below:

|  |  |  |  |
| --- | --- | --- | --- |
| **Broadcast Channels (BCHs)** | | | |
| Logical Channel | Direction | BTS | MS |
| Frequency Correction Channel (FCCH) | Downlink, point to multipoint | Transmits a carrier frequency. | Identifies BCCH carrier by the carrier frequency and synchronizes with the frequency. |
| Synchronization Channel (SCH) | Downlink, point to multipoint | Transmits information about the TDMA frame structure in a cell (e.g. frame number) and the BTS identity (Base Station Identity Code (BSIC)). | Synchronizes with the frame structure within a particular cell, and ensures that the chosen BTS is a GSM BTS - BSIC can only be decoded by an MS if the BTS belongs to a GSM network. |
| Broadcast Control Channel (BCCH) | Downlink, point to multipoint | Broadcasts some general cell information such as:   * Location Area Identity (LAl), * maximum output power allowed in the cell and * the identity of BCCH carriers for neighbouring cells. | Receives LAI and will signal to the network as part of the Location Updating procedure if the LAI is different to the one already stored on its SIM. MS sets its output power level based on the information received on the BCCH. The MS stores the list of BCCH carrier frequencies on which Rx level measurement is done for Handover decision. |

#### Common Control Channels

The first common control channel is the Random-Access Channel (RACH). This is an uplink channel used by MSTs to make requests to the BST.

Requests are granted through the second common control channel, the Access Grant Channel (AGCH). Thus, it is a downlink channel.

The last common control channel, the Paging Channel (PCH), is used to locate the MST that must receive the call. This is also a downlink channel. Notice that this means that even if we are not on a call, MSTs are always connected to the network.

The details of the three channels are given below:

|  |  |  |  |
| --- | --- | --- | --- |
| **Common Control Channels (CCCHs)** | | | |
| Logical Channel | Direction | BTS | MS |
| Paging Channel (PCH) | Downlink, point to multipoint | Transmits a paging message to indicate an incoming call or short message. The paging message contains the identity number of the mobile subscriber that the network wishes to contact. | At certain time intervals the MS listens to the PCH. If it identifies its own mobile subscriber identity number on the PCH, it will respond. |
| Random Access Channel (RACH) | Uplink, point to multipoint | Receives access-request from MS for call setup / loc. Update / SMS | Answers paging message on the RACH by requesting a signalling channel. |
| Access Grant Channel (AGCH) | Downlink, point to multipoint | Assigns a signalling channel (SDCCH) to the MS. | Receives signalling channel assignment (SDCCH). |

#### Dedicated Control Channels

When an MST request is granted, a channel is assigned to the MST via the Access Grant Channel, as we saw above. The channel being assigned is a Standalone Dedicated Control Channel (SDCCH). The SDCCH is used to setup the call, so it is both uplink and downlink. Once the call is setup, then the MST switches to a traffic channel.

The Slow Associated Control Channel (SACCH) is used by MSTs to send RSSI values to the BTS.

The Fast Associated Control Channel (FACCH) is used by BTSs during handovers.

The details of the dedicated control channels are given below:

|  |  |  |  |
| --- | --- | --- | --- |
| **Dedicated Control Channels (DCCHs)** | | | |
| Logical Channel | Direction | BTS | MS |
| Standalone Dedicated Control Channel (SDCCH) | Uplink and downlink, point to point | The BTS switches to the assigned SDCCH, used for call set-up signalling. TCH is assigned on SDCCH. (SDCCH is also used for SMS messages to MS). | The MS switches to the assigned SDCCH. Call set-up is performed. The MS receives a TCH assignment information (carrier and time slot). |
| Cell Broadcast Channel (CBCH) | Downlink, point to multipoint, mapped on SDCCH | Uses this logical channel to transmit short message service cell broadcast. | MS receives cell broadcast messages. |
| Slow Associated Control Channel (SACCH) | Uplink and downlink, point to point | Instructs the MS on the allowed transmitter power and parameters for time advance. SAACH is used for SMS during a call. | Sends averaged measurements on its own BTS (signal strength and quality) and neighbouring BTS's (signal strength). The MS continues to use SACCH for this purpose during a call. |
| Fast Associated Control Channel (FACCH) | Uplink and downlink, point to point | Transmits handover information. | Transmits necessary handover information in access burst. |

## Chapter 7: Traffic Cases

Traffic cases deal with how MSTs communicate with the network.

### Location Updates

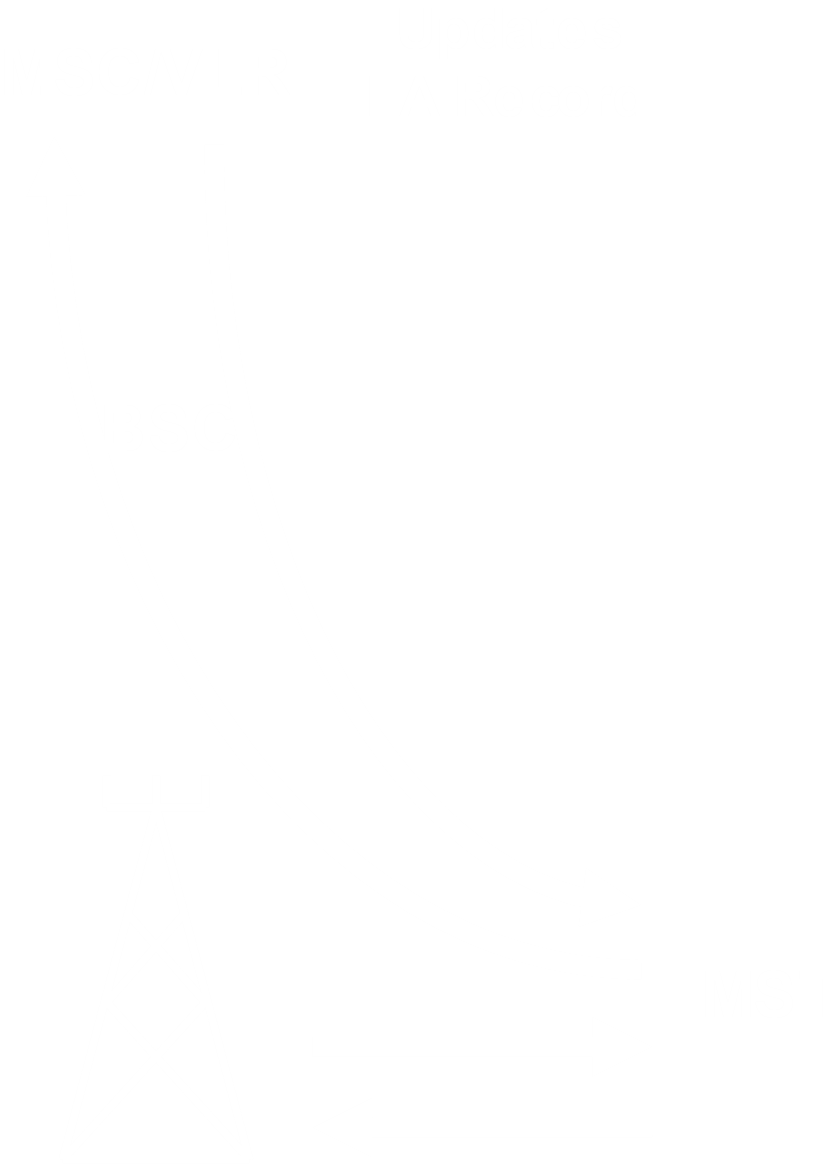
The location update process aims to identify the location of every MST within the network so that incoming calls go directly to them. To fulfil this aim, one approach could be to update the system with the cell ID every time an MST changes their serving cell. However, this will cause a huge number of location update messages. The other extreme would be to never send location update messages, which would mean having to send a paging message to the entire network every time we needed to connect to an MST to send them a call.

In compromise, the coverages area for an MSC is divided into Location Areas (LAs). The MST only updates the network with its location when it changes LAs.

There are four different types of Location Updates:

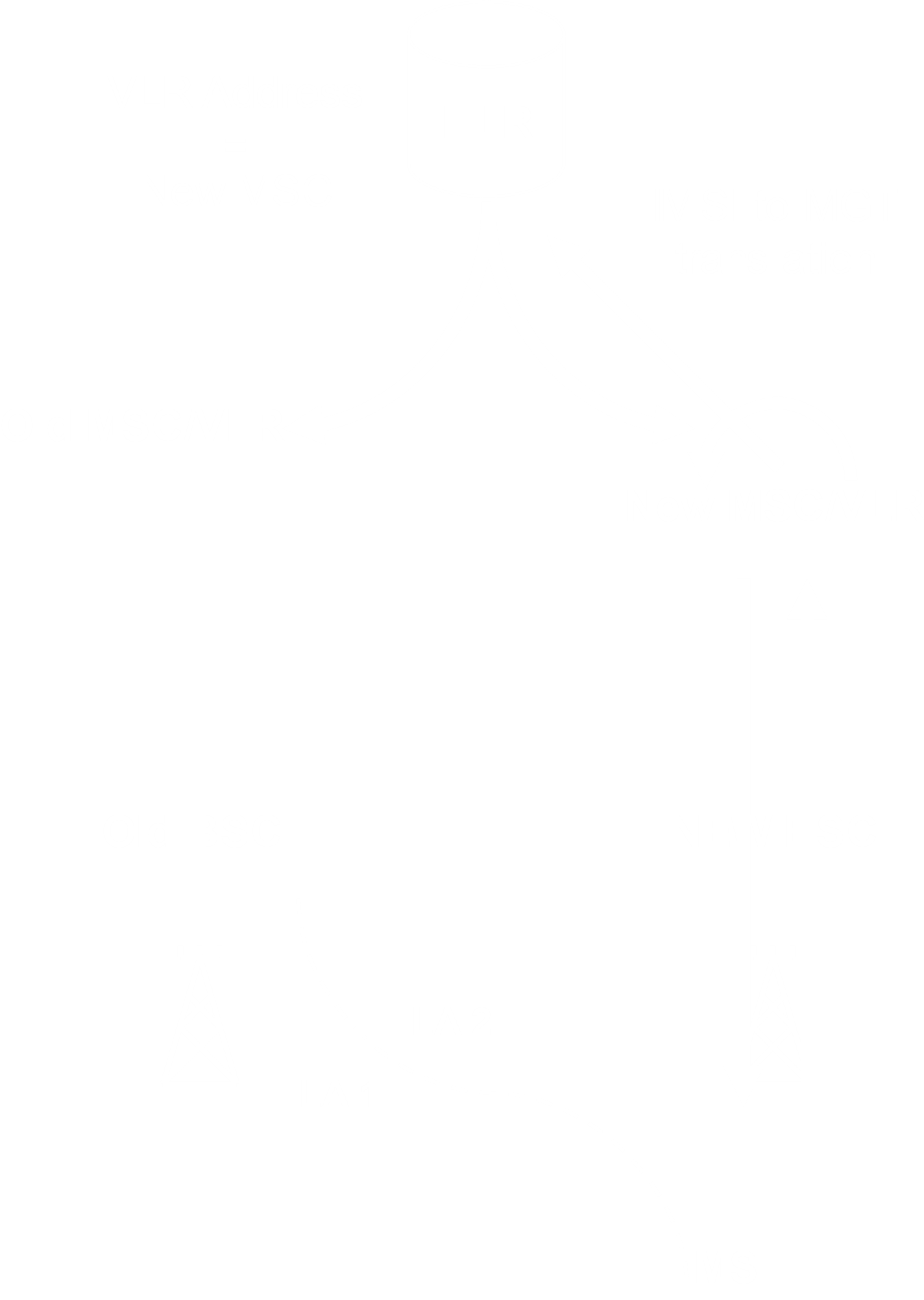
1. Normal Location Update within the same MSC
2. Normal Location Update between different MSCs
3. IMSI Attach/Detach
4. Periodic Location Updates

#### Normal Location Update Within the Same MSC



1. The MST sends an allocation request to the BTS.
2. The BTS responds with an allocation message.
3. The MST sends a location update request along with its International Mobile Subscriber Identity (IMSI) to the MSC.
4. The MSC updates the location information and sends a location update confirmation.

#### Normal Location Update Between Different MSCs



The difference between the last process and this one is that the old MSC must send the location update to the HLR, which sends it to the new MSC. Once this is done, the HLR tells the old MSC to remove the data. The new MSC sends a confirmation to the MST.

#### IMSI Attach/Detach

This process occurs when an MST is powered off or comes back on.

When powering off

1. The MST requests a signalling channel.
2. The MST uses the signalling channel to send an IMSI detach message to the MSC.
3. In the VLR, the IMSI detach flag is set, which rejects incoming calls.

When powering on

1. The MST requests a signalling channel.
2. The MST uses the signalling channel to send an IMSI attach message to the MSC.
3. The MSC sets the IMSI attach flag in the VLR, meaning the mobile can receive calls now.
4. The VLR returns an acknowledgement to the MST.
5. If the MST has changed locations, a normal location update takes place.

#### Periodic Location Update

During a predefined time period, if an MST makes no location updates, the network performs a routine task to check for its location. If there is no response, the MST is marked as detached.

### Handover

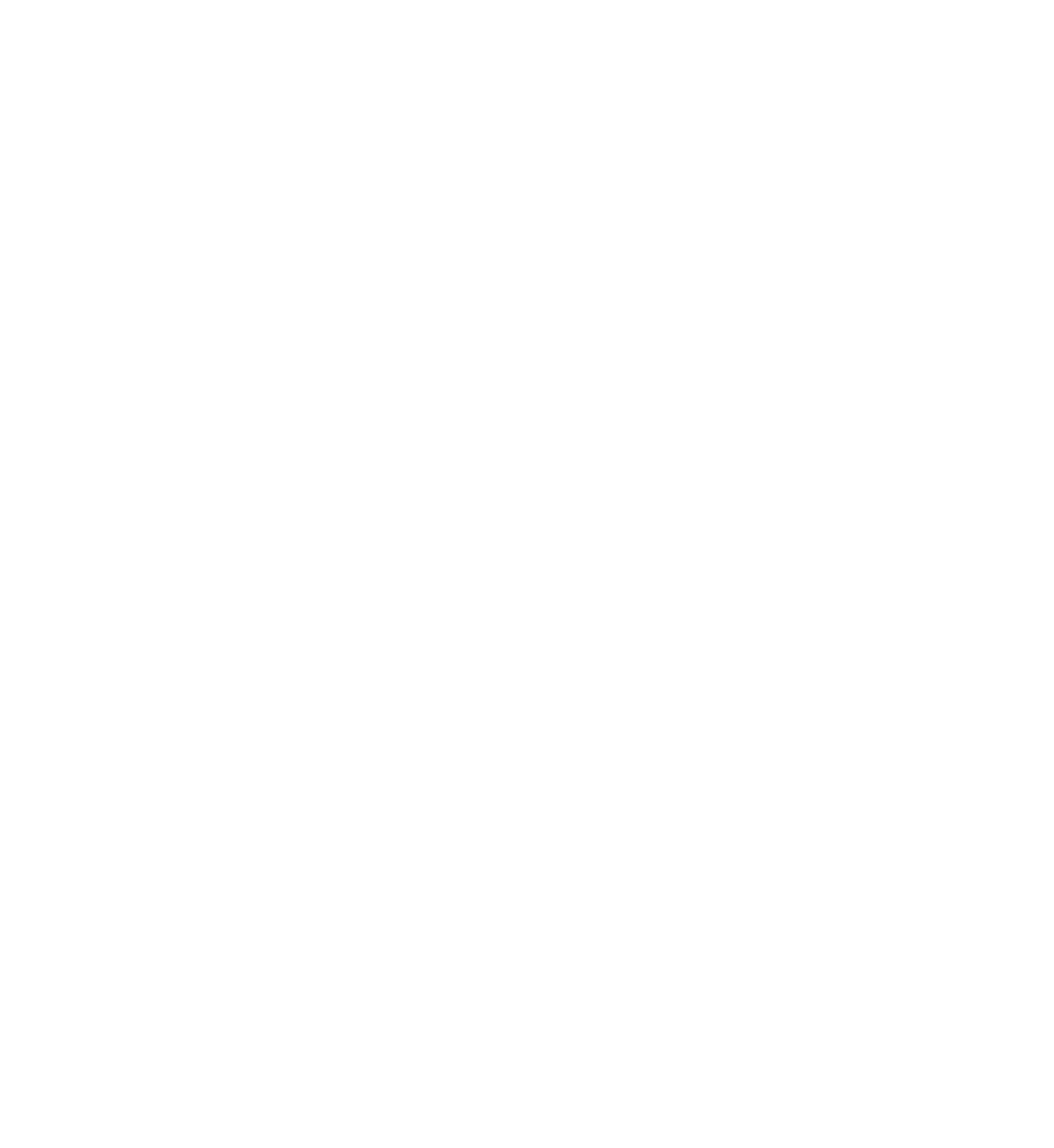
We have already studied in detail about how handovers work, so this will just be a brief overview of some parts we may have missed.

During a call, an MST continuously measures the transmission quality of neighbouring cells and reports these results to the BSC through the BTS. The BSC is responsible for initiating handovers when it feels the current signal strength between the BTS and the MST is too weak.

There are three types of handovers:

1. Intra BSC Handover – This is when the new cell belongs to the same BSC as the old one.
2. Inter BSC / Intra MSC Handover – This is when the new cell belongs to a different BSC, but that BSC belongs to the same MSC.
3. Inter MSC Handover – This is when the new cell belongs to a BSC that is from a different MSC.

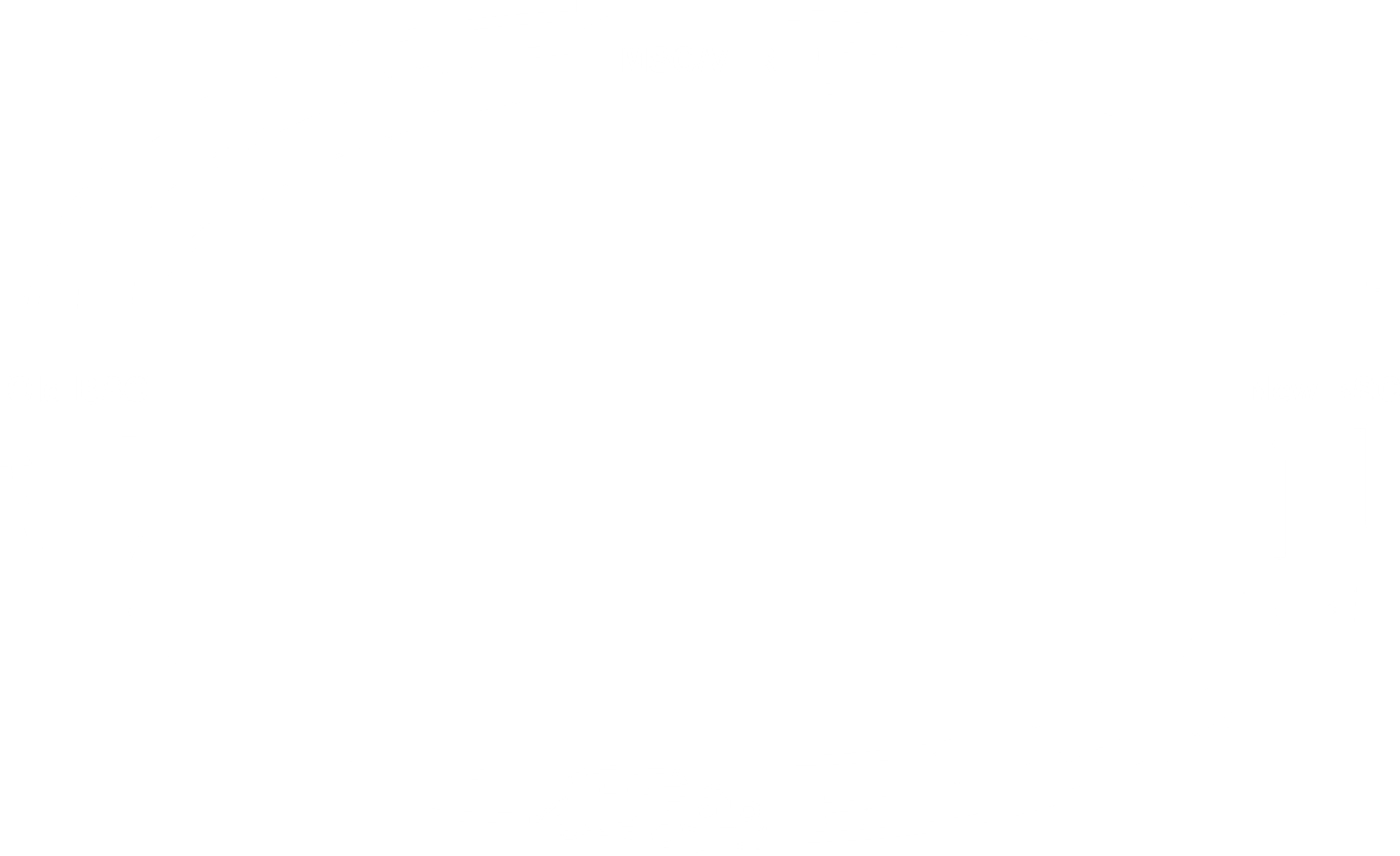
#### Intra BSC Handover



1. The BSC decides that the call must be handed over to a new cell.
2. The BSC finds a vacant traffic channel in the new cell.
3. The BSC sends information about the traffic channel found in the new cell to the current BTS, which forwards it to the MST via the Fast Associated Control Channel (FACCH).
4. The MST requests access to the provided traffic channel from the new BTS.
5. The new BTS grants access to the MST, again via the FACCH.
6. The MST sends a handover complete message to the new BTS.
7. The new BTS sends a handover complete message to the BSC.
8. The BSC orders the old BTS to release its now free traffic channel.

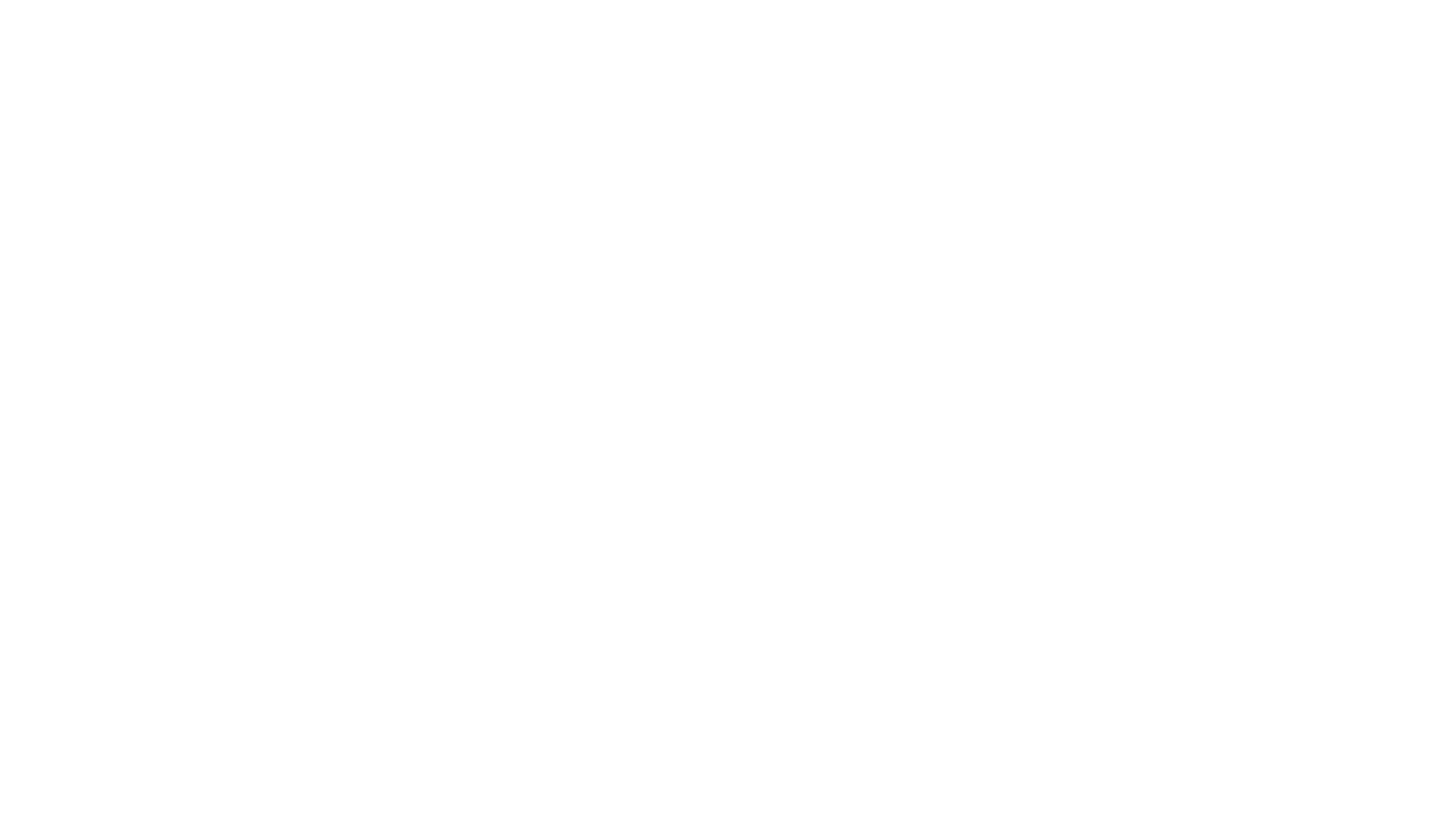
#### Inter BSC / Intra MSC Handover

The only difference between an Inter BSC handover and an Intra BSC handover is that the BSC must send a request to its MSC, which will contact the new BSC. The new BSC will in turn send back information about the new BTS to the MSC, which will forward it to the old BSC. The changes are made, and once it is done, the confirmation about the successful handover must follow the same path, going from the new BSC to the MSC and then the old BSC.

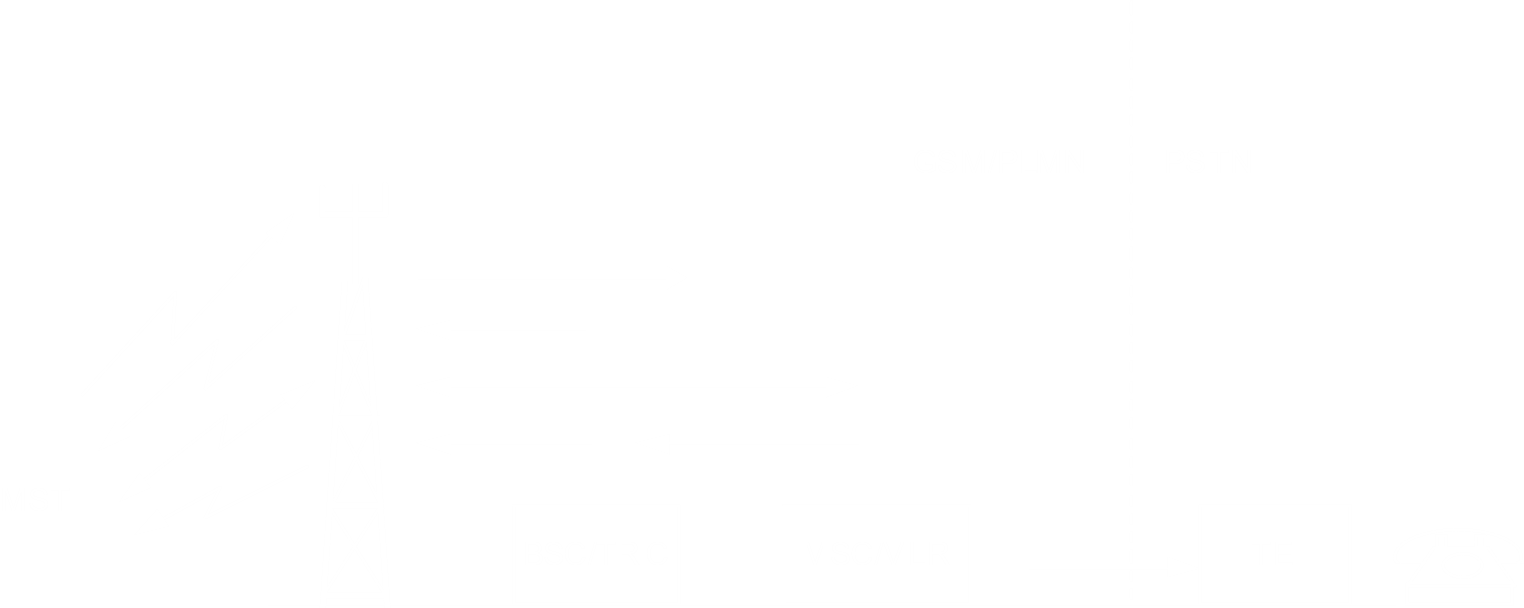


#### Inter MSC Handover

Again, the only difference between an inter MSC handover and the previous processes is that two MSCs must communicate with each other. If the MSCs belong to different network providers, the PSTN might have to get involved.

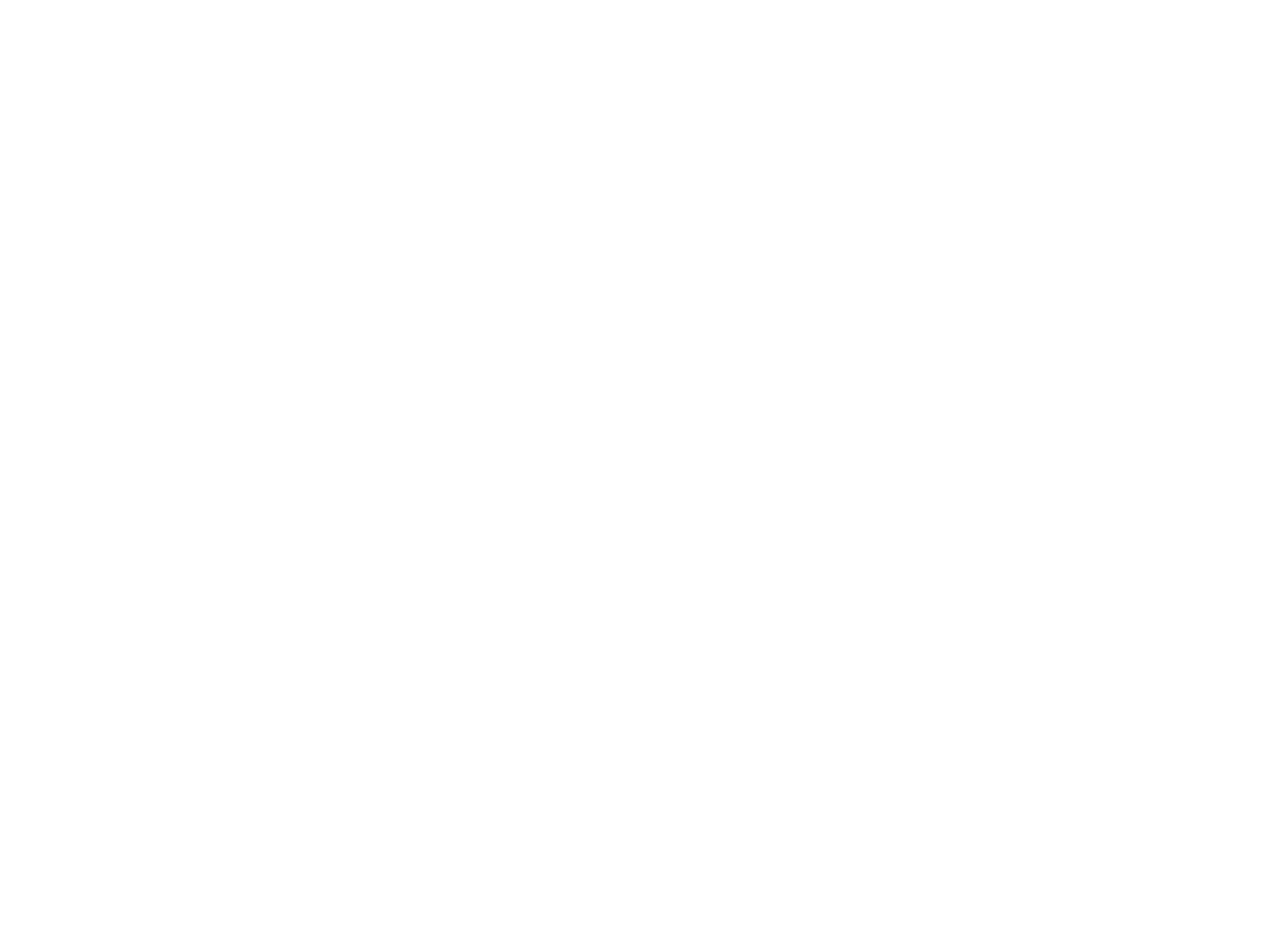


### Call from an MST



1. The MST uses a Random-Access Channel (RACH) to ask for a signalling channel.
2. The BSC allocates a signalling channel using the Access Grant Channel (AGCH).
3. The MST sends a call set up request via the allocated Standalone Dedicated Control Channel (SDCCH) to the MSC. Via the SDCCH,
   1. The MST is marked as active in the VLR.
   2. The authentication process takes place.
   3. Ciphering starts.
   4. Equipment is identified.
   5. The receiver’s number is sent to the network.
   6. It is checked if the subscriber is allowed to make a call.
4. The MSC instructs the BSC to allowed a free traffic channel (TCH) to the MST. The MST is told to tune to that TCH.
5. The MSC forwards the receiver’s number to the Public Switched Telephone Network (PSTN), which makes a connection.
6. If the receiver answers, the connection is made.

### Calls to an MST



1. The PSTN identifies the required mobile network and connects to the relevant Gateway MSC (GMSC), a special MSC meant to deal with calls from outside the network.
2. The GMSC checks the HLR to find which MSC is serving the relevant MST. The GMSC routes the call to this MSC.
3. The MSC finds the relevant BSC, which sends a paging message via the Paging Channel (PCH).
4. When the MST detects the paging message, it sends a request via the RACH for an SDCCH.
5. The BSC allocates an SDCCH via the AGCH.
6. Over the SDCCH:
   1. The MS is marked as active in the VLR.
   2. The authentication process takes place.
   3. Ciphering is started.
   4. Equipment is identified.
7. The MSC orders the BSC to allocate an idle TCH. The MST is told to tune to the TCH. The phone rings, and if the receiver picks up, a connection is made.