Experiment No -9

Student name: Yahyah shaikh   Date of performance : 9/10/23
Roll No : 59   Date of Completion : 9/10/23
Course / Year: BE EXTC

Aim: Study and Performance Analysis of General GPRS (packet switching Network) using AT Commands

Objective- Students will understand and analyze **GPRS Network using AT commands**

Requirements:
Hardware- GSM Modem Sim 900 ,Rs232 cable, adapter.
Software: -Terminal or Putty software

Theory

General Packet Radio Services (GPRS) is a packet-based wireless communication service that promises data rates from 56 up to 114 Kbps and continuous connection to the Internet for mobile phone and computer users. The higher data rates allow users to take part in video conferences and interact with multimedia Web sites and similar applications using mobile handheld devices as well as notebook computers. GPRS is based on Global System for Mobile (GSM) communication and complements existing services such circuit-switched cellular phone connections and the Short Message Service (SMS).

In GPRS if we want to access packet network MS need to attach to the network then PDP exchange procedure will followed.

Mobility management

Mobility management states. The mobility management (MM) function is to support the mobility of user terminals. The MM activities related to a GPRS terminal are characterized by one of the three different states, i.e., IDLE, STANDBY, and READY. Figures 1 and 2 illustrate the MM state models of the MS and the SGSN, respectively.

In GPRS IDLE state, the MS camps onto the GSM network. The MS can receive circuit-switched paging and perform location area updates. In this stage, the MS behaves like any other GSM phone. It is not attached to GPRS mobility management yet. The MS and the SGSN contexts hold no valid location or routing information for the subscriber.
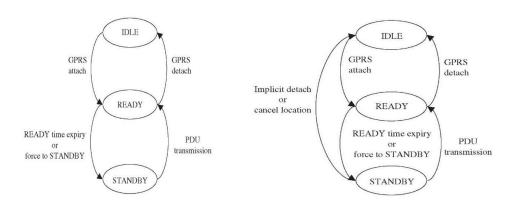
Figure1. MM state model of an MS.   Figure 2 MM state model of an SGSN.

Data transmission to and from the MS is not possible. The GPRS MS is not reachable, as paging is not possible. The MS makes the transition to the STANDBY state by attaching itself with the network using the GPRS attach procedure.

In the GPRS READY state, the network is aware of cell location as a result of the successful mobility management procedure. The MS can send or receive PDP PDUs and activate and deactivate PDP contexts. The MS makes the transition to the STANDBY state if no data transmission occurs for a settable timer period. A GPRS detach procedure brings the MS back to the IDLE state.

In GPRS STANDBY, the MS is attached to the network. The MS and the SGSN have established MM contexts. The MS can be paged for PS and CS call via SGSN. The MS can initiate activate and deactivate PDP context. The MS makes the transition to the READY state by transmitting or receiving an LLC PDU. The transition to the IDLE state happens when the MS implicit detach from the network occurs or the SGSN receives a MAP cancel location from the HLR.

GPRS attach. The mobile station must perform a GPRS attach in order to be known to the network and move to the READY state. Following the successful GPRS attach, an MM context is said to be active at the MS and the SGSN. The MS can activate PDP context only after a successful attach.
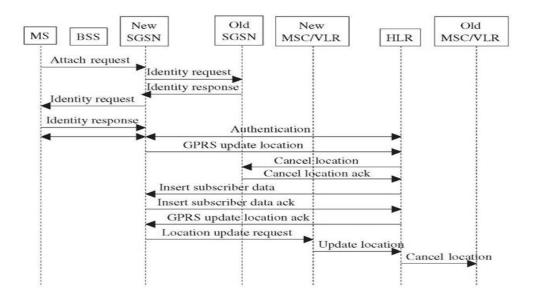
Figure 3.GPRS attach procedure .

Figures 3 and Figure 4 show the steps for the GPRS attach procedure.

STEPS

1. The MS sends the attach request message to the serving SGSN. The key parameters are:

■ **IMSI or P-TMSI**

■ **Routing area identifier (RAI)**

■ **Cipher key sequence number**

■ **Attach type**

■ **DRX**

2. If the MS is known to the SGSN, i.e., the SGSN has not changed since the MS was last attached to the network, then step 3 is not required.

3. If this MS is unknown to the serving SGSN, the SGSN takes additional steps to get the IMSI from the old SGSN. In case the old SGSN failed to provide the IMSI, the new SGSN requests the MS to provide the IMSI. The identity request message is used in both cases.
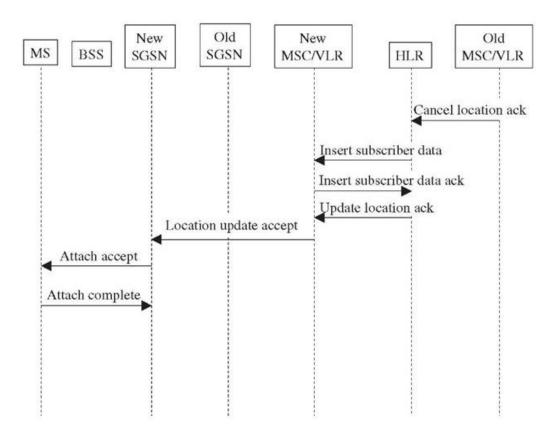

Figure 4 GPRS attach procedure

4. Once the IMSI is known, the serving SGSN initiates the authentication procedure by sending an authentication and ciphering request' to the MS.

5. If the SGSN has changed since the MS was last attached to the network, the new serving SGSN initiates the update location procedure with the HLR.

6. The HLR sends a cancel location to the old SGSN and sends subscription data to the new SGSN by sending an insert subscriber data message.

7. The SGSN sends an attach accept to the MS. The MS acknowledges by sending an attach complete message.

In the case of GPRS attach failure, one of the following errors is returned in the attach reject message.

■ **Illegal MS**

■ **GPRS service not allowed**

■ **GPRS and non-GPRS services not allowed**

■ **PLMN not allowed**

■ **Location area not allowed**

■ **Roaming not allowed in this location area**

■ **GPRS services not allowed in the PLMN**

■ **No suitable cells in location area**

The Gs interface between the SGSN and the MSC/VLR is not a mandatory interface. In case this interface is active, the MS can perform combined GPRS/IMSI attach. In addition to action shown in step 6, the HLR also performs a cancel location with the old MSC/VLR and updates the new MSC/VLR with the subscription data.

GPRS detach. GPRS detach can be performed either by the MS or the network. The MS uses this procedure to inform the network that it does not want GPRS services anymore. The SGSN or the HLR initiates a detach procedure to inform the MS that GPRS services are no more accessible to the MS. The three different types of detach are:

■ **IMSI detach**

■ **GPRS detach**

■ **Combined IMSI/GPRS detach**

The detach request could be explicit or implicit. The explicit detach can be initiated by the MS or the network.

In case of implicit detach, it is the network that initiates the detach procedure, without informing the MS. This may happen in the following cases: (1) after the mobile reachable

timer expiry and (2) once the logical link disconnects because of irrecoverable radio error causes.
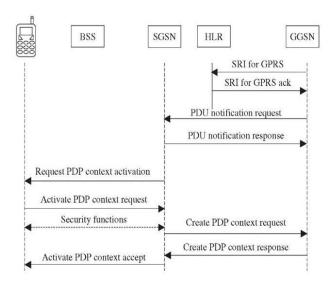

Figure 6 shows the MS-initiated detach procedure. The information elements included in the detach request message are:

■ Detach type (GPRS detach only, IMSI detach only, combined GPRS/IMSI detach)

■ P-TMSI

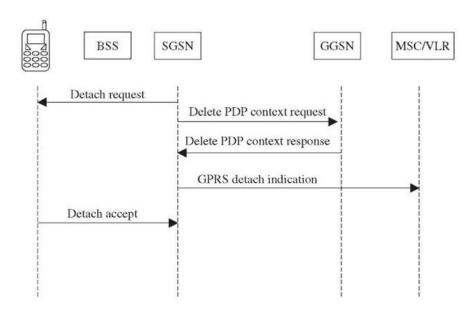**■ Switch off (detach because of switch off)**

Figure 8. shows the SGSN-initiated detach procedure. The main parameter in the detach request message is detach type. This parameter indicates whether the MS has been requested to perform a new attach and PDP context activation for the previously activated PDP contexts. If yes, then the attach procedure will be initiated when the detach procedure is completed.
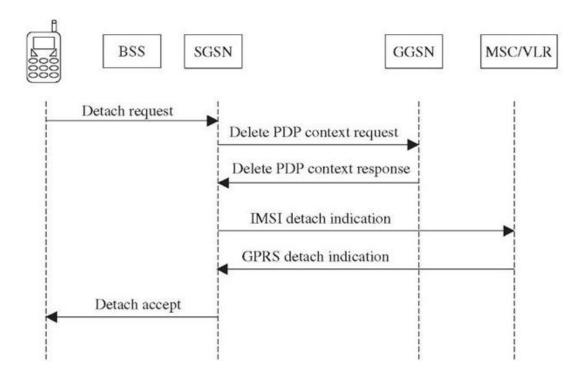
Figure 9MS-initiated detach procedure.

Session management
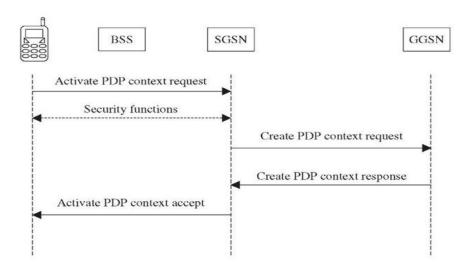
MS-initiated PDP context activation. Once the MS is attached to the GPRS network, it can send and receive SMS. The MS must perform PDP context activation to use other GPRS services such as Internet access, intranet access, email, and MMS. This is required to establish a tunnel between the MS and the requested external packet data network for the data transfer.

The steps to successful PDP context activation are as follows:

1. **The MS sends an activate** PDP context message to the serving SGSN. This message contains following parameters.

■ **PDP type (IP or X.25)**

■ **PDP address (static IP address or NULL for dynamic IP address)**

■ **APN (access point name: points to a certain packet data network or service a user wishes to access)**

■ **QoS requested**

■ **NSAPI**

■ **PDP configuration options**

2. The SGSN may decide to perform standard security checks, i.e., ciphering and authentication, IMSI check, IMEI check, P-TMSI real-location, etc.)

3. The SGSN validates the activated DP context request for PDP type, PDP address, APN, etc. against the subscription. The SGSN also requests its local DNS to provide the GGSN address serving the requested APN.
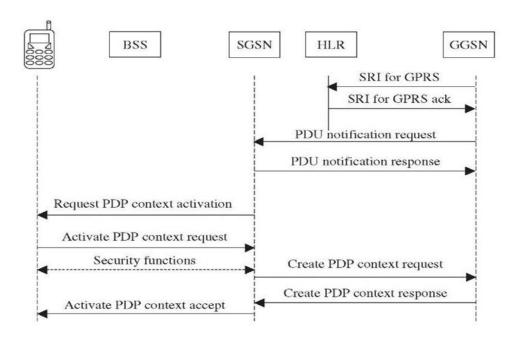

If any of the validation checks fail, the SGSN rejects the request and provides an appropriate cause value. On successful validation, the SGSN determines the tunnel ID (TID) by a combination of IMSI and NSAPI and sends a create PDP context request message to the GGSN. This message contains the following parameters.

■ **PDP type (IP or X.25)**

■ **PDP address (static IP address or NULL for dynamic IP address)**

■ **APN (access point name: points to a certain packet data network or service a user wishes to access)**

■ **QoS negotiated**

■ **TID**

■ **NSAPI**

■ **MSISDN**

■ **Selection mode (subscribed or non subscribed APN)**

■ **PDP configuration options**

4. The GGSN uses APN to identify the packet data network or services using DNS. It also uses DHCP or an external RADIUS server to get a PDP address for the MS. If the GGSN has been configured to use external PDN address allocation for the requested APN, the PDP address is set to 0.0.0.0, indicating that the PDP address shall be negotiated by the MS with the external PDN after the PDP context is activated.

5. The GGSN sends the create PDP context response to the SGSN. This message contains the following parameters.

■ **PDP address**

■ **QoS negotiated**

■ **TID**

■ **PDP configuration options**

■ **BB protocol (TCP/UDP)**

■ **Cause**

6. The SGSN inserts address parameters, i.e., NSAPI and GGSN address and sends an activate PDP context response message to the MS.

Network-initiated PDP context activation. When a GGSN receives a PDP PDU, it checks whether a PDP context exists for the PDP address. If not, the GGSN tries to deliver the PDP PDU by initiating a network-initiated PDP context request. Figure 4-18 illustrates this procedure. Network-initiated PDP context activation is possible only if the GGSN has static PDP information about the PDP address. The steps to successful PDP context activation are as follows:

1. On receiving a PDP PDU, the GGSN checks if there is static PDP information for that PDP address. If so, it starts storing subsequent PDP PDUs for that PDP address.

AT Commands for GPRS Support

Overview of AT Commands for GPRS Support

Command	Description
AT+CGATT	ATTACH/DETACH FROM GPRS SERVICE
AT+CGDCONT	DEFINE PDP CONTEXT
AT+CGQMIN	QUALITY OF SERVICE PROFILE (MINIMUM ACCEPTABLE)
AT+CGQREQ	QUALITY OF SERVICE PROFILE (REQUESTED)
AT+CGACT	PDP CONTEXT ACTIVATE OR DEACTIVATE
AT+CGDATA	ENTER DATA STATE
AT+CGPADDR	SHOW PDP ADDRESS
AT+CGCLASS	GPRS MOBILE STATION CLASS
AT+CGEREP	CONTROL UNSOLICITED GPRS EVENT REPORTING
AT+CGREG	NETWORK REGISTRATION STATUS
AT+CGSMS	SELECT SERVICE FOR MO SMS MESSAGES

1. AT+CGATT Attach /Detach From GPRS Service

AT+CGATT Attach /Detach From GPRS Service

Test Command AT+CGATT=?	Response +CGATT: (list of supported <state>s) **OK** Parameter See Write Command
Read Command AT+CGATT?	Response +CGATT: <state> **OK** Parameter See Write Command

Write Command
AT+CGATT=<state>
	Response
	OK
	If error is related to ME functionality:
	+CME ERROR: <err>
	Parameter
	<state> indicates the state of GPRS attachment
	    0 – detached
	    1 – attached
	    Other values are reserved and will result in an ERROR
	    response to the Write Command.

2. AT+CGDCONT Define PDP Context

AT+CGDCONT	Define PDP Context
Test Command **AT+CGDCONT =?**	Response **+CGDCONT**: (range of supported <cid>s),<**PDP_type**>,,,(list of supported<**d_comp**>s),(list of supported<**h_comp**>s) [<**CR**><**LF**>+**CGDCONT**: (range of supported <cid>s), <**PDP_type**>,,,(list ofsupported <**d_comp**>s),(list of supported <**h_comp**>s) [...]] **OK** Parameters See Write Command
Read Command **AT+CGDCONT ?**	Response **+CGDCONT**: <cid>,<**PDP_type**>,<**APN**>,<**PDP_addr**>,<**data_comp**>,<**head_comp**> [<**CR**><**LF**>+**CGDCONT**: <cid>,<**PDP_type**>,<**APN**>,<**PDP_addr**>,<**data_comp**>,<**head_comp**> [...]] **OK** Parameters See Write Command

Write Command	Response
AT+CGDCONT **=\<cid>[,\<PDP_ty pe>,[APN>[,\<PD P_addr>[,\<d_co mp>[,\<h_comp>]]]]]**	**OK**
	ERROR
	Parameters

\<cid>		(PDP Context Identifier)
1		PDP Context Identifier 1
		Definition stored in non-volatile memory
2		PDP Context Identifier 2
		Definition stored in non-volatile memory
3		PDP Context Identifier 3
		Default \<cid>
		Locked in non-volatile memory and is always defined, it can not be changed by user.
\<PDP_type>		(Packet Data Protocol type)
IP		Internet Protocol (IETF STD 5)
\<APN>		(Access Point Name) a string parameter(string should be included in quotation marks) which is a logical name that is used to select the GGSN or the external packet data

3. AT+CGQMIN Quality Of Service Profile (Minimum Acceptable)

AT+CGQMIN	Quality Of Service Profile (Minimum Acceptable)
Test Command AT+CGQMIN=?	Response +CGQMIN: <PDP_type>,(list of supported <precedence>s),(list of supported <delay>s),(list of supported <reliability>s),<list of supported <peak>s),(list of supported <mean>s) [<CR><LF>+CGQMIN: <PDP_type>,(list of supported <precedence>s),(list of supported <delay>s),(list of supported <reliability>s),<list of supported <peak>s),(list of supported <mean>s) […]] OK Parameters See Write Command
Read Command AT+CGQMIN?	Response +CGQMIN: <cid>,<precedence>,<delay>,>reliability>,<peak>,<mean> [<CR><LF>+CGQMIN: <cid>,<precedence>,<delay>,<reliability>,<peak>,<mean> […]] OK Parameters See Write Command

Write Command	Response
AT+CGQMIN=< cid>[,<precedenc e>[,<delay>[,<rel iability>[,<peak [,<mean>]]]]]	OK If error is related to ME functionality: +CME ERROR: <err> Parameters <cid> 1..3 PDP Context Identifier Definition stored in non-volatile memory (refer to +CGDCONT). cid 3 is reserved and is always defined, it cannot be changed by user. <precedence> 0 (default) QOS precedence class subscribed value 1..3 QOS precedence class <delay> 0 (default) QOS delay class subscribed value 1..4 QOS delay class subscribed <reliability> 0(default) QOS reliability class subscribed value

4. AT+CGQREQ Quality Of Service Profile (Requested)

AT+CGQREQ	Quality Of Service Profile (Requested)
Test Command **AT+CGQREQ=?**	Response **+CGQREQ:** <PDP_type>,(list of supported <precedence>s),(list of supported <delay>s),(list of supported <reliability>s),<list of supported <peak>s),(list of supported <mean>s) [<CR><LF>**+CGQREQ:** <PDP_type>,(list of supported <precedence>s),(list of supported <delay>s),(list of supported <reliability>s),<list of supported <peak>s),(list of supported <mean>s) […]] **OK** Parameters See Write Command
Read Command **AT+CGQREQ?**	Response **+CGQREQ:** <cid>,<precedence>,<delay>,>reliability>,<peak>,<mean> [<CR><LF>**+CGQREQ:** <cid>,<precedence>,<delay>,<reliability>,<peak >,<mean> […]] **OK** Parameters See Write Command

Write Command	Response
AT+CGQREQ= **<cid>[,<precede** **nce>[,<delay>[,<** **reliability>[,<pea** **k>[,<mean>]]]]]**	**OK**

Response

OK

If error is related to ME functionality:

+CME ERROR: <err>

Parameters

<cid>   a numeric parameter which specifies a particular PDP context definition (see +CGDCONT Command)

    1..3   Definition stored in non-volatile memory (refer to +CGDCONT) cid 3 is reserved and is always defined, it cannot be changed by user.

The following parameter are defined in GSM 03.60

<precedence>   a numeric parameter which specifies the precedence class

    0 (default)   QOS precedence class subscribed value

    1..3   QOS precedence class

<delay>   a numeric parameter which specifies the delay class

    0 (default)   QOS delay class subscribed value

    1..4   QOS delay class

<reliability>   a numeric parameter which specifies the reliability class

    0   QOS reliability class subscribed value

    1..5   QOS reliability class; default value: 3

<peak>   a numeric parameter which specifies the peak throughput class

    0 (default)   QOS peak throughput class subscribed value

    1..9   QOS peak throughput class

<mean>   a numeric parameter which specifies the mean throughput class

    0 (default)   QOS mean throughput class subscribed value

    1..18   QOS mean throughput class

    31   QOS mean throughput class best effort

5. AT+CGACT PDP Context Activate Or Deactivate

AT+CGACT	PDP Context Activate Or Deactivate
Test Command AT+CGACT=?	Response +CGACT: (list of supported <state>s) OK Parameter See Write Command
Read Command AT+CGACT?	Response +CGACT: <cid>,<state>[<CR><LF>+CGACT:<cid><state>...] OK

Write Command
AT+CGACT=<state>,<cid>
	Response
	OK
	If error is related to ME functionality:
	+CME ERROR: <err>
	Parameters
	<state> indicates the state of PDP context activation
	       0 – deactivated
	       1 – activated
	       Other values are reserved and will result in an ERROR
	       response to the Write Command.
	<cid> a numeric parameter which specifies a particular PDP

6. AT+CGDATA Enter Data State

AT+CGDATA Enter Data State	
Test Command **AT+CGDATA=?**	Response **+CGDATA:** list of supported **<L2P>**s **OK** Parameter See Write Command

Write Command
AT+CGDATA[=
<L2P>,[<cid>]]
	Response
	CONNECT
	If error is related to ME functionality:
	+CME ERROR: <err>
	Parameters
	<L2P> a string parameter(string should be included in quotation marks) that indicates the layer 2 protocol to be used between the TE and MT:
	     PPP – Point to Point protocol for a PDP such as IP
	     Other values are not supported and will result in an ERROR response to the execution Command.
	<cid> a numeric parameter which specifies a particular PDP context definition (see +CGDCONT Command)
	     1..3 PDP Context Identifier. cid 3 is reserved and is always defined, it cannot be changed by user.

7. AT+CGPADDR Show PDP Address

AT+CGPADDR	Show PDP Address
Test Command AT+CGPADDR= ?	Response +CGPADDR: (list of defined <cid>s) OK Parameter See Write Command
Write Command AT+CGPADDR=	Response +CGPADDR: <cid>,<PDP_addr>

[<cid>]	[<CR><LF>+CGPADDR: <cid>,<PDP_addr>[...]]
	
	OK
	ERROR
	Parameters
	<cid> a numeric parameter which specifies a particular PDP
	    context definition (see +CGDCONT Command) If no <cid>
	    is specified, the addresses for all defined contexts are
	    returned.
	    1..3 PDP Context Identifier, cid 3 is reserved and is always
	    defined, it cannot be changed by user.
	<PDP_addr>
	    String type IP address
	        Format: "<n>.<n>.<n>.<n>" where <n>=0..255

8. AT+CGCLASS GPRS Mobile Station Class

AT+CGCLASS	GPRS Mobile Station Class
Test Command **AT+CGCLASS=** **?**	Response **+CGCLASS:** (list of supported <class>s) **OK** Parameter See Write Command
Read Command **AT+CGCLASS?**	Response **+CGCLASS:** <class> **OK** Parameter See Write Command
Write Command **AT+CGCLASS=** <class>	Response **OK** **ERROR** If error is related to ME functionality: **+CME ERROR:** <err> Parameter <class>　　　　a string parameter(string should be included in quotation marks) which indicates the GPRS mobile class (in

	descending order of functionality)
B	Class-B mode of operation (A/Gb mode), (not applicable in Iu mode) MT would operate PS and CS services but not simultaneously
CC	Class-C mode of operation in CS only mode (A/Gb mode), or CS (Iu mode) (lowest mode of operation). MT would only operate CS services

9.
AT+CGEREP Control Unsolicited GPRS Event Reporting

AT+CGEREP	Control Unsolicited GPRS Event Reporting
Test Command AT+CGEREP=?	Response +CGEREP: (list of supported \<mode\>s) ,(list of supported \<bfr\>s) OK Parameter See Write Command
Read Command AT+CGEREP?	Response +CGEREP: \<mode\>,\<bfr\> OK Parameter See Write Command

Write Command
AT+CGEREP=\<
mode\>[,\<bfr\>]
	Response
	OK
	ERROR
	Parameter
	\<mode\>
	
	     0 Buffer unsolicited result codes in the MT; if MT
	         result code buffer is full, the oldest ones is discarded.
	
	     1 Discard unsolicited result codes when MT TE link
	         is reserved (e.g. in on line data mode); otherwise
	         forward them directly to the TE
	
	     2 Buffer unsolicited result codes in the MT when MT

TE link is reserved (e.g. in on line data mode) and flush them to the TE when MT TE link becomes available; otherwise forward them directly to the TE

<bfr>   0   MT buffer of unsolicited result codes defined within this command is cleared when <mode> 1 or 2 is entered

          1   MT buffer of unsolicited result codes defined within this command is flushed to the TE when <mode> 1 or 2 is entered

10. AT+CGREG Network Registration Status

AT+CGREG	Network Registration Status
Test Command **AT+CGREG=?**	Response **+CGREG:** (list of supported <n>s) **OK** Parameter See Write Command
Read Command **AT+CGREG?**	Response **+CGREG:** <n>,<stat>[,<lac>,<ci>] **OK** **+CME ERROR:** <err> Parameter See Write Command

Write Command
AT+CGREG=[<
n>]
	Response
	OK
	ERROR
	Parameters
	<n> 0 disable network registration unsolicited result code
	        1 enable network registration unsolicited result code
	            +CGREG:<stat>
	        2 enable network registration and location information

	unsolicited result code +CGREG: <stat>[,<lac>,<ci>]
	<stat> 0 Not registered, MT is not currently searching an operator to register to The GPRS service is disabled, the UE is allowed to attach

		for GPRS if requested by the user
	1	Registered, home network
	2	Not registered, but MT is currently trying to attach or searching an operator to register to The GPRS service is enabled, but an allowable PLMN is currently not available. The UE will start a GPRS attach as soon as an allowable PLMN is available.
	3	Registration denied The GPRS service is disabled, the UE is not allowed to attach for GPRS if requested by the user.
	4	Unknown
	5	Registered, roaming
<lac>		string type (string should be included in quotation marks); two byte location area code in hexadecimal format (e.g. "00C3" equals 195 in decimal)
<ci>		string type (string should be included in quotation marks); two bytes cell ID in hexadecimal format

11.AT+CGSMS Select Service For MO SMS Messages

AT+CGSMS	Select Service For MO SMS Messages
Test Command AT+CGSMS=?	Response +CGSMS: (list of currently available <service>s) OK Parameter See Write Command
Read Command AT+CGSMS?	Response +CGSMS: <service> OK Parameter See Write Command
Write Command AT+CGSMS=[<service>]	Response OK If error is related to ME functionality: +CME ERROR: <err> Parameter <service> a numeric parameter which indicates the service or service

	preference to be used
0	Packet Domain
1	Circuit switched
2	Packet Domain preferred (use circuit switched if GPRS not available)
3	Circuit switched preferred (use Packet Domain if circuit switched not available)

12. AT+CIPSTART Start Up TCP Or UDP Connection

AT+CIPSTART	Start Up TCP Or UDP Connection
Test Command AT+CIPSTART= ?	Response 1) If AT+CIPMUX=0 +CIPSTART: (list of supported \<mode>),IP address range,(port range) +CIPSTART: (list of supported \<mode>),(domain name),(port range) OK 2) If AT+CIPMUX=1 +CIPSTART: (list of supported \<n>),(list of supported \<mode>),IP address range,(port range) +CIPSTART: (list of supported \<n>),(list of supported \<mode>),(domain name),(port range) OK Parameters See Write Command
Write Command 1)If single IP connection (+CIPMUX=0) +CIPSTART=\<mode>,\<IP address>,\<port> Or	Response 1)If single IP connection (+CIPMUX=0) If format is right response OK, otherwise response +CME ERROR \<err> If connection exists, response ALREAY CONNECT If connected successfully response CONNECT OK

Conclusion

We studied & performed Analysis of General GPRS (packet switching Network) using AT Commands

Output
GPRS Command
1. AT+CGATT?
     +CGATT: 1 //(1 Indicate that it is attached)

2. AT+CGACT(AT+CGACT AT command is used to activate ot deactivate the PDP context.)
     ERROR
     AT+CGACT?
     +CGACT: 3,0

      OK

3. AT+CGCLASS? (AT command is used to set the device to operate according to specified GPRS mobile class.)
     +CGCLASS: "B"

     OK

4. AT+CIPSTATUS (AT comamnd returns the current connection status. This command returns the applicable server status, client status, conenction number (for multi-ip) and GPRS bearer info. May be STATE -Ip INITIAL., STATE -IP-PROCESSING, STATE -IP-PDP-DEACT)

     AT+CIPSTATUS
     OK

     STATE: IP INITIAL

5 . AT+CIPSTART="TCP","www.google.com","80"

     OK

     CONNECT OK

     CLOSED

COM1 - PuTTY

```
RING

NO CARRIER
AT+CGATT?
+CGATT: 1

OK
AT+CGACT
ERROR
AT+CGACT
ERROR
At+CGACT?
+CGACT: 3,0

OK
AT+CGCLASS?
+CGCLASS: "B"

OK
AT+CIPSTATUS
OK

STATE: IP INITIAL
\T+CIP="TCP"
ERROR
AT+CIPSTART="TCP","www.google.com","80"
OK

CONNECT OK
CLOSED
```