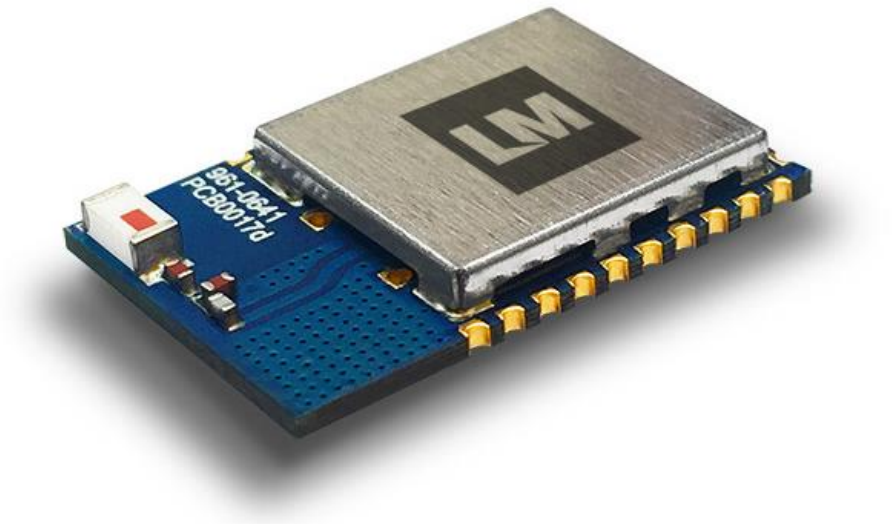
LM961

SPP with GAP Central Application

USER GUIDE



Revision	Date	Changes Description
v1.0	17/11/2017	First revision of this document.
v1.1	8/12/2017	Minor document revisions.

Contents

Table of Figures

1. Introduction

This document describes the functionality of the “SPP with GAP Central” application.

1. SPP with GAP Central application specific AT commands and information
2. All AT commands and default configurations on device
3. Over the Air Firmware Upgrade procedure
4. Secure simple pairing procedure

The LM961 is a dual mode module with the capability for simultaneous connections to Bluetooth (v1.0 – v3.0), and Bluetooth low energy devices. LM Technologies supports various firmware applications on the LM961 module enabling users to develop their own applications with AT commands.

2. Functionality of SPP with GAP Central application

In the SPP with GAP Central application the LM961 can either be a SPP Master or Slave; or dual mode with one SPP connection at a time. The SPP role supports BOND, ACON, and features similar to those of LM Technologies’ legacy products such as the LM048, LM072 and LM400,

For Bluetooth low energy, it will be in the GAP Central role and can establish connections to up to five low energy peripherals simultaneously. Users can have a maximum of six active connections with this application (five low energy and one SPP). Data can be transferred between devices using AT commands.

For the Bluetooth low energy GAP Central role, the user can perform functions normally performed by Android tablets or phones. A user can discover nearby Bluetooth low energy peripherals, and up to ten devices will be reported. They can then connect to any of those devices and read or write data on various services or characteristics with the help of AT commands. The Bluetooth low energy connection also supports whitelisting. If you add the paired devices to the whitelist it will only report advertising packets from the devices added to the whitelist, or only connect to devices on the whitelist.

3. LM961 GAP Central Role

This section describes the AT commands for the GAP Central role to initiate a connection, pair, whitelist, or read/write data to a BLE peripheral device.
AT commands for the SPP role and generic device configuration are described in section 4 “LM961 AT commands and Default configuration”.

Every command is terminated with “CR-LF”. The module will begin parsing the AT command string after receiving the “CR-LF” sequence.

For every AT command issued by a user via UART the module responds with OK/ERR. If the user issues an incorrect AT command string (e.g. instead of "AT*Settings=?" the user issues "AT*Setting=?"), or issues a correct AT command string but in an invalid state (e.g. the user issues a connection command "AT*CONN=001122334455" while the SPP-role is Slave), the module will respond with ERR.

AT commands are used to enable or disable the GAP Central role of the module. By default, this mode is disabled and the module only initiates the SPP functionality. To enable GAP Central functions, use the AT command AT*ENBGAP=ON. The module will perform a soft reset and initialize itself with both SPP and GAP Central functions initialized. When the module has the GAP Central role disabled, for every AT command of GAP Central functionality or settings, module will respond with “ERR”.

When the module is in the GAP Central role it supports BLE device discovery, connection initiation, and reading/writing data. Users can use different AT commands to read/write data on BLE peripherals or receive updates from BLE peripherals via UART.

The SPP with GAP Central application enables the SPP and BLE connections. If the module is in the slave role it is ready to accept an SPP connection at any moment. If the user application only requires GAP Central roles, then set the SPP role as Master and ACON as OFF. This means that module will only connect to a remote SPP device when the connection is initiated by the LM961 module with an AT command.

If the user application requires a SPP connection with ACON ON and BLE connections it’s possible that the LM961 might connect with a remote SPP master device while reading/writing data on the BLE Peripheral, or while performing some other task. This will be indicated to user with “IND*:CONNECTED=001122334455”. If so the user should use the escape sequence i.e. +++ to come out of SPP-Online-Connected mode and then issue the required AT commands.

3.1 GAP Central AT commands in brief

The table below shows the AT commands for the GAP Central role with examples for reference.

Sr no	AT command string	Command type	Default setting	AT command format for reference
1	“AT*ENBGAP”	Query and Set	OFF	AT*ENBGAP=? AT*ENBGAP=ON AT*ENBGAP=OFF
2	“AT*LESEC”	Query and set	OFF	AT*LESEC=ON / AT*LESECOFF /ATLESEC=?
3	“AT*GETCID”	Query only	-	
4	“AT*LEFIND”	Execution only	-	AT*LEFIND=ON AT*LEFIND=OFF
5	“AT*LECONN”	Execution only	-	AT*LECONN=0011223 34455
6	“AT*LEDROP”	Execution only	-	AT*LEDROP=00112233 4455
7	“AT*ENBCCFG”	Execution only	-	AT*ENBCCFG=CID,CH AR-Handle e.g. At*enbccfg=5,0019
8	“AT*BLECONN”	Query only	-	AT*BLECONN=?
9	“AT*INDRESP”	Execution only	-	AT*INDRESP=CID e.g. At*indresp=5
10	“AT*FINDSERV”	Execution only	-	AT*FINDSERV=CID e.g. At*findserv=5
11	“AT*FINDCHAR”	Execution only	-	AT*FINDCHAR=CID,St art-Handle,End-Handle e.g. At*findchar=5,0001,ffff
12	“AT*CLRWHITE”	Execution only	-	“AT*CLRWHITE”\r\n

Sr no	AT command string	Command type	Default setting	AT command format for reference
13	“AT*WRWORESP”	Execution only	-	AT*WRWORESP=CID,Char-Handle,no-of-bytes,actualbytes e.g. at*wrworesp=5,0012,14,0123456789012345678 9
14	“AT*RDCHARVAL”	Execution only	-	AT*RDCHARVAL=CID, char-handle e.g. At*rdcharval=5,0020
15	“AT*WRCHARVAL”	Execution only	-	AT*WRCHARVAL=CID, char-handle,no-of-bytes,actualbytes e.g. at*wrcharval=5,0012,14,0123456789012345678 9
16	“AT*LEAUTOSCAN”	Query and Set	-	AT*LEAUTOSCAN=ON AT*LEAUTOSCAN=OFF AT*LEAUTOSCAN=?
17	“AT*RDMULTCHAR”	Execution only	-	AT*RDMULTCHAR=CID,no-of-read,char-handle1,char-handle-2,char-handle3,char-handle4, char-handle5 e.g. At*rdmultchar=5,05,0003,0005,0008,0008,000a
18	“AT*RDLONGCHAR”	Execution only	-	AT*RDLONGCHAR=CID,Char-Handle e.g. at*rdlongchar=5,0029
19	“AT*SIWRWORESP”	Execution only	-	AT*SIWRWORESP=CID,Char-Handle,no-of-bytes,actual-bytes e.g. at*siwrworesp=5,0028,14,0123456789012345 6789

3.2 Enable GAP Central functionality:

3.2.1 "AT*ENBGAP"\r\n

i. Query and Set command.
ii. To query settings use the command "AT*ENBGAP=?" \r\n
iii. Response to the query command will be "OK"/"ERR" and report will be "REP*:GAP_ENABLE=ON" or "REP*:GAP_ENABLE=OFF"
iv. By default, this setting is OFF i.e. the GAP Central role is disabled. The module is only initialized for the SPP functionality.
v. To enable the GAP Central role, use the command "AT*ENBGAP=ON".
vi. The module will respond with OK and display the message "Module soft-Reset.." to indicate that the module is performing a soft reset to enable the GAP Central role.
vii. After reset, the module shows the power on sequence "SPP+GapCentral_Message_Loop"
viii. If the module currently has ENBGAP set to OFF, and command is issued to turn it OFF, the module shows an ERR response. Similarly, if the current setting is ON and the command is issued to turn it ON, the module will output an ERR response.
ix. Response of the "AT*SETTINGS=?" query command depends on the ENBGAP setting.
x. Response of the AT*SETTINGS=? Command displays the settings of LESEC, LE-Auto-Scan only if the ENBGAP is ON.

```
SPP+GapCentral_Message_Loop

at*enbgap=?at*enbgap=?
OK
REP*:GAP_ENABLE=OFF

at*settings=?at*settings=?
OK
 NAME=LM961_GAP_Central
 ADDR=0002-5b-00a5a5
 FLOW=OFF
 SPPRole=SLAVE
 ACON=OFF
 BOND=0000-00-000000
 DPIN=OFF
 PIN=1234
 GAP_ENABLE=OFF
 VER=961LM_GAPCEN_01.01
REP*:SETTINGS=END

at*enbgap=offat*enbgap=off
ERR

at*enbgap=onat*enbgap=on
OK
 Module soft-Reset..SPP+GapCentral_Message_Loop
```

GATT Initialised
REP*:LESEC=Success

at*settings=?at*settings=?
OK
NAME=LM961_GAP_Central
ADDR=0002-5b-00a5a5
FLOW=OFF
SPPRole=SLAVE
ACON=OFF
BOND=0000-00-000000
DPIN=OFF
PIN=1234
GAP_ENABLE=ON
LE_SEC=OFF
LE_AUTO_SCAN=ON
VER=961LM_GAPCEN_01.01
REP*:SETTINGS=END

at*enbgap=?at*enbgap=?
OK
REP*:GAP_ENABLE=ON

at*enbgap=onat*enbgap=on
ERR

at*enbgap=offat*enbgap=off
OK
Module soft-Reset..SPP+GapCentral_Message_Loop

3.3 BLE discovery commands:

3.3.1 "AT*LEFIND"\r\n

i. Execution only command.
ii. To begin discovery of nearby BLE peripheral devices, use the command "AT*LEFIND=ON"\r\n
iii. The module responds with OK to this command if it is not already scanning the devices, otherwise it responds as "ERR".
iv. The module reports the name and BT address of the device as soon as it finds the advertisement packet and keeps on updating the report as devices are discovered.
v. The module stops the BLE scanning process when it finds 10 BLE devices and displays END of report message.
vi. There is no time limit set in the firmware to end the BLE scanning process. If the user wants to terminate the scanning process, they should issue the "AT*LEFIND=OFF" command.

vii. If the module is displaying the scan report and user issues a connection request to any of the devices, then the scan is terminated and connection procedure is started.
viii. The module indicates the beginning and end of discovery response as "REP*:BLE_SCAN_REP=START" and "REP*:BLE_SCAN_REP=END" respectively.
ix. Below is an example report for BLE scanning:

"at*lefind=onat*lefind=on
OK
REP*:BLE_SCAN_REP=START
= 1 :1028-00-5b0002 :0
= 2 :1032-00-5b0002 :0
= 3 :3333-33-333333 :0
= 0: 3333-33-333333, LM Serial Server
= 4 :8863-df-be936c :0 :LML8
= 5 :0000-00-000000 :3
= 6 :1029-00-5b0012 :0 :CSR BP Sensor
= 7 :1030-00-5b0012 :0 :CSR HR Sensor
= 8 :1031-00-5b0012 :0 :CSR HR Sensor
at*lefind=offÑlefind=off
at*lefind=offat*lefind=off
OK"

x. If the user terminates the scanning process by issuing the "AT*LEFIND=OFF" command, the module responds to it with an OK/ERR message but it does not issue an end of report message.
xi. When the module finds a BLE advertising report, it does not show the device in the report immediately, it waits for the advertising packet in which BLE-Device-name is included.
    a. If the module finds address and name same packet, it displays both.
    b. If the module finds address only it shows address and waits for name.
    c. When the module finds name of the device for which it has reported address previously, it will show name in report with the serial number as 0 to indicate this is not new device but only name is appended for the device already reported.

xii. If the LM961 has setting "AT*LESEC=OFF", LM961 reports BLE devices even if not present in its Whitelist. If setting is "AT*LESEC=ON", LM961 will only report advertising devices which are in its whitelist.
xiii. In the discovery report, after the BD-address there is an indication for "advertising Indication type" ranging from 0 to 5 as mentioned below.
    a. ble_adv_event_connectable_undirected = 0 = Connectable Undirected Advert.
    b. ble_adv_event_connectable_directed = 1 = Connectable Directed Advert.
    c. ble_adv_event_discoverable = 2 = Discoverable advert.

d. ble_adv_event_non_connectable = 3 = Non-connectable.
e. ble_adv_event_scan_response = 4 = Scan Response.
f. ble_adv_event_unknown = 5 = Unknown event type.

xiv. The LM961 SPP with GAP central application also supports SPP connection. The module may establish a SPP connection while performing LE discovery. When the module connects with the SPP device, it enters in SPP-Data mode and shows data from the remote device on UART. It treats data sent on local UART as data to be sent to remote device. To access UART for commands and responses, the user needs to use the escape sequence and then continue with other AT commands.

xv. Refer to the screenshots below.

```
at*lefind=onat*lefind=on
OK
REP*:BLE_SCAN_REP=START
 = 1 :1032-00-5b0002 :0
 = 2 :1028-00-5b0002 :0
 = 3 :3333-33-333333 :0
 = 0: 3333-33-333333, LM Serial Server
 = 4 :8863-df-be936c :0 :LML8
IND*:CONNECTED=0012-6f-0819c2
+++OK
 = 7 :2053-ca-20126e :0
 = 8 :2053-ca-20126f :0
at*lefind=offat*lefind=off
OK
```

xvi. Data during the SPP connection and receive of escape command is lost in this report (data is lost as UART is given to SPP connection).

3.4 BLE security commands:

3.4.1 “AT*LESEC”\r\n

i. Query and Set command.
ii. LESEC stands for Low Energy Security i.e. whether to apply whitelist security or not.
iii. Query command to query the setting is “AT*LESEC=?”\r\n.
iv. Query report is “REP*:LE_SEC=OFF”\r\n or “REP*:LE_SEC=ON”\r\n.
v. When LESEC is ON, the module will scan advertising packets only from whitelist added devices and connect to the devices already added to whitelist (i.e. already BLE paired devices)
vi. When LESEC is OFF, the module will scan and connect to any BLE discoverable and connectable device (module will discover and connect any device even if it is not paired with module before)

Note: If the LM961 wants to add a new device in its whitelist then while establishing the connection with the device at first time user should use setting “AT*LESEC=OFF”. This enables the

authentication procedure to start to add a new device to the white list.
Once the module completes the pairing procedure successfully the BLE device is added to the white list. Then the LM961 can use the setting "AT*LESEC=ON" for further connections with the same device.

3.4.2 "AT*CLRWHITE"\r\n

i. Execution only command.
ii. This command is used to delete all the devices from BLE paired devices list i.e. White list.
iii. Command format is "AT*CLRWHITE"\r\n
iv. Module responds OK and deletes all the devices from the whitelist.

3.5 BLE connection commands:

3.5.1. "AT*LEAUTOSCAN"\r\n

i. Query and set command.
ii. Enable or disable the feature to scan the connected BLE peer device automatically for its services.
iii. Low energy auto scan query: "AT*LEAUTOSCAN=?"\r\n.
iv. Low energy auto scan query report: "REP*:LE_AUTOSCAN_SERVER=ON" (Module default setting as LE-Auto-Scan enabled)
v. Low energy auto scan enable command: "REP*:LE_AUTOSCAN_SERVER=ON"\r\n. If LE Auto Scan is enabled, after connection module starts scanning Peer device for its services and characteristics automatically.
vi. Low energy auto scan disable command: "REP*:LE_AUTOSCAN_SERVER=OFF"\r\n. If disabled, module does not scan the Peer device for its services and characteristics automatically. Module will wait for AT*FindServ command from user.

3.5.2 "AT*BLECONN"\r\n

i. Query only command.
ii. User can query how many BLE connections module is having and details for those connections.
iii. Command format is : "AT*BLECONN=?"\r\n
iv. GAP Central application can have maximum 5 BLE connections simultaneously.
v. Example report for this command shall be as shown below
at*BLECONN=?at*BLECONN=?

```
OK
REP*:BLE_CONN
 = 1 : 3333-33-333333 : 0101
 = 2 : 1030-00-5b0012 : 0182
 = 3 : 1032-00-5b0002 : 0203
 = 4 : Open
 = 5 : Open
REP*:BLE_CONN END
```

vi. The report above shows that the module is now connected with three devices. The report lists connection ID given by module, remote device BD-Address and Connection-ID i.e. CID given by BLE stack.
vii. Start and end of report is mentioned.
viii. E.g. In above report, row "= 3 : 1032-00-5b0002 : 0203" mentions module has 3rd connection with 1032-00-5b0002 device and CID given by BLE stack is 0203.
ix. CID given in above response is referred while reading/writing data with AT commands, reporting disconnection, notification etc. User should note this carefully.
x. Response to this module depends on current state of the module for BLE connections.
xi. In a scenario where module has established 3 connections as shown above and if it drops connection 2 then the response to command AT*BLECONN=? Will be

```
at*BLECONN=?at*BLECONN=?
OK
REP*:BLE_CONN
 = 1 : 3333-33-333333 : 0101
 = 2 : Open
 = 3 : 1032-00-5b0002 : 0203
 = 4 : Open
 = 5 : Open
REP*:BLE_CONN END
```

3.5.3 "AT*LECONN"\r\n

i. Execution only command
ii. GAP Central application gives more details on connection parameters when connection is successful and error code value if connection fails.
iii. User need to mention the BD address of the remote device with which the BLE connection is to be established, e.g. "at*leconn=1031-00-5b0012"\r\n tries to establish connection with "1031-00-5b0012" device.
iv. Response to this command will be ERR if any of the following is true
    a. string format is incorrect
    b. BT address is invalid
    c. 5 BLE connections are already established
v. Response to this command will be OK if all the following conditions are true
    a. Command string format is correct
    b. BT address is valid

c. Module has at least one BLE connection open

vi. After displaying OK response, module starts the BLE connection procedure.

vii. If the connection is failed the report is given with the error code e. g. “REP*:BLE_CONN_FAIL:=1031-00-5b0012,4 err_code:0014”\r\n.

viii. Refer the Error code list mentioned in the appendix section.

ix. If the module is successfully connected to a remote device it will show a report with details about the connection. E.g. “REP*:BLE_CONNECTED:=1030-00-5b0012-0 : 1 : 0080 : 0017 : 0008”\r\n

x. Here report includes extra information for the connection details as below.
   a. 1030-00-5b0012 is BD address of the remote BLE device.
   b. -0 with the address mentions Address type of remote BLE device.
   c. TYPED_BDADDR_PUBLIC is noted as 0, TYPED_BDADDR_RANDOM is noted as 1.
   d. 1 indicates Connection ID given by LM961 module (refer to BLEconn=? report).
   e. 0080 mentions CID given by BLE stack (hex value 0x0080).
   f. 0017 is MTU i. e. Maximum Transfer Unit for this BLE connection (hex value 0x0017).
   g. 0008 is Connection configuration flag (hex value 0x0008)

xi. User should take note of MTU mentioned in connection report, while reading and writing data on this device, using one command (rdcahval/wrworesp etc) up to MTU number of bytes can be sent/received. If user need to read/write more than MTU number of bytes, it needs two commands.

```
at*leconn=1030005b0012at*leconn=1030005b0012
OK
REP*:BLE_CONNECTED:=1030-00-5b0012-0 : 1 : 0080 : 0017 :
0008
BLE Auth start
OK
REP*:SERVICE START: =1030-00-5b0012
 = 1 : 1801 : 0001 : 0004
 = 2 : 1800 : 0005 : 000b
 = 3 : 180d : 000c : 0013
 = 4 : 180f : 0014 : 0017
REP*:BLE_PAIR=1030-00-5b0012,Success
 = 5 : 00001016d10211e19b2300025b00a5a5 : 0018 : 0021
 = 6 : 180a : 0022 : ffff
REP*:SERVICE END: =1030-00-5b0012
```

xii. BLE Pairing:
   a. After module is connected with Peer device, If LESEC i.e. LE Security is OFF, module starts BLE Authentication process and Shows message “BLE Auth start” to indicate start of authentication process.
   b. If LESEC is ON, module will report or connect to only with previously Paired devices which are present in its whitelist.

c. Pairing Success or Failure indication report is given to user as "REP*:BLE_PAIR=1030-00-5b0012,Success" or "REP*:BLE_PAIR=1030-00-5b0012,Fail" .
d. After module completes the pairing procedure successfully, module adds this device to its whitelist.
e. Pairing procedure runs at the background and can show the status of pairing at any time. e.g. above report shows the pairing report has displayed while showing Service-scan report.

xiii. If LEAutoScan server setting is ON then, module starts scanning services supported on the remote device and displays the report. If LEAutoScan server setting is OFF, module waits for commands from user to scan the services (FINDSERV).

3.5.4 "AT*LEDROP"\r\n

i. Execution only command
ii. Command is used to disconnect the BLE connection. Command requires peer devices BT address.
iii. BLE connection disconnection command format: "AT*LEDROP=1030005b0012"\r\n
iv. Response for BLE drop connection will be OK if the module is connected to the BLE device with the same address provided in Drop command.
v. Response for BLE drop connection will be ERR if the module is not connected with any BLE device or BD address mentioned in the AT command is not same as the connected BLE device.
vi. Module shows a report for the disconnection command e.g.

```
at*ledrop=1030005b0012at*ledrop=1030005b0012
OK
REP*:BLE_DIS_CONN:=1030-00-5b0012,2 err_code:0000
```

vii. Error code 0000 mentions the device has terminated connection gracefully i.e. either device started disconnection procedure.
viii. Number 2 near the BD address mentions the BLE Connection ID (refereed to BLEconn=? response).
ix. If disconnection is started by remote device or due to link loss the indication for disconnection is shown as below with the reason code.
"REP*:BLE_DIS_CONN:= 1030-00-5b0012,2 err_code:0019"
x. Refer to the error code in the appendix.

3.6 BLE Services/characteristic scan commands:

3.6.1 "AT*FINDSERV"\r\n

i. Execution only command
ii. Command is used to scan services supported on connected BLE device.
iii. User needs to state connection ID for the device whose services are to be scanned. E. g. "at*findserv=1" finds services on 1st connected device.
iv. Module provides a detailed report for the services supported by the remote device.
v. If the BLE device has any service with 128-bit UUID then it is indicated with all bytes.
vi. IN below report the row mentions " 1 : 1800 : 0001 : 0005 " where "1" is serial number, "1800" is 16bit UUID for service, "0001" is start handle of the service and "0005" is end handle of the service.
vii. Report is marked for start and end.
viii. For e.g refer below report.

```
at*findserv=1at*findserv=1
OK
REP*:SERVICE START: =3333-33-333333
 = 1 : 1800 : 0001 : 0005
 = 2 : 180a : 0006 : 0016
 = 3 : 00005500d10211e19b2300025b00a5a5 : 0017 : 001a
 = 4 : 180f : 001b : ffff
REP*:SERVICE END: =3333-33-333333
```

3.6.2 "AT*FINDCHAR"\r\n

i. Execution only command
ii. Command used to scan characteristics supported by services on the BLE device.
iii. User needs to mention connection ID for the device whose services are to be scanned. And start and end handle of the services for which scan is to be performed.
iv. User can scan characteristics for only one service or multiple services or for all services in single command.

```
at*findserv=1at*findserv=1
OK
REP*:SERVICE START: =3333-33-333333
 = 1 : 1800 : 0001 : 0005
 = 2 : 180a : 0006 : 0016
 = 3 : 00005500d10211e19b2300025b00a5a5 : 0017 : 001a
 = 4 : 180f : 001b : ffff
REP*:SERVICE END: =3333-33-333333
```

v. Considering the above report for services, below are the possible commands.

a. Scan characteristics of single service i.e. 1800 service, handles are 0001 and 0005. Command should be "AT*findchar=1,0001,0005"
b. Scan characteristics for first two services i.e. 1800 and 180a. User shall issue command as "at*findchar=0001,0016".
c. Scan characteristics of all services in single command, user shall issue command "at*findchar=1,0001,ffff".

vi. Report is marked for start and end.
vii. The example report below shows a characteristic scan command report.

```
at*findchar=1,0001,001bat*findchar=1,0001,001b
OK
REP*:CHAR start
 =1: 2a00 : 0003 : 02 : 0002 [ Rd ]
 =2: 2a01 : 0005 : 02 : 0004 [ Rd ]
 =3: 2a25 : 0008 : 02 : 0007 [ Rd ]
 =4: 2a24 : 000a : 02 : 0009 [ Rd ]
 =5: 2a23 : 000c : 02 : 000b [ Rd ]
 =6: 2a27 : 000e : 02 : 000d [ Rd ]
 =7: 2a26 : 0010 : 02 : 000f [ Rd ]
 =8: 2a28 : 0012 : 02 : 0011 [ Rd ]
 =9: 2a29 : 0014 : 02 : 0013 [ Rd ]
 =10: 2a50 : 0016 : 02 : 0015 [ Rd ]
 =11: 00005501 : 0019 : 14 : 0018 [ Wr_cmd CCFG ]
REP*:CHAR END
```

viii. For report above, the row "=1: 2a00 : 0003 : 02 : 0002 [Rd]" indicates "1" as serial number, "2a00" as 16 bit characteristic UUID, "0003" is characteristic handle, "02" is properties value and "0002" is declaration value for that characteristic.
ix. For details on Characteristic value and Declaration values refer appendix A.
x. "=11: 00005501 : 0019 : 14 : 0018 [Wr_cmd CCFG]" row indicates the characteristic has 128 bit UUID, but here only lower 32 bits are displayed. "0019" is characteristic handle. "14" is properties value, this characteristic has two properties as WR-cmd and CCFG. "0018" is declaration value for that characteristic.
xi. User needs to use characteristic-Handle to read or write data on that characteristic.

3.7 BLE read data from Characteristic:

3.7.1 "AT*RDCHARVAL"\r\n

i. Execution only command
ii. This command is used to read data from the BLE device for the characteristic which has properties as read "Rd" i.e. 0x02.
iii. The command format is "AT*RDCHARVAL=conn-ID, char-Handle".
iv. e.g. "at*rdcharval=1,0003" command is used to read data from 1st connected device, for characteristic 0003.

v. The module shall output an OK response if the CID and the Char-handle is correct.
vi. After the module gives OK response to read command, module shows data received from remote device as a report.
vii. E.g. "REP*:RDCHARVAL=1:Rcvd_Bytes:0010 LM Serial Server" is a report of read data for characteristic 0003.
viii. Report shows connection ID as 1, Received bytes as 0x10 i.e. 16 bytes, and the actual bytes are "LM Serial Server".
ix. If module receives an error response it is reported to user with the error code.
x. Users can refer to error codes as mentioned in the appendix section.

at*rdcharval=1,000cat*rdcharval=1,000c
OK
REP*:RDCHARVAL=0001:Err_code:02

xi. Below show some reference reports for read command.

at*rdcharval=1,0003at*rdcharval=1,0003
OK
REP*:RDCHARVAL=1:Rcvd_Bytes:0010
LM Serial Server

at*rdcharval=1,0005at*rdcharval=1,0005
OK
REP*:RDCHARVAL=1:Rcvd_Bytes:0002

at*rdcharval=1,000aat*rdcharval=1,000a
OK
REP*:RDCHARVAL=1:Rcvd_Bytes:0016
CSR-GATT-SERVER-MODEL-

at*rdcharval=1,000cat*rdcharval=1,000c
OK
REP*:RDCHARVAL=0001:Err_code:02

xii. Above screenshots are taken on Hercules software on Windows PC, it does not show non-printable characters in received response. If user analyse the RX line on Oscilloscope or protocol analyser, all bytes can be seen.

3.7.2 "AT*RDMULTCHAR"\r\n

i. Execution only command
ii. This command is used to read data from multiple characteristic on single remote device.
iii. Read data from BLE device for the characteristic which has properties as "Rd" i.e. 0x02.
iv. Maximum of 5 characteristic's data can be read in one single command.
v. Command format is "AT*RdMultChar=conn-ID, no-of-chars-to-read, char-Handle1, char-Handle2, char-Handle3, char-Handle4, char-Handle5,".

vi. e.g. command to read data from 3 characteristics shall be “at*rdmultchar=1,03,0008,000a,0010” command is used to read data from 1st connected device, on characteristic 0003, 0008 and 0010.

at*rdcharval=1,0008at*rdcharval=1,0008
OK
REP*:RDCHARVAL=1:Rcvd_Bytes:0005
SR_no

at*rdcharval=1,000aat*rdcharval=1,000a
OK
REP*:RDCHARVAL=1:Rcvd_Bytes:0006
mod_no

at*rdcharval=1,0010at*rdcharval=1,0010
OK
REP*:RDCHARVAL=1:Rcvd_Bytes:0006
FW_Ver

at*rdmultchar=1,03,0008,000a,0010at*rdmultchar=1,03,0008,000a,0010
OK
REP*:RDMULTCHAR=1:Success length:0011
SR_nomod_noFW_Ver

vii. If the read number of bytes from characteristics exceeds than MTU bytes then lower bytes are lost and only first MTU bytes are reported. This is limitation of BLE stack and not of LM961 application.

viii. E.g. refer below response. (last bytes form 0003 characteristic are lost while reading multiple characteristics in one command)

at*rdcharval=1,0008at*rdcharval=1,0008
OK
REP*:RDCHARVAL=1:Rcvd_Bytes:0005
SR_no

at*rdcharval=1,000aat*rdcharval=1,000a
OK
REP*:RDCHARVAL=1:Rcvd_Bytes:0006
mod_no

at*rdcharval=1,0010at*rdcharval=1,0010
OK
REP*:RDCHARVAL=1:Rcvd_Bytes:0006
FW_Ver

at*rdcharval=1,0012at*rdcharval=1,0012
OK
REP*:RDCHARVAL=1:Rcvd_Bytes:0007
App_ver

at*rdcharval=1,000eat*rdcharval=1,000e
OK
REP*:RDCHARVAL=1:Rcvd_Bytes:000b

CSR101x A05

at*rdmultchar=1,05,0008,000a,0010,0012,000eat*rdmultchar=1,
05,0008,000a,0010,0012,000e
OK
REP*:RDMULTCHAR=1:Success length:0016
SR_nomod_noFW_VerApp_v

ix. Above screen shots are taken on Hercules software on Windows PC, it does not show non printable characters in received response. If user analyse the RX line on Oscilloscope or protocol analyser, all bytes can be seen.

3.7.3 "AT*RDLONGCHAR"\r\n

i. Execution only command
ii. When the Characteristic Value is longer than can be sent in a single Read Response message, user can use this command to read that value in one command.
iii. Read data from BLE device for the characteristic which has properties as "Rd" i.e. 0x02.
iv. Command format is "AT*RdLongChar=conn-ID, char-Handle".
v. Commands which support "rdcharval" can also be read by this command.
vi. Response to the command shows bytes received, offset of current data with respect to the whole data, and MoreToCome (MTC) flag if there is next data packet expected on the same characteristic read.
vii. Refer following read examples for more detail.

at*leconn=333333333333at*leconn=333333333333
OK
REP*:BLE_CONNECTED:=3333-33-333333-0 : 1 : 0100 : 0017 :
0008
BLE Auth start
OK
REP*:SERVICE START: =3333-33-333333
= 1 : 1800 : 0001 : 0005
= 2 : 180a : 0006 : 0016
= 3 : 00005500d10211e19b2300025b00a5a5 : 0017 : 001a
= 4 : 180f : 001b : ffff
REP*:SERVICE END: =3333-33-333333

at*rdlongchar=1,0008at*rdlongchar=1,0008
OK
REP*:RDLONGCHAR=1:0008:Success Rcvd:0005 Offset:0000
MTC:0
SR_no

at*rdlongchar=1,000aat*rdlongchar=1,000a
OK
REP*:RDLONGCHAR=1:000a:Success Rcvd:0024 Offset:0000
MTC:0
abcdEFGHIJklmnopQRSTUvwxyz0123abcdEF

at*rdlongchar=1,000cat*rdlongchar=1,000c
OK
REP*:RDLONGCHAR=1 Err_code:0002

at*rdlongchar=1,0005at*rdlongchar=1,0005
OK
REP*:RDLONGCHAR=1:0005:Success Rcvd:0002 Offset:0000
MTC:0

at*rdlongchar=1,0003at*rdlongchar=1,0003
OK
REP*:RDLONGCHAR=1:0003:Success Rcvd:0010 Offset:0000
MTC:0
LM Serial Server

3.8 BLE write data on Characteristic:

3.8.1 "AT*ENBCCFG"\r\n

i. Execution only command.
ii. Command used to enable the Client-Configuration-Flag (CCFG) on specific characteristic.
iii. When the module scans the characteristics of the device, it shows the CCFG flag if supported by that characteristic. E.g Serial-Over-Gatt service supports this flag (highlighted yellow in below report).
iv. While issuing command, user should mention the device-connection-ID and characteristic handle.
v. E.g The device 1 has CCFG flag characteristic with handle 0019. To enable the CCFG flag use command "at*enbccfg=1,0019".
vi. Module shall give OK response if the characteristic has CCFG flag otherwise module shall give ERR response if wrong characteristic handle is mentioned.
vii. After the module responds with "OK", the module receives feedback from the BLE device regarding success or failure, which is reported to the user.
viii. The report "REP*:WRCHARVAL=1:Success" shows enable CCFG operation is performed successfully.

at*findchar=1,0001,001bat*findchar=1,0001,001b
OK
REP*:CHAR start
=1: 2a00 : 0003 : 02 : 0002 [Rd]
=2: 2a01 : 0005 : 02 : 0004 [Rd]
=3: 2a25 : 0008 : 02 : 0007 [Rd]
=4: 2a24 : 000a : 02 : 0009 [Rd]
=5: 2a23 : 000c : 02 : 000b [Rd]
=6: 2a27 : 000e : 02 : 000d [Rd]
=7: 2a26 : 0010 : 02 : 000f [Rd]
=8: 2a28 : 0012 : 02 : 0011 [Rd]
=9: 2a29 : 0014 : 02 : 0013 [Rd]

=10: 2a50 : 0016 : 02 : 0015 [Rd]
=11: 00005501 : 0019 : 14 : 0018 [Wr_cmd CCFG]
REP*:CHAR END

at*enbccfg=1,0019at*enbccfg=1,0019
OK
REP*:WRCHARVAL=1:Success

3.8.2 "AT*INDESPr\n

i. Execution only command.
ii. This command gives feedback to server/peripheral for notification indication from server/peripheral.
iii. This command is used to acknowledge the sever that client(BLE-Central) has received characteristic value Indication, and server(BLE-Peripheral) may send another indication.
iv. Command format is "at*INDRESP=Conn-ID".
v. e.g. "AT*INDRESP=1" gives indication response for 1st connected BLE device for receiving notification indication.
vi. OK/ERR response is given by LM961 after checking the Connection ID and Connection status.
vii. After OK response is given Response is forwarded to remote device by BLE-Stack.
viii. No feedback form BLE-Stack is provided to this command.

3.8.3 "AT*WRWORESP"\r\n

i. Execution only command
ii. This command is used to send data to BLE device for the characteristic which has properties as "Wr_cmd" i.e. 0x04.
iii. Command format is "AT*WRWORESP=conn-ID, char-Handle, length, actual-bytes ".
iv. e.g. "at*wrworesp=1,0019,10,12345abcdef!()12" command is used to send data to 1st connected device, on characteristic 0019. No of bytes to write are 0x10 i.e. 16 and actual bytes are 1,2,3,4,5,a,b,c,d,e,f,!,(,),1,2.
v. As shown in the example command number of bytes to transmit is hex value.
vi. As shown in the example command, actual data bytes are not separated by a comma. When the value 0x31 is sent i.e. ASCII 1 is sent, the data buffer is copied and sent to remote device transparently.
vii. **Note :** The actual data bytes to be sent shall not have "\r\n" as the data itself because it is the terminating string for AT command parser.

viii. For command "AT*WRWORESP=conn-ID, char-Handle, length, actual-bytes" module gives OK response if all the following conditions are true:
   a. connection ID is correct (if module is connected to 3 devices and CID mentions 4, then it is invalid)
   b. Characteristic handle has WR_cmd properties
   c. Value of "length" field is less than 21 i.e. (0x15).
   d. Actual data bytes are same as value of "length" field.

ix. After the module responds to the command with "OK", the module sends the data to the remote BLE device.
x. If the remote device receives the data and sends feedback to the LM961, that feedback is displayed on UART.
xi. E.g. report shows, "REP*:WRWORESP=1:0019:Success" which indicates the data has been received by the remote device successfully. 1 is the CID-given by module and 0019 is the characteristic handle.

```
at*wrworesp=1,0019,05,12345at*wrworesp=1,0019,05,12345
OK
REP*:WRWORESP=1:0019:Success
at*wrworesp=1,0019,10,12345abcdef!()12at*wrworesp=1,0019,10,1
2345abcdef!()12
OK
REP*:WRWORESP=1:0019:Success
```

3.8.4 "AT*WRCHARVAL"\r\n

i. Execution only command
ii. This command is used to send data to BLE device for the characteristic which has properties as "Wr_req" i.e. 0x08.
iii. Command format is "AT*WRCHARVAL=conn-ID, char-Handle, length, actual-bytes".
iv. e.g. "at*WRCHARVAL=1,0019,10,12345abcdef!()12" command is used to send data to 1st connected device, on characteristic 0019. No of bytes to write are 16 (0x10) and actual bytes are 12345abcdef!()12.
v. As shown in the example command, no of bytes to transmit is hex value
vi. As shown in the example command, actual data bytes are not separated by comma. When the value 0x31 is sent i.e. ASCII 1 is sent, the data buffer is copied and sent to remote device transparently.
vii. **Note :** The actual data bytes to be sent should not have "\r\n" as the data itself because it is the terminating string for AT command parser.
viii. For command "AT*WRWORESP=conn-ID, char-Handle, length, actual-bytes" module gives OK response if all the following conditions are true:
   a. connection ID is correct (if module is connected to 3 devices and CID mentions 4, then it is invalid)

b. Characteristic handle has Wr_req properties
c. Value of “length” field is less than 21 i.e. (0x15).
d. Actual data bytes are same as value of “length” field.

ix. After module responds to this command as “OK”, module sends the data to remote BLE device.

```
at*findchar=2,0001,ffffat*findchar=2,0001,ffff
OK
REP*:CHAR start
 =1: 2a05 : 0003 : 20 : 0002
[ Indi ]
 =2: 2a00 : 0007 : 0a : 0006
[ Rd Wr_req ]
 =3: 2a01 : 0009 : 02 : 0008
[ Rd ]
 =4: 2a04 : 000b : 02 : 000a
[ Rd ]
 =5: 2a37 : 000e : 10 : 000d
[ CCFG ]
 =6: 2a38 : 0011 : 02 : 0010
[ Rd ]
 =7: 2a39 : 0013 : 08 : 0012
[ Wr_req ]
 =8: 2a19 : 0016 : 12 : 0015
[ Rd CCFG ]
 =9: 00001013 : 001a : 0a : 0019
[ Rd Wr_req ]
 =10: 00001018 : 001c : 08 : 001b
[ Wr_req ]
REP*:CHAR END

at*wrcharval=2,0013,05,12345at*wrcharval=2,0013,05,12345
OK
REP*:WRCHARVAL=2:Err_code:fd
at*wrcharval=2,0007,05,12345at*wrcharval=2,0007,05,12345
OK
REP*:WRCHARVAL=2:Success

at*wrcharval=2,0007,05,abCDEat*wrcharval=2,0007,05,abCDE
OK
REP*:WRCHARVAL=2:Success
at*wrcharval=2,001c,05,abCDEat*wrcharval=2,001c,05,abCDE
OK
REP*:WRCHARVAL=2:Err_code:0d
at*wrcharval=2,001a,05,abCDEat*wrcharval=2,001a,05,abCDE
OK
REP*:WRCHARVAL=2:Err_code:0e
at*wrcharval=2,0013,05,abCDEat*wrcharval=2,0013,05,abCDE
OK
REP*:WRCHARVAL=2:Err_code:fd
```

x. If the remote device receives the data and sends feedback to the LM961, that feedback is displayed on UART.

xi. Above report shows the WRCharval command is successful only on characteristic 0005 and 0007.
xii. If the WrCharVal command fails in execution, then the error code reported by BLE-stack is reported to user in failure report. E.g. Err_code:fd , Err_code:0e, Err_code:0d
xiii. Refer Appendix section for more details on error code.

3.8.5 "AT*SIWRWORESP"\r\n

i. Execution only command
ii. This command is used to send data to BLE device for the characteristic which has properties as "Si_Wrt" i.e. 0x40.
iii. Command format is "AT*WRCHARVAL=conn-ID, char-Handle, length, actual-bytes".
iv. e.g. "at*WRCHARVAL=1,0019,10,12345abcdef!()12" command is used to send data to 1st connected device, on characteristic 0019. No of bytes to write are 16 (0x10) and actual bytes are 12345abcdef!()12.
v. As shown in the example command, no of bytes to transmit is hex value
vi. As shown in the example command, actual data bytes are not separated by comma. When the value 0x31 is sent i.e. ASCII 1 is sent, the data buffer is copied and sent to remote device transparently.
vii. Note : The actual data bytes to be sent should not have "\r\n" as the data itself because it is the terminating string for AT command parser.
viii. For command "AT*WRWORESP=conn-ID, char-Handle, length, actual-bytes" module gives OK response if all the following conditions are true:

    a. connection ID is correct (if module is connected to 3 devices and CID mentions 4, then it is invalid)
    b. Characteristic handle has Wr_req properties
    c. Value of "length" field is less than 21 i.e. (0x15).
    d. Actual data bytes are same as value of "length" field.

ix. After module responds to this command as OK, module sends the data to remote BLE device.

3.8.6 NOTIF_IND notification Indication

i. Indication given by module.
ii. When the module receives data from the remote BLE device, it notifies the user on UART.
iii. E.g. the command below shows some indication reports:

```
IND*:NOTIF_IND=1:0019 R_bytes:0014
dataFromBLEDev123456
```

IND*:NOTIF_IND=1:0019 R_bytes:0003
789

IND*:NOTIF_IND=1:0019 R_bytes:0014
abcdefghijklmnopqrst

IND*:NOTIF_IND=1:0019 R_bytes:0006
uvwxyz

IND*:NOTIF_IND=1:0019 R_bytes:0014
abcdefghijklmnopqrst

IND*:NOTIF_IND=1:0019 R_bytes:0006
uvwxyz

iv. In report "IND*:NOTIF_IND=1:0019 R_bytes:0014 dataFromBLEDev123456" the module shows CID as 1, Characteristic from which data is received is 0x0019, the actual received bytes are 0x0014, and then the actual bytes as "dataFromBLEDev123456".
v. The module can receive a maximum of 20 bytes i.e. 0x14 bytes in one notification packet.
vi. If the remote device sends more than 20 bytes in one packet then the module shows two notification indication messages. E.g. if the remote device sends the string "dataFromBLEDev123456789", the module shows "dataFromBLEDev123456" first and then "789".

4. LM961 AT commands and Default configuration

This section describes the AT command structure for the LM961 module.

Serial terminals (such as Hercules, HyperTerminal, Tera Term or Putty) can be used for serial communication with the LM961.

Every command is terminated with “CR-LF”. T parsing the AT command strings after receiving “CR-LF” sequence.

AT Commands are case insensitive e.g. “At*Resp=On”, “at*resp=on” and “AT*RESP=ON” are all valid.

Following are the AT command types:

1. Query only commands - Commands to query Module state, firmware version number etc.
2. Query and Set commands - Commands to query the setting and modify Module setting e.g. discoverability, Role, Baud, etc.
3. Execution only command – commands to perform specific action e.g. start discovery for Bluetooth devices, start connection procedure, start upgrade procedure etc.

The LM961 outputs indication messages to the user through the serial port for indications like connection/pairing request, result of connection/pair procedure, result of Bluetooth devices discovery, disconnection indication etc.

After the indication message is displayed, the LM961 waits for inputs from the user to execute further action. For example, after incoming pairing indications, enter accept/reject pair response or after indication for PASSKEY_cfm, provide yes/no confirmation for the passkey etc.

The module responds to each AT command as “OK”\r\n or “ERR”\r\n. After this response the module takes requested action or it will output report to the user on UART. If module does not receive “AT” as a start of new command, the module may not respond to this command even if it is terminated with “\r\n” (e.g. instead of “AT*NAME=?”, user issues “A*name=?”). Module will neglect the received string and is ready to receive new AT command and to process it.

When the module does not receive any command on UART for more than 30 seconds, the module enters deep sleep mode. The module can come out of this mode on UART activity or BT activity. If the user enters AT commands while the module is in deep sleep, the module may lose the first character of an AT command, e.g. for command “AT*NAME=?”, module may show the echo as “t*name=?” or “Ñname=?” i.e. some garbage character at start. The module will not respond to AT commands such as ERR/OK, but it ignores this data and waits for a new AT command to process.

AT commands expects the BT address in the string. In this document “0126f357215” is considered a reference BT address, whereas 0012 is nap, 6f is

uap and 357215 is lap in the BT address. Users should use the BT address of their devices.

4.1 AT commands

The table below shows all the AT commands that are supported on the LM961 module and the default settings wherever applicable for quick reference.

4.1.1 General settings AT commands:

Sr no	AT command string	Command type	Default setting
1	AT*ADDR	Query only	--
2	AT*NAME	Query and set	Firmware version dependent e.g. 068LM_SPP_0104
3	AT*ECHO	Query and set	ON
4	AT*RESP	Query and set	ON
5	AT*DCOV	Query and set	ON
6	AT*PAIR	Query and set	ON
7	AT*STATE	Query only	--
8	AT*VER	Query only	--
9	AT*RESET	Execution only	--
10	AT*SETTINGS	Query only	Refer command details

4.1.2 UART settings AT commands:

Sr no	AT command string	Command type	Default setting
1	AT*BAUD	Query and set	19200 (5)
2	AT*PAR	Query and set	No parity (0)
3	AT*STOP	Query and set	One stop bit (0)
4	AT*FLOW	Query and set	Off
5	AT*CTS	Query only	--
6	AT*RTS	Set only	--
7	AT*DTR	Set only	--
8	AT*DSR	Query only	--
9	AT*MODEM	Query and set	NONE

Note: CTS, RTS, DTR, DSR, MODEM commands are not applicable for LM961 module.

4.1.3 Bluetooth security settings commands:

Sr no	AT command string	Command type	Default setting
1	AT*PIN	Query and set	1234
2	AT*DPIN	Query and set	OFF
3	AT*MITM	Query and set	OFF
4	AT*IOTYPE	Query and set	NO_InOut
5	AT*DEL	Execution only	--
6	AT*PASSKEY	Execution only	--
7	AT*PASSCFM	Execution only	--
8	AT*STOPPAIR	Execution only	--
9	AT*PAIRLIST	Query only	--

4.1.4 SPP related AT commands:

Sr no	AT command string	Command type	Default setting
1	AT*FIND	Execution only	--
2	AT*ROLE	Query and set	Dual
3	AT*ACON	Query and set	OFF
4	AT*CONN	Execution only	--
5	Escape sequence “+++”	Execution only	--
6	AT*AUTO	Execution only	--
7	AT*DROP	Execution only	--
8	AT*BOND	Query and set	Default bond device address = 0000-00-000000

4.1.5 Firmware Upgrade AT commands:

Sr no	AT command string	Command type	Default setting
1	AT*UPGRADE	Execution only	--

4.2 Module Settings commands:

4.2.1 "AT*ADDR"\r\n

i. Query only command
ii. Address query: "AT*ADDR=?"\r\n
iii. Address query report: "REP*:ADDR=00025b00a5a5"

4.2.2 "AT*NAME"\r\n

i. Query and set command
ii. Name query: "AT*NAME=?"\r\n
iii. Name query report: "REP*:NAME=LM961_2_Default"
iv. Name set command: "AT*NAME=testname"
v. Default name: (Depends on firmware version number)

4.2.3 "AT*ECHO"\r\n

i. Query and set command
ii. Echo query: "AT*ECHO=?"\r\n
iii. Echo query report: "REP*:ECHO=ON" or "REP*:ECHO=OFF"
iv. Echo enable command: "AT*echo=on"
v. Echo disable command: "AT*echo=off"
vi. Default Echo: "ON"

4.2.4 "AT*RESP"\r\n

i. Query and set command
ii. Response query: "AT*RESP=?"\r\n
iii. Response query report: "REP*:RESP=ON" or "REP*:RESP=OFF"
iv. Response enable command: "AT*RESP=on"
v. Response disable command: "AT*RESP=off"
vi. Default Response: "ON"
vii. When response is ON, the module responds as "OK" or "ERR" to every command string before sending report/response of the command.
viii. When response is OFF, the module will not provide "OK" or "ERR" reply to any AT command. This might not be helpful to users as the user will not get any response if incorrect AT command strings are entered.
ix. Below is the sequence of messages when ECHO and RESP are ON.

```
at*echo=?at*echo=?
OK
REP*:ECHO=ON
at*resp=?at*resp=?
OK
REP*:RESP=ON
at*name=?at*name=?
OK
REP*:NAME=068LM_SPP_0104
```

x. Below is the sequence of messages when ECHO is OFF and RESP is ON.

```
at*echo=offat*echo=off
OK
at*echo=?OK
REP*:ECHO=OFF
at*resp=?OK
REP*:RESP=ON
at*name=?OK
REP*:NAME=068LM_SPP_0104
```

xi. Below is the sequence of messages when ECHO and RESP are both off. The module will show only reports for the query commands. The module will not show any indication messages for connect or disconnect. This is to ensure backwards compatibility with LM048/LM058/LM072 module firmware.

```
at*resp=?REP*:RESP=OFF
at*echo=?REP*:ECHO=OFF
at*name=?REP*:NAME=068LM_SPP_0104
```

4.2.5 "AT*DCOV"\r\n

i. Query and set command
ii. Discoverable query: "AT*DCOV=?"\r\n
iii. Discoverable query report: "REP*:DCOV=ON" (Module discoverable for classic role) or "REP*:DCOV=OFF" (Module non discoverable for classic role)
iv. Module make discoverable command: "AT*DCOV=ON"
v. Module make non-discoverable command: "AT*DCOV=OFF"
vi. Default discoverability : "ON"
vii. Enabling discoverability may generate further events of incoming pairing/connection requests.

4.2.6 "AT*PAIR"\r\n

i. Query and set command
ii. Pairable query: "AT*PAIR=?"\r\n
iii. Pairable query report: "REP*:PAIR=ON" (Module is in pairable state and will give indications to host of any incoming pairing requests)
iv. Pairable query report: "REP*:PAIR=OFF" (Module is in non-pairable state will reject pairing request internally)
v. Module make pairable command: "AT*PAIR=ON"
vi. Module make non-pairable command: "AT*PAIR=OFF"
vii. Default Pairable: ON
viii. Enabling pair-ability may generate further events of incoming pairing/connection requests.
ix. Module displays the message "IND*:PAIR=00126f357215" to indicate that the device with BT-address 00126f357215 is requesting to pair.
x. To accept the pairing request the user should respond as "AT*PAIR=00126f357215,accept"\r\n.

xi. To reject the pairing request user should respond as "AT*PAIR=00126f357215,reject"\r\n.
xii. After pairing procedure is complete, module shows indication message for success or failure of pairing "IND*:PAIR=OK,00126f357215" or "IND*:PAIR=ERR,00126f357215" .

4.2.7 "AT*STATE"\r\n

i. Query only command
ii. Module state query: "AT*STATE=?"\r\n
iii. Module state query report: "REP*:STATE-DP=ON,ON" ("STATE-DP" indicates states as D-discoverable is ON and P-Pairable is ON)
iv. Module state query report: "REP*:STATE-DP=ON,OFF" ("STATE-DP" indicates states as D-discoverable is ON and P-Pairable is OFF)

4.2.8 "AT*VER"\r\n

i. Query only command
ii. Firmware version query: "AT*VER=?"\r\n
iii. Firmware version query report: "REP*:VER=961LM_GAPCEN_01.02" (current firmware version major number 1, minor number 04) string "961LM_GAPCEN" shows it is firmware on LM068 device with SPP profile.

4.2.9 "AT*RESET"\r\n

i. Execution only command, LM951/LM961 supports execution of two "Reset" levels
ii. "AT*RESET=1"\r\n
    1. Module applies soft reset, starts execution as if applied power on-off.
    2. Retains all user modified settings
    3. Causes disconnection for Bluetooth connections

iii. "AT*RESET=2"\r\n
    4. Module applies hard reset
    5. Loads default settings for all setting types
    6. Causes disconnection for Bluetooth connections
    7. Deletes all the paired devices and corresponding data

4.2.10 "AT*SETTINGS"\r\n

i. Query only command
ii. Module settings query: "AT*SETTINGS=?"\r\n
iii. Report for "AT*SETTINGS=?" command is multiple line, at the end of the report a message "REP*:SETTINGS=END" is delivered.
iv. Module settings query report varies according to DPIN setting. If DPIN is OFF i.e. supporting to BT2.0, Module PIN is displayed. If

DPI is ON, i.e. support to BT2.1, then settings for IO-capability, MITM are displayed.

"AT*Settings" report when DPIN is OFF	**"AT*Settings" report when DPIN is ON**
at*settings=?at*settings=? OK NAME=LM961_SPP+GAPCEN_0102 ADDR=0002-5b-00a5a5 PAIR=ON DCOV=ON BAUD=19200(2) STOP=Stop_One(0) PARITY=None(0) FLOW=OFF SPPRole=SLAVE ACON=OFF BOND=0000-00-000000 DPIN=OFF PIN=1234 GAP_ENABLE=OFF VER=961LM_GAPCEN_01.01 REP*:SETTINGS=END OR at*settings=?at*settings=? OK NAME=LM961_SPP+GAPCEN_0102 ADDR=0002-5b-00a5a5 PAIR=ON DCOV=ON BAUD=19200(2) STOP=Stop_One(0) PARITY=None(0) FLOW=OFF SPPRole=SLAVE ACON=OFF BOND=0000-00-000000 DPIN=OFF PIN=1234 GAP_ENABLE=ON LE_SEC=OFF LE_AUTO_SCAN=ON VER=961LM_GAPCEN_01.02 REP*:SETTINGS=END	at*settings=?at*settings=? OK NAME=LM961_SPP+GAPCEN_0102 ADDR=0002-5b-00a5a5 PAIR=ON DCOV=ON BAUD=19200(2) STOP=Stop_One(0) PARITY=None(0) FLOW=OFF SPPRole=SLAVE ACON=OFF BOND=0000-00-000000 DPIN=ON MITM=OFF IOTYPE=NO_InOut GAP_ENABLE=OFF VER=961LM_GAPCEN_01.01 REP*:SETTINGS=END OR at*settings=?at*settings=? OK NAME=LM961_SPP+GAPCEN_0102 ADDR=0002-5b-00a5a5 PAIR=ON DCOV=ON BAUD=19200(2) STOP=Stop_One(0) PARITY=None(0) FLOW=OFF SPPRole=SLAVE ACON=OFF BOND=0000-00-000000 DPIN=ON MITM=OFF IOTYPE=NO_InOut GAP_ENABLE=ON LE_SEC=OFF LE_AUTO_SCAN=ON VER=961LM_GAPCEN_01.02 REP*:SETTINGS=END

v. Also, Module response depends on ENBGAP settings. Refer section 1.2 "Enable GAP Central role" for more details.