



BTM410/411 DATA MODULE

User Guide

Version 6.1



global solutions: local support™

Embedded Wireless Solutions Support Center: <http://ews-support.lairdtech.com>

Americas: +1-800-492-2320

Europe: +44-1628-858-940

Asia: +852-2923-0610

www.lairdtech.com/bluetooth

REVISION HISTORY

Revision	Date	Description	Approved By
1.0	1 Mar 2012	Initial Release	Jonathan Kaye
2.0	12 Mar 2012	General updates and compliant with firmware v16.1.3.0	Jonathan Kaye
3.0	13 Apr 2012	Reformatting and general edits	Jonathan Kaye
4.0	15 Aug 2012	Reformatting. Addition of Table 2-6. Reference to Table 2-6 in Table 2-1. Update to Sniff Mode section (everything following Figure 5). Cross References. Updated ATI Commands table. Added links to Low Power and Absolute Current Ratings application notes.	Jonathan Kaye
5.0	21 Mar 2013	Updated mechanical drawings, updated FCC statements, general formatting edits.	Jonathan Kaye
6.0	16 Jan 2014	Separated document into two documents: Hardware Integration Guide and User Guide	Jonathan Kaye
6.1	4 Sept 2014	Added sniff register mapping section and AT commands for persistent storing	Jonathan Kaye

TABLE OF CONTENTS

Revision History.....	2
Table of Contents	3
1. Overview and Key Features	4
Features and Benefits	4
Applications	4
2. AT Command Set Reference	5
2.1 Introduction	5
2.2 Glossary of Terms	5
2.3 Overview of the BTM Product Family.....	7
2.4 BTM - AT Command Set	7
2.5 General AT Commands.....	8
2.6 AT Commands for S Registers.....	11
2.7 General S Registers	13
2.8 AT Commands for Inquiry	13
2.9 AT Commands for Extended Inquiry Response Data	16
2.10 Persistent Store	19
2.11 Secure Simple Pairing (SSP)	20
2.12 AT Commands for Legacy Pairing	24
2.13 AT Commands Managing Trusted Devices	25
2.14 AT Commands for Serial Stream Oriented Profiles (SSO)	26
2.15 AT Commands for a Selected Peer Device	29
2.16 Bluetooth Profiles.....	31
2.17 Hardware Units (BTM410 / 411).....	36
2.18 Miscellaneous	39
3. Appendix.....	50
3.1 S Registers	50
3.2 ATI Commands	61
3.3 Error Responses	64
3.4 List of UUIDs	66
3.5 References	68
4. Related Documents and Files	69

1. OVERVIEW AND KEY FEATURES

The BTM410 and BTM411 Bluetooth® modules from Laird are designed to meet the needs of developers who wish to add robust, short range Bluetooth data connectivity to their products. These modules are based on the market leading Cambridge Silicon Radio BC04 chipset, providing exceptionally low power consumption with outstanding range. They support the Bluetooth® version 2.1 specification, providing the important advantage of Secure Simple Pairing (SSP), which improves security and ease of use for end customers.

With physical sizes as small as 12.5 mm x 18.0 mm and best of class, low-power operation, these modules are the ideal choice for applications where designers need both performance and minimum size. For maximum flexibility in systems integration, the modules are designed to support a separate power supply for I/O.

To aid product development and integration, Laird has integrated a complete Bluetooth protocol stack within the modules, including support for the Bluetooth Serial Port Profile. The modules are fully qualified as Bluetooth End Products, allowing designers to integrate them within their own products with no further Bluetooth Qualification. They can then list and promote products on the Bluetooth website free of charge.

A comprehensive AT command interface is included, which simplifies firmware integration. Combined with a low cost developer's kit, choosing Laird Bluetooth modules guarantees the fastest route to market.

Features and Benefits



- Bluetooth® v2.1+EDR
- Adaptive Frequency Hopping to handle interference from other wireless devices
- Secure Simple Pairing (SSP) support
- External or internal antenna options
- Comprehensive AT interface for simple programming
- Bluetooth® End Product Qualified
- Compact size
- Class 2 output – 4 dBm
- Low power operation
- UART interface
- PCM and SCO for external codec
- GPIO lines under AT control
- Wi-Fi co-existence

Applications

- Embedded devices
- Phone accessories
- Security devices
- Medical and wellness devices
- Automotive applications
- Bluetooth advertising
- ePOS

2. AT COMMAND SET REFERENCE

2.1 Introduction

This section describes the protocol used to control and configure the BTM Bluetooth device.

The protocol is similar to the industry standard Hayes AT protocol used in telephony modems which is appropriate for cable replacement scenarios, as both types of devices are connection oriented.

Just like telephony modems, Laird's devices power up in an unconnected state and only respond via the serial interface. In this state the device does not even respond to Bluetooth inquiries. Then, just like controlling a modem, the host can issue AT commands which map to various Bluetooth activities. The configuration of the device can be saved, so that on a subsequent power up the device is discoverable or automatically connects.

The device has a serial interface which can be configured for baud rates from 1200 up to 921600 (default setting is 9600) and an RF communications end point. The latter has a concept of connected and unconnected modes and the former has a concept of command and data modes. This leads to the matrix of states shown below.

Table 2-1: Mode RF connections

	RF Unconnected	RF Connected
Local Command Mode	OK	OK
Remote Command Mode	ILLEGAL	OK
Data Mode	ILLEGAL	OK

The combinations 'Data and RF Unconnected Mode' and 'Remote Command and RF Unconnected Mode' do not make sense and are ignored.

Navigation between these states is done using the AT commands which are described in detail in subsequent sections.

2.2 Glossary of Terms

Table 2-2: Glossary of Terms

Term	Description
A2DP	: Advanced Audio Distribution Profile
ACL	: Asynchronous Connection-Oriented Link
ADC	: Analogue to Digital Converter
AGHFP	: Audio Gateway Hands-Free Profile
AT	: Command prefix, 'Attention'
AVRCP	: Audio/Video Remote Control Profile
BISM	: Bluetooth Intelligent Serial Module
CoD	: Class of Device (also referred to as "device class")
Codec	: Device capable of encoding / decoding an analogue / digital signal
DAC	: Digital to Analogue Converter
DSP	: Digital Signal Processor

Term	Description
DUN	: Dial-Up Network Profile
EIR	: Extended Inquiry Response
eSCO	: Enhanced Synchronous Connection Oriented Link (used for Audio)
FTP	: File Transfer Profile
GOEP	: Generic Object Access Exchange Profile
GPIO	: General Purpose Input Output
HF	: Hands-free Role of Hands-free Profile ("Hands-free Unit")
HFG	: Audio Gateway Role of Hands-free Profile ("Hands-free Gateway")
HFP	: Hands Free Profile
HID	: Human Interface Device Profile
HS	: Headset Role of Headset Profile ("Headset")
HSG	: Audio Gateway Role of Headset Profile ("Headset Gateway")
HSP	: Headset Profile
I/O (IO)	: Input/Output
Mic	: Microphone
MITM	: Man In The Middle
OPP	: Object Push Profile
PBAP	: Phone Book Access Profile
PT	: PASS THROUGH Command
PWM	: Pulse Width Modulation
SBC	: Sub Band Codec
SCO	: Synchronous Connection Oriented Link (used for Audio)
SLC	: Service Level Connection
SPP	: Serial Port Profile
SSO	: Serial Stream Oriented
SSP	: Secure Simple Pairing
SUI	: SUBUNIT INFO Command
Sxxx	: S-Register No. xxx
TDL	: Trusted Device List
UART	: Universal Asynchronous Receiver / Transmitter
UI	: UNIT INFO Command

2.3 Overview of the BTM Product Family

Table 2-3: BTM 410 and 411 products

Chipset	CSR BC4-Ext
Bluetooth version	2.1
Features	SSP, EIR, SCO ⁽¹⁾ , eSCO ⁽¹⁾
Profiles	SPP

(1) External codec required

Table 2-4: BTM 510 and 511 products

Chipset	CSR BC5MM-Ext
Bluetooth version	2.1
Features	SSP, EIR, SCO, eSCO
Profiles	SPP, A2DP, AVRCP, HSP, HFP, DUN(DT)

Table 2-5: BTM 520 and 521 products

Chipset	CSR BC5MM-Ext
Bluetooth version	2.1
Features	SSP, EIR, SCO, eSCO
Profiles	SPP, A2DP, AVRCP, HSP, HFP, DUN(DT)

2.4 BTM - AT Command Set

This section describes the AT Command Set for a BTM module. This section is structured in functional groups of AT commands related to module configuration, Bluetooth profiles, hardware units, and miscellaneous purposes.

2.4.1 Assumptions

All commands terminate by the carriage return character 0x0D, which is represented by the string <cr> in descriptions below; this cannot be changed.

All responses from the BTM device have carriage return and linefeed characters that precede and append the response. These dual character sequences have the values 0x0D and 0x0A respectively and shall be represented by the string <cr,lf>.

All Bluetooth addresses are represented by a fixed 12 digit hexadecimal string, case insensitive.

All Bluetooth Device Class codes are represented by a fixed 6 digit hexadecimal string, case insensitive.

All profile specific commands are identified by the prefix shown in [Table 2-6](#).

Table 2-6: AT command prefix for profiles

Profile	Term	AT-Command Prefix
Serial Port Profile	SPP	AT+SP...

2.4.2 Command Syntax

The following syntax is employed throughout this document to describe optional or mandatory parameters for AT commands.

<bd_addr>	A 12 character Bluetooth address consisting of ASCII characters '0' to '9', 'A' to 'F' and 'a' to 'f'.
<devclass>	A 6 character Bluetooth device class consisting of ASCII characters '0' to '9', 'A' to 'F' and 'a' to 'f'.
N	A positive integer value.
M	An integer value which could be positive or negative, which can be entered as a decimal value or in hexadecimal if preceded by the '\$' character. E.g. the value 1234 can also be entered as \$4D2
<string>	A string delimited by double quotes. E.g. "Hello World". The " character MUST be supplied as delimiters.
<uuid>	A four-character UUID number consisting of ASCII characters '0' to '9', 'A' to 'F' and 'a' to 'f'.

2.5 General AT Commands

2.5.1 AT

This command checks whether or not the module is available.

Response: <cr,lf>OK<cr,lf>

2.5.2 ATEn {Enable/Disable Echo}

This command enables or disables the echo of characters to the screen. A valid parameter value writes to S Register 506.

E0 Disable echo.

E1 Enable echo.

All other values of n generate an error.

Response: <cr,lf>OK<cr,lf>

Or <cr,lf>ERROR nn<cr,lf>

2.5.3 ATZ<n> {Hardware Reset and emerge into boot mode 'n'}

Forces the device through a hardware reset which means it eventually comes alive in the local command and unconnected mode. This allows changes to the non-volatile memory to take effect. The module issues an OK response after the reset completes and it is ready to receive commands once again.

ATZ and ATZ0 signify reset and emerge into the current boot mode (see command AT114 in [Table 3-2](#)). ATZ1 to ATZ4 instructs the module to reset and emerge into the appropriate boot mode. Note that S Register 103 specifies the boot mode from cold.

Boot modes are required to configure some low level device settings which cannot be configured by S registers and AT commands. Currently there are predefined settings defining the PCM data format to be used with certain codec ICs (applies mainly to BC04).

Response (after reset): <cr,lf>OK<cr,lf>

2.5.4 AT+BTC<devclasshex> {Set Device Class Code Temporarily}

This command sets the device class code which is sent in subsequent inquiry responses. It can be read back using the [AT+BTC?](#) {Read Device Class Code} command.

<devclass> is a six digit hexadecimal number derived as per “Bluetooth Assigned Numbers” [3].

The 24 bits are made of four fields briefly described as follows (bit 0 corresponds to the least significant bit):

Bits 0-1:	Format Type. This field currently only has a value of 00 (i.e. format type 1).
Bits 2-7:	Minor Device Class: The value of these 6 bits is interpreted differently based on the Major Device Class stored in the next 5 bits.
Bits 8-12:	Major Device Class: 5 bits, refer to Figure 1 and Table 3 in “Bluetooth Assigned Numbers” [3].
Bits 13-23:	Major Service Class: 11 bit field, used as a mask to define service classes, refer to Figure 1 and Table 2 in “Bluetooth Assigned Numbers” [3].

Laird devices do not map to any predefined Major Service Class or Major Device Class and so the default devclass as shipped is 001F00, which means no Major Service Class and “Unclassified” Major Device class.

Other examples of device class codes are displayed in [Table 2-7](#).

Table 2-7: Device class codes

Code (Hexadecimal)	Name	Major Service	Major Device	Minor Device
0x001F00	Unclassified	None	Unclassified	n/a
0x200404	Headset	Audio	Audio	Headset

There is a tool available on the Internet for creating a particular device class code: refer to [Reference \[4\]](#). A device class set by AT+BTC becomes visible immediately but is on the next power cycle.

Response: <cr,
>OK<cr,
>

Or for an invalid <devclass> value (usually a value which is not six hexadecimal characters long):

Response: <cr,
>ERROR 08<cr,
>

2.5.5 AT5515=<devclasshex> {Set Device Class Code Permanently}

S Register 515 sets the device class code permanently. Use AT&W to save the setting to non-volatile memory. The new value becomes visible on the next power cycle which can be initiated by ATZ. Refer to [Section 3](#) for more information about the device class code.

Response: <cr,
>OK<cr,
>

2.5.6 AT+BTC? {Read Device Class Code}

This command reads the current device class code.

Response: <cr,
>123456
<cr,
>OK<cr,
>

2.5.7 AT+BTF="<string>" {Set Friendly Name Temporarily}

This sets the friendly name of this device as seen by other devices. The new name becomes immediately visible. Any name set by this command is lost on the next power cycle.

Please refer to S register 593 in [Table 3-1](#) for more information.

Response: <cr,lf>OK<cr,lf>

2.5.8 AT+BTN="<string>" {Set Friendly Name Permanently}

This sets the default friendly name of this device as seen by other devices. It is stored in non-volatile memory. The new name becomes visible to other devices on the next power cycle. Use AT+BTF to make the name visible immediately. Use AT+BTN? to read it back. An empty string ("") deletes the string from non-volatile memory which forces the default name (Laird BTM 789012) to be used.

The digits in the default friendly name represent the last six digits of the local Bluetooth address.

Please refer to S register 593 in [Table 3-1](#). If a new value of S593 needs to be retained permanently, save it to non-volatile memory by "AT&W".

Response: <cr,lf>OK<cr,lf>

2.5.9 AT+BTN? {Read Friendly Name from Non-volatile Memory}

Read the default friendly name from non-volatile memory.

Response: <cr,lf>"My Friendly Name"<cr,lf>
<cr,lf>OK<cr,lf>

2.5.10 AT+BTF<bd_addr> {Get Remote Friendly Name}

This command gets the remote friendly name of the peer specified.

Response: <cr,lf><bd_addr>,"Friendly Name"
<cr,lf>OK<cr,lf>

2.5.11 AT+BTP {Make Device Discoverable and Connectable }

Makes the device discoverable and connectable and waits for a connection from any device.

The setting remains valid until the next reset or power cycle (unless not changed by any other AT command subsequently). For permanent discoverable/connectable settings, please refer to S Register 512 in [Table 3-1](#).

Response: <cr,lf>OK<cr,lf>

2.5.12 AT+BTQ {Make Device Discoverable}

Makes the device discoverable but not connectable. Being discoverable implies that this device responds to inquiries from other devices (inquiry scans enabled).

The setting remains valid until the next reset or power cycle (unless not changed by any other AT command subsequently). For permanent discoverable/connectable settings, please refer to S Register 512 in [Table 3-1](#).

Use AT+BTX to make the device not discoverable.

Response: <cr,lf>OK<cr,lf>

2.5.13 AT+BTG {Make Device Connectable}

Makes the device connectable but not discoverable and waits for a connection from any device.

The setting remains valid until the next reset or power cycle (unless not changed by any other AT command subsequently). For permanent discoverable/connectable settings, please refer to S Register 512 in [Table 3-1](#).

Response: <cr,lf>OK<cr,lf>

2.5.14 AT+BTV<bd_addr>,<uuid> {SDP Query for Service }

This command interrogates the SDP database of the peer device <bd_addr> for the service <uuid>. It results in an ACL connection and then an SDP transaction.

If the <uuid> service is present:

Response: <cr,lf>0
<cr,lf>OK<cr,lf>

If the <uuid> service is not present:

Response: <cr,lf>1
<cr,lf>OK<cr,lf>

If the device < bd_addr > cannot be reached, or is in non-connectable mode:

Response: <cr,lf>2
<cr,lf>OK<cr,lf>

If the SDP database is corrupt or invalid:

Response: <cr,lf>3
<cr,lf>OK<cr,lf>

If the device is not in idle mode:

Response: <cr,lf>4
<cr,lf>OK<cr,lf>

In this case, the command AT+BTX may put the device into the correct idle mode.

2.5.15 ATIn {Information}

This returns the information about the Laird device and its status. Please refer to [Table 3-2](#) for a complete list of supported ATIn parameters.

For recognized values of n:

Response: <cr,lf>As Appropriate<cr,lf>OK<cr,lf>

For unrecognized values of n:

Response: <cr,lf>Laird Technologies Inc, UK, (c)2009<cr,lf>

2.6 AT Commands for S Registers

As with modems, the Bluetooth module employs a concept of registers which are used to store parameters, such as escape sequence character, inquiry delay time, etc.

For a list of general S registers please refer to [Table 3-1](#).

S registers associated with a particular profile or specific functions, are described in the appropriate profile section of this document. The following AT commands allow the manipulation of S registers.

2.6.1 ATSn=m {Set S Register}

The value part 'm' can be entered as decimal or hexadecimal. A hexadecimal value is specified by a '\$' leading the character. For example, \$1234 is a hexadecimal number.

When S register values change, the changes are not stored in non-volatile memory until the AT&W command is used. Note that AT&W does not affect S registers 520 to 525 or 1000 to 1010 as they update in non-volatile memory when the command is received.

2.6.2 ATSn? {Read S Register Value}

This returns the current value of register n.

For recognized values of n:

Response: <cr,lf>As Appropriate<cr,lf>OK<cr,lf>

For unrecognized values of n:

Response: <cr,lf>ERROR nn<cr,lf>

2.6.3 ATSn=? {Read S Register – Valid Range}

This returns the valid range of values for register n.

For recognized values of n:

Response: <cr,lf>Sn:(nnnn..mmmm)<cr,lf>OK<cr,lf>

For unrecognized values of n:

Response: <cr,lf>ERROR nn<cr,lf>

2.6.4 AT&Fn {Set S Register Defaults}

This command only works when the device is in local command and unconnected mode. Depending on the value of 'n', it installs S Register values appropriate for various power modes, ranging from minimum to maximum power consumption.

Legal values of 'n' are listed in the following table. All other values of n generate a syntax error response. If 'n' is not specified then a default value of zero is assumed where the baud rate is NOT changed.

&F0 (Default)	Medium power consumption, UART baud rate unchanged
&F1	Minimum power consumption, UART baud rate set to 9600
&F2	Minimum power consumption, UART baud rate set to 38400
&F3	Minimum power consumption, UART baud rate set to 115200
&F4	Medium power consumption, UART baud rate set to 115200
&F5	Maximum power consumption, UART baud rate set to 115200

The new values are NOT updated in non-volatile memory until the AT&W command is sent to the device.

Response: <cr,lf>OK<cr,lf>

Or <cr,lf>ERROR nn<cr,lf>

2.6.5 AT&F* {Clear Non-volatile Memory}

The AT&F* variant of the command installs values in S registers as per command AT&F4 and then all other user parameters in non-volatile memory are erased. This means that the trusted device database clears, and parameters related to the following commands also clear: AT+BTR, AT+BTN, AT+BTS.

Response: <cr,lf>OK<cr,lf>
Or <cr,lf>ERROR nn<cr,lf>

2.6.6 AT&F+ {Clear Non-volatile Memory}

This command erases all user parameters in non-volatile memory except S Registers 520 to 525. This means that the trusted device database clears, and so do parameters related to the following commands: AT+BTR, AT+BTN, AT+BTS.

Response: <cr,lf>OK<cr,lf>
Or <cr,lf>ERROR nn<cr,lf>

2.6.7 AT&W {Write S Registers to Non-volatile Memory}

Writes current S Register values to non-volatile memory so that they retain over a power cycle.

Response: <cr,lf>OK<cr,lf>
Or <cr,lf>ERROR nn<cr,lf>

2.7 General S Registers

Please refer to [Table 3-1](#) for a list of supported S Registers.

The main purpose of S Registers is to make the device configuration persistent. All S Registers can be saved to non-volatile memory by AT&W.

In some cases, an AT command and an S register exist for one and the same setting. In the majority of those cases the AT command's setting is lost on the next power cycle whereas the S register can be saved and is still available after the power cycle. This rule applies to many but not to all of those cases.

2.8 AT Commands for Inquiry

2.8.1 AT+BTI <devclass> {Inquire}

This makes the device perform an inquiry for delay seconds and the maximum number of unique responses, where delay is defined by S register 517 and maximum is specified by S register 518.

The <devclass> is an optional parameter where the value specifies either a six digit device class code or a two digit major device class. If it is not specified, the value is taken from S register 516.

When <devclass> is six hexadecimal characters long, it specifies an AND mask which filters inquiry responses. When <devclass> is two hexadecimal characters long, it forces the inquiry to filter responses to devices that match their major device class code to this value – which can only be in the range 00 to 1F.

The response format to AT+BTI is defined by S Register 330 by bitmask. This is device address, device class, friendly name, receiver strength indicator and extended inquiry data. Please refer to [Table 2-8](#) and [Table 2-9](#).

For S330=1:

Response: <cr,lf>12346789012
<cr,lf>12345678914
<cr,lf>OK<cr,lf>

A Bluetooth inquiry process is such that for a single inquiry request, a device could respond many times. To ensure that an address sends to the host only once for a particular AT+BTI, an array of addresses is created at the start of each AT+BTI and is filled as responses arrive. This array of addresses stores in dynamic memory


```
"\01ABCD\02\03456\04\0A\0D"
```

No validation is performed on incoming EIR data.

If a higher significant flag is set and a lower significant bit is not set in S 330, for each disabled item, a comma prints.

Example: S330 = 9 (ADDR enabled, COD and FN disabled, RSSI enabled)

Inquiry Response:

```
<cr,lf>123456789012,,, -54
```

```
<cr,lf>123456789014,,, -54
```

```
<cr,lf>OK<cr,lf>
```

2.8.3 AT+BTIV<devclass> { Inquire }

As per AT+BTI but the response comprises for all inquiry responses:

- Bluetooth device address
- Device class code

S register 330 is not referenced.

2.8.4 AT+BTIN<devclass> { Inquire }

As per AT+BTI but the response comprises for all inquiry responses:

- Bluetooth device address
- Device class code
- Friendly name

S register 330 is not referenced.

2.8.5 AT+BTIR<devclass> { Inquire }

As per AT+BTI but the response comprises for all inquiry responses:

- Bluetooth device address
- Device class code
- Friendly name
- RSSI (receiver signal strength indicator)

S register 330 is not referenced.

2.8.6 AT+BTIE<devclass> { Inquire }

As per AT+BTI but the response comprises for all inquiry responses:

- Bluetooth device address
- Device class code
- Friendly name
- RSSI (receiver signal strength indicator)
- Extended inquiry data

S register 330 is not referenced.

2.8.7 AT+BTE="<EIR-Data>" {Set up outgoing EIR Data}

This command sets up outgoing EIR (extended inquiry response) data.

Format: <EIR-Data> = printable ASCII character whenever possible, otherwise a two digit hexadecimal with preceding '\ ' presenting one byte. Please note that the given data writes to the baseband as it is (raw data) and no checks on the data format are performed. Hence, the user is responsible for writing data that corresponds to the extended inquiry response data format as described in the Bluetooth Specification Version 2.1 + EDR [1], vol3, Part C – Generic Access Profile, 8 Extended Inquiry Response Data Format (page 1305 in the PDF file).

Response: <cr,lf>OK<cr,lf>

2.8.8 AT+BTE? {Query outgoing EIR Data}

This command prints the outgoing EIR data that is currently set up.

Response: <cr,lf>
<EIR-Data>
<cr,lf>OK<cr,lf>

2.9 AT Commands for Extended Inquiry Response Data

Bluetooth 2.1 specification allows up to 240 Bytes of extended inquiry data. Extended inquiry data can be used to transmit the friendly name, UUIDs of supported profiles or user defined data within the inquiry process and without a Bluetooth connection.

The architecture for managing EIR data is composed of three buffers and a set of AT commands surrounding them:

- Baseband (EIR data visible to inquiring devices)
- RAM buffer (allows accumulation of data)
- EIR persistent store (non-volatile buffer, copied to baseband at boot time)

Because the input buffer length for one AT command is limited, there is a RAM buffer to accumulate several short data packets. The accumulated data of the RAM buffer can be copied to the baseband where it becomes immediately visible to other inquiring devices. The content of the RAM buffer can also be copied to the EIR persistent store. If the EIR persistent store contains data, it is copied to the baseband automatically upon boot.

This allows a flexible use of extended inquiry data. For example, data with a low data rate (such as temperature) can be transmitted without creating a connection between Bluetooth devices, however at the cost of no encryption and no authentication.

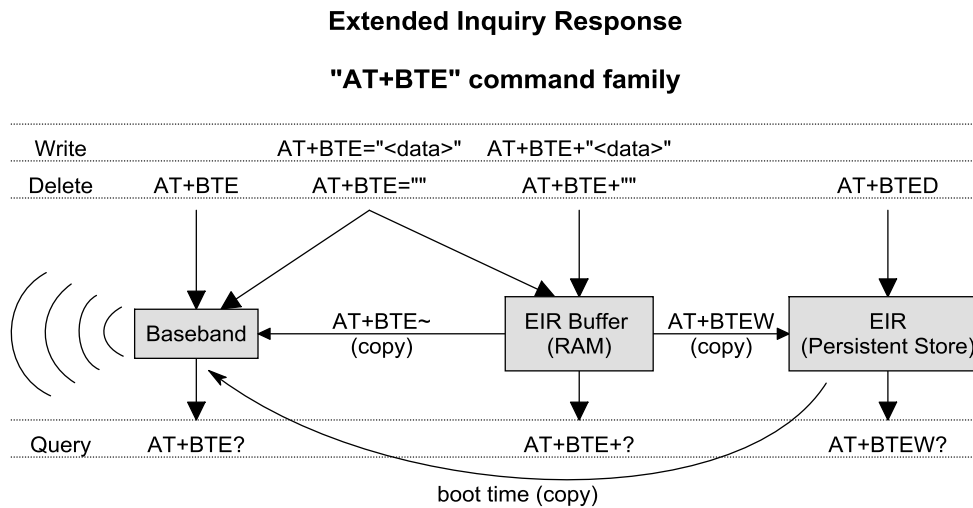


Figure 2-1: Extended Inquiry Response – command overview

2.9.1 EIR Data Format

When passing EIR data ("`<data>`") to AT commands (`AT+BTE="<data>"` / `AT+BTE+"<data>"`), each byte should be presented by its ASCII representation whenever it is a printable character. Each non-printable ASCII character must be presented as two hex digits with a preceding `\`. For example, a byte of decimal value 5 would be presented as `"\05"` because the ASCII character of 05d is not printable. A decimal value of 43 should be presented as `'+'` because `'+'` is the ASCII character representing 43d. The module also accepts `"\2B"` (the hexadecimal presentation of 43d) but at the price of two redundant characters.

When querying the content of any buffer (Baseband / RAM / Persistent Store), non-printable ASCII characters are presented by two hex digits with preceding `\`.

Exceptions:

- `""` (quotation mark) is presented as `\22`
- `\` (backslash) is presented as `\5C`
- `,` (comma) is presented as `\2C`

Any data passed to the baseband must match the format defined in the Bluetooth Specification Version 2.1 + EDR [1], vol3, Part C – Generic Access Profile, 8 Extended Inquiry Response Data Format (page 1305 in the PDF file). The AT command interpreter does not perform any checks on the baseband data format.

2.9.2 AT+BTE+"<data>" {Accumulate data in RAM buffer}

This command adds `<data>` to the content of the RAM buffer. The maximum number of characters for `<data>` is 25 due to the limited AT command input buffer. See [Section 2.9.1](#) for more information.

Response: `<cr,<lf>OK<cr,<lf>`

Or `<cr,<lf>ERROR 05<cr,<lf>`

2.9.3 AT+BTE="<EIR-data>" {Write EIR data to baseband and RAM buffer}

This command writes EIR (extended inquiry response) data to the baseband and to the RAM buffer. The maximum number of characters for <EIR-data> is 25 due to the limited AT command input buffer. See [Section 2.9.1](#) for more information.

Response: <cr,&lf>OK<cr,&lf>

Or <cr,&lf>ERROR 05<cr,&lf>

2.9.4 AT+BTE~ {Copy RAM buffer to baseband}

This command copies all data from the RAM buffer to the baseband. The data passed to the baseband must match the EIR data format as specified in the BT2.1 specification (page 1305 in the PDF file). See [Section 2.9.1](#) for more information.

Response: <cr,&lf>OK<cr,&lf>

2.9.5 AT+BTEW {Copy RAM buffer to EIR persistent store}

This command copies all data from the RAM buffer to the (non-volatile) persistent store. If the EIR persistent store contains any data at boot time, this data copies to the baseband at boot time automatically. After copying data to the EIR persistent store it is visible to other inquiring devices from the next power cycle onwards. Data passed to the baseband must match the EIR data format as specified in the BT2.1 specification (page 1305 in the PDF file). See [Section 2.9.1](#) for more information.

Response: <cr,&lf>OK<cr,&lf>

2.9.6 AT+BTE+? {Query data from RAM buffer}

This command prints the data that is currently stored in the RAM buffer.

Response: <cr,&lf><data><cr,&lf>OK<cr,&lf>

2.9.7 AT+BTE? {Query outgoing EIR data from baseband}

This command prints the outgoing EIR data that is currently set up in the local baseband. Some interpretation on the EIR data format is done here. If the leading byte of a data block contains the wrong length information, then some unexpected output may appear; e.g. \00 appends.

Response: <cr,&lf><EIR-data><cr,&lf>OK<cr,&lf>

2.9.8 AT+BTEW? {Query data from EIR persistent store}

This command prints the data currently stored in the EIR persistent store.

Response: <cr,&lf><data><cr,&lf>OK<cr,&lf>

2.9.9 AT+BTE {Delete EIR data from baseband}

This command deletes the EIR data in the baseband.

Response: <cr,&lf>OK<cr,&lf>

2.9.10 AT+BTE="" {Delete EIR data from baseband and RAM buffer}

This command deletes the EIR data in the baseband and deletes any data from the RAM buffer.

Response: <cr,lf>OK<cr,lf>

2.9.11 AT+BTE+"" {Delete RAM buffer}

This command deletes all data from the RAM buffer.

Response: <cr,lf>OK<cr,lf>

2.9.12 AT+BTED {Delete EIR persistent store}

This command deletes the EIR persistent store.

Response: <cr,lf>OK<cr,lf>

2.10 Persistent Store

Management of persistent store

- **AT+NVQ<size>**- query available free space in current flash segment, size=optional
- **AT+NVF**- flood current flash segment to trigger defragmentation on next reset

Extensive usage of the persistent store (=non-volatile memory) can cause scenarios where some AT commands or functions cannot be successfully finished and cause an error message. This section explains the background of persistent store and suggests strategies to avoid these scenarios.

2.10.1 Persistent store characteristic

The persistent store of BTM41x is made of flash memory, which has the typical characteristic that a single bit can be written only once. For deletion of data, a larger area, a so called segment must be deleted in common. This means that all data of the segment would be lost. So in order to delete a small amount of data but retaining all other data of the segment, the data to be deleted is not actually deleted but is invalidated by internal flash memory pointers. Similarly, overwriting does not actually delete old data but stores the new data in the remaining space of the segment and declares the old location invalid by pointing to the new location. As one can spot, the flash segment fills up with each write (or delete) operation to persistent store. At some point the segment will be full and write/delete operations won't succeed any more, resulting in error messages (e.g. ERROR 11). The firmware has a built-in mechanism to recover from this state with a power cycle / reset (ATZ): If the remaining free space of the current segment is below a certain limit, the flash segment is defragmented and copied to a free segment. Due to this defragmentation, which clears out all invalidated data, plenty of new space in the new segment becomes available. From now on, the new segment is being used for all operations (read/write/delete). Finally, the old segment is deleted in order to be readily prepared for the next defragmentation/copy cycle.

2.10.2 AT commands for managing persistent store

BTM41x firmware provides AT commands allowing to manage the persistent store:

- **AT+NVQ** query the remaining space in current segment
- **AT+NVF** flood the remaining space of current segment. On next power cycle (ATZ) a defragmentation cycle will occur.

2.10.3 Commands which use persistent store

The following operations and commands use persistent store:

- Write EIR data (AT+BTEW)
- Save S-Registers (AT&W)
- ...

2.10.4 Strategy to prevent persistent store write errors

If an application makes extensive use of persistent store (PS) operations, then the PS consumption of the application should be considered and evaluated.

AT+NVQ helps to analyze the consumption of each relevant operation by querying the free space before and after. It also allows monitoring the free space over a longer application period by polling the NVQ value regularly. This should give an idea on the persistent store consumption of an application.

It has been observed that persistent memory is automatically defragmented on a reset if the NVQ value is less than 300. Although this seems to be working well, an additional AT+NVF is always recommended before making a reset for the purpose of defragmentation, just to be on the safe side.

As a strategy to prevent write operation errors (e.g. ERROR 011) it is recommended to first analyze the persistent store consumption of the application. If in the course of the application it is likely that no reset will occur over long time and that the NVQ value will decrement down to a critical level, then the host controller should foresee flooding (AT+NVF) and reset (ATZ) in situations where it doesn't hurt (e.g. no connection) and when the NVQ value is getting too low.

2.11 Secure Simple Pairing (SSP)

Secure Simple Pairing (SSP) has been introduced since Bluetooth 2.1 + EDR. It aims to increase the security provided by a Bluetooth link while making the pairing process more user-friendly.

There are white papers about SSP available through the internet (provided by the Bluetooth SIG and other companies), explaining the mechanisms and backgrounds of SSP. They can be found by searching the internet for "Bluetooth Secure Simple Pairing". Please familiarize yourself with those documents to get a better understanding of SSP and the following settings.

2.11.1 Security Level (S320)

The security level is defined in the BT2.1+EDR specification (See [Reference 1](#)).

There are four different levels of security ([Table 2-10](#)).

Table 2-10: Security levels

Security Level	Characteristics	Comment
Level 3	MITM protection (MITM = "Man in the Middle" attack) Encryption User interaction	High security
Level 2	No MITM protection Encryption	Medium security
Level 1	No MITM protection (No) encryption ⁽¹⁾ Minimal user interaction	Low security
Level 0	No MITM protection	Permitted only for

Security Level	Characteristics	Comment
	No encryption Minimal user interaction	service discovery

(1) Although encryption is not necessary for security level 1, encryption is always enabled because this specification mandates encryption for all services other than SDP (service discovery).

The security level is defined by S Register 320 and is referenced at boot time only. Hence the register must be saved by “AT&W ” and the module must be power cycled (or “ATZ”) subsequently.

S320 = 3 overwrites the setting of S Register 322 (enable MITM).

The security level remains the same until the next power cycle and is valid for all profiles and services of the module. For SDP (service discovery profile), security level 0 is always assigned internally.

2.11.2 IO-Capability (S321)

S-Register 321 defines the IO-capability of the device. The setting is used for IO-capability negotiations prior to SSP in order to identify whether the IO-capabilities of both devices are sufficient for MITM protection (if required). Table 2-11 lists possible values.

Table 2-11: IO capabilities

S321	IO-Capability	Comment
0	Display only	The device has the capability to display or communicate a six digit decimal number.
1	Display yes/no	The device has the capability to display or communicate a six digit decimal number and at least two buttons that can be easily mapped to ‘yes’ and ‘no’, or a mechanism whereby the user indicates either ‘yes’ or ‘no’ (e.g. pressing a button within a certain time limit).
2	Keyboard only	The device has a numeric keyboard that can input numbers ‘0’ through ‘9’ and a confirmation. The device also has at least two buttons that can be easily mapped to ‘yes’ and ‘no’ or a mechanism whereby the user can signal ‘yes’ or ‘no’ (e.g. pressing a button within a certain time limit).
3	No input no output	The device does not have the ability to indicate ‘yes’ or ‘no’, and the device does not have the ability to display or communicate a six digit decimal number.
4	Reject IO-Cap requests	IO-capability requests prior to SSP are rejected.

2.11.3 Force Man-In-The-Middle Protection (MITM, S322)

Protection against MITM-attacks are enabled by S332. This S-Register only applies if the security level (S320) is less than three. In case of security level (S320) = 3, MITM protection is always enabled and this S 322 is ignored.

- A new value written to S322 applies immediately. No power cycle is required.
- A link key created with MITM protection is named “authenticated link key”.
- A link key created without MITM protection is named “unauthenticated link key”.

2.11.4 Disable Legacy Pairing (S323)

If the remote device is a legacy device (BT2.0 or earlier), legacy pairing with PIN codes is performed. Legacy Pairing can be disabled by S-Register 323 = 1, but pairing with legacy devices always fails.

2.11.5 SSP Timeout (S324)

The SSP timeout is defined by S-Register 324. The timeout must be at least 60 seconds to meet the BT specification requirements [1]. This time is required to be sufficient for the user to compare or read and input a six digit number. A time of 90 seconds (the default value) is recommended.

2.11.6 SSP Input Commands

Table 2-12 lists all AT commands related to SSP input operations.

Table 2-12: SSP Input commands

AT Command	Operation	Comment
AT+BTBY	Accept pairing request	Representing 'yes' input
AT+BTBN	Reject pairing request	Representing 'no' input
AT+BTB012345	Enter 6 digit passkey displayed by remote device	Representing keyboard input

2.11.7 AT+BTW<bd_addr> {Initiate SSP}

This command initiates SSP (dedicated bonding) with a device whose Bluetooth address is <bd_addr>. The correct term for this command's action with respect to the Bluetooth specification 2.1+EDR [1] is "Dedicated Bonding". Dedicated bonding means the exchange of link keys (pairing) without creating a connection to a particular profile or service immediately.

The remote device must be a Bluetooth 2.1 device, otherwise (BT2.0 or earlier) legacy pairing occurs automatically if S323=0. For legacy pairing please refer to Section 2.12.

The "OK" response sends immediately on receipt of the AT+BTW command. Depending on the combination of IO-capabilities of both devices, one of the asynchronous messages from Table 2-14 may appear during the pairing process. Please refer to that table for the required actions.

On pairing completion, an unsolicited message in the form PAIR n <bd_addr> is sent to the host.

2.11.8 S Registers for Secure Simple Pairing

Table 2-13 lists all S Registers for SSP. For the registers' details please refer to their descriptions above.

Table 2-13: S-Registers for SSP

Register	Default	Range	Comment
S320	2	1..3	Security Level: see Reference 1. Needs subsequent 'AT&W' and power cycle to take effect Value = 3 overwrites S322
S321	1	0..4	Set IO capability: 0 – display only 1 – display yes/no 2 – keyboard only 3 – no input/no output 4 – reject IO-cap requests
S322	0	0..1	Force man-in-the-middle-protection (MITM): 0 – disabled

Register	Default	Range	Comment
			1 – enabled Referenced only if security level (S320) < 3
S323	0	0..1	Disable legacy (pre-BT2.1) Pairing: 0 – legacy pairing enabled 1 – legacy pairing disabled
S324	90	1..255	Secure Simple Pairing timeout in s This value must be at least 60 in order to meet the recommendation of BT2.1 specification

2.11.9 Asynchronous SSP Messages

Table 2-14 lists asynchronous messages which occur if MITM is enabled. The actual sent message depends on the combination of the IO capabilities of both ends. The combination of IO capabilities of both devices can also be insufficient for MITM protection. In that case, the pairing fails (PAIR 2 <BdAddr>). Please refer to Table 5.6 in Reference 1 for sufficient combinations of IO-capabilities for MITM (=authenticated link key).

Table 2-14: Asynchronous messages for SSP

Message	Action / Comment
PAIR ? <BdAddr>,"<friendlyname>",<Passkey> Example: PAIR ? 0016A4000002,"Laird BTM 000002",863611	Passkey compare request: Expecting the user to compare the passkey displayed on both ends and to confirm a match by "AT+BTBY" at both ends or reject by "AT+BTBN" if passkey does not match
PASSKEY ? <BdAddr>,"<friendlyname>" Example: PASSKEY ? 0016A4000001,"Laird BTM 000001"	Passkey request: Expecting the user to enter the passkey displayed by the remote device. Use AT+BTB<passkey>, Example: AT+BTB012345 *see(1) below
PAIR N <BdAddr>,"<friendlyname>",<Passkey> Example: PASSKEY N 0016A4000002,"Laird BTM 000002",164585	Passkey notification: Display BdAddr, friendly name and passkey to user, expecting the user to enter the passkey from this message at the remote device's numeric keyboard.
PAIR 0 <BdAddr> <nn>	Successfully paired with device of <BdAddr>. <nn> (optional) indicates the status of automatic storage to trusted device list. Value 0 = success; settings controlled by S325 to S328. Please refer to Section 2.11.9.
PAIR 1 <BdAddr>	Pairing timeout
PAIR 2 <BdAddr>	Pairing failed
PAIR 3 <BdAddr>	Pairing failed (too many repeat attempts)
PAIR 4 <BdAddr>	Pairing rejected by remote device
PAIR 5 <BdAddr>	Pairing failed (unit keys not supported)
PAIR 6 <BdAddr>	Pairing failed (SSP not supported)
PAIR 7 <BdAddr>	Pairing failed (already busy with pairing)

- (1) If both devices have a “KeyboardOnly” capability, no pass key can be displayed. In that case, the user is required to invent and enter the identical 6 digit numeric passkey at both ends.

2.11.10 Known SSP Issues

General Bonding (automatic pairing on link setup if devices have not been paired previously) does not work with legacy devices (BT2.0 and earlier). If the remote device is BT2.0 or earlier, initiate dedicated bonding (AT+BTW<BdAddr>) prior to connection establishment.

Outgoing General Bonding with MITM does not work with two BTM devices because any UART input on the initiating device does not accept until the link establishes. Workaround: Initiate dedicated bonding (AT+BTW<BdAddr>) prior to connection establishment.

If the link key of previously paired devices is no longer available in the remote device but is still available in the trusted device list (TDL) of the local device (query by AT+BTT?), pairing fails. In that case, remove the device address from the local TDL using AT+BTD<BdAddr> and reinitiate pairing from the local device (AT+BTW<Bd_addr>)

2.12 AT Commands for Legacy Pairing

2.12.1 AT+BTW<bd_addr> {Initiate Pairing}

Provided the remote device is a Bluetooth 2.0 device or earlier and legacy pairing is not disabled (S323 = 0), this command initiates legacy pairing with the device with <bd_addr>. Legacy pairing refers to the mechanism of entering an identical PIN key on both ends. If the PIN is required (if not set earlier by AT+BTK=”<PIN>”), asynchronous indications send to the host in the form PIN? <bd_addr> where the address confirms the device with which the pairing performs. To supply a PIN, use the AT+BTK command.

For a successful pairing, the link key stores in a volatile cache which is overwritten every time a new pairing initiates using this command. If S register 325=1, the link key automatically saves to the non-volatile trusted device list. Otherwise (S325=0) the link key can be added to the trusted device list by AT+BTT. Please refer to [Section 2.13](#) Devices for further AT commands related to trusted device list.

The “OK” response sends immediately on receipt of the AT+BTW command. On pairing completion, an unsolicited message sends to the host in the form PAIR n <bd_addr>.

If AT+BTI or AT+BTP or AT+BTG or AT+BTQ or ATD issues between the AT+BTW command and the subsequent PAIR asynchronous response, then an ERROR response sends to those commands as the device is not in a mode from where such commands can be actioned.

Response: <cr,lf>OK<cr,lf>

2.12.2 AT+BTK=”<string>” {Set Passkey}

This command is used to provide a PIN passkey. The PIN is stored in non-volatile memory for future use. If this command is used as response to a “PIN? 12345678” asynchronous message, the PIN provided by this command is not stored in non-volatile memory.

Specifying an empty string deletes the PIN from the non-volatile memory. The string length must be in the range 0 to 8, otherwise an error is returned.

Response: <cr,lf>OK<cr,lf>

2.12.3 Legacy Pairing – Asynchronous Messages

PIN?

This response sends to the host during a pairing negotiation.

The fully qualified string is PIN? 012345678901 where 012345678901 is the Bluetooth address of the peer device. In response, the host must supply a pin code which is entered using the AT+BTK command. If the peer does not supply the address in the message exchange, then the address is specified as 000000000000 – and the pairing proceeds as normal.

```
PAIR n <bd_addr>
```

This response sends to the host on termination of a pairing process. If pairing is successful then 'n' = 0, if a timeout occurs then 'n'=1, and for all other unsuccessful outcomes the value is 2. The parameter <bd_addr> is the address of the peer device, if available.

```
PAIR 0 <bd_addr> MM
```

This response sends to the host on termination of a successful pairing process. The optional MM sends only if the according S Register 325..328 is set to 1 to automatically save the link key. The value MM indicates the result of the save operation and a value of 00 implies success, otherwise the value corresponds to an error code.

2.13 AT Commands Managing Trusted Devices

2.13.1 AT+BTT? {List Trusted Device}

This command lists the contents of the trusted device database. The link key is NOT displayed so the response is as shown below. If the list is empty then just the OK response is sent, otherwise an OK is used to terminate the list. Use the command ATi6 to read the maximum size of the trusted device database.

```
Response: <cr,lf>12346789012
          <cr,lf>12345678913
          <cr,lf>12345678914
          <cr,lf>OK<cr,lf>
```

2.13.2 AT+BTT {Add Trusted Device}

This command is used to store the cached link key in the non-volatile database. If the database is full it responds with ERROR. If the device is already in the database, then the key is replaced. If the link key cache is empty (a pairing has not been performed since the device was powered), then the response is ERROR.

```
Response: <cr,lf>OK<cr,lf>
Or        <cr,lf>ERROR<cr,lf>
```

2.13.3 AT+BTD<bd_addr> {Remove Trusted Device}

This command removes the specified device from the list of trusted devices in the non-volatile database. If the device is not in the database then the response is still OK.

```
Response: <cr,lf>OK<cr,lf>
```

2.13.4 AT+BTD* {Remove All Trusted Devices}

This command removes all devices from the trusted device list (TDL) in the non-volatile database. **No confirmation is requested.**

WARNING: If you make a connection, the link key gets cached in the underlying stack. So if you subsequently delete the key using AT+BTD* and immediately request a connection to the same device, then the connection will be established. To ensure this does not happen, send ATZ after the AT+BTD*.

Response: <cr,lf>OK<cr,lf>

2.13.5 AT+BTW? {List Cached Trusted Device}

This command lists the cached trusted device.

Response: <cr,lf>12346789012
<cr,lf>OK<cr,lf>

If the cache is empty the response is as follows:

Response: <cr,lf>OK<cr,lf>

2.14 AT Commands for Serial Stream Oriented Profiles (SSO)

The SSP and the Dial-up Networking Profile (DUN) belong to the group of Serial Stream Oriented (SSO) profiles.

When activated, an SSO profile claims one UART for its data stream and assumes all data at the UART to transmit over or received from RF 1:1. Hence, as there is only one UART available on a BTM device, the UART is not available for other profiles, services or module control purposes.

One approach of managing data and control over UART is to configure local command mode with S531=3. In this mode, incoming RF data is presented by the asynchronous message RX<string>. Outgoing data sends by ATX<string> or ATY<string>.

With this approach it is possible to manage several non-SSO connections (e.g. A2DP, AVRCP) and at maximum one SSO connection (SSP or DUN). An attempt to connect a second SSO profile while there is one SSO already connected results in Error 65.

Any incoming connection request to an SSO profile is rejected if one SSO is already connected.

The following section describes AT- commands related to SSO-profiles.

2.14.1 ATX"<string>" {Send Data in Local Command and Connected Mode}

This command sends data to the remote device when in local command and connected mode.

The parameter <string> is any string not more than 29 characters long whereby a non-printable character (\hh, see below) counts three characters. This restriction results from the maximum AT command length which is 34 (query by AT+I15). The difference of five is caused by "ATX" (three characters) and the enclosing quotation marks (two characters).

If the maximum string length is exceeded, ERROR 05 (syntax error) occurs.

If a non-visual character is sent, then insert the escape sequence \hh where hh are two hexadecimal digits. The three character sequence \hh converts into a single byte before transmission to the peer.

Response: <cr,lf>OK<cr,lf>
Or <cr,lf>ERROR 05<cr,lf> (e.g. <string> too long)

2.14.2 ATY"<string>" {Send Data in Local Command and Connected Mode}

This command is similar to ATX in syntax and functionality, except that the string only copies to the output RF buffer. Only when an empty string presents does all pending data in the output RF buffer flush out.

The parameter <string> is any string not more than 29 characters long whereby a non-printable character (\hh, see below) counts 3 characters. This restriction results from the maximum AT command length which is 34 (query by AT15). The difference of five is caused by "ATX" (three characters) and the enclosing quotation marks (two characters).

If the maximum string length is exceeded, ERROR 05 (syntax error) occurs.

If a non-visual character is sent, insert the escape sequence \hh where hh are two hexadecimal digits. The three character sequence \hh converts into a single byte before transmission to the peer.

Response: <cr,lf>OK<cr,lf>
Or <cr,lf>ERROR 05<cr,lf> (e.g. <string> too long)

2.14.3 ^^^ {Enter Local Command Mode}

When in data and connected mode and when S 507 is set to 0 or 1, the host can force the device into a command and connected mode so that AT Commands can issue to the device. The character in this escape sequence specifies in the S2 register, so it can change. In addition, the escape sequence guard time is specified by S Register 12. By default the guard time is 100 milliseconds.

Leaving data mode by "^^^" has a severe penalty on data throughput because each incoming character needs to be checked for '^' with respect to the guard time.

Alternatively, a de-assertion of the DTR/DSR line can be used as the only trigger to leave data mode (S507=2). This gives a significant higher data throughput because data passes directly between UART and RF without character checking..

In modems this escape sequence is usually "+++".

"^^^" is specified to avoid confusion when the module is providing access to a modem.

Response: <cr,lf>OK<cr,lf>

2.14.4 !!! {Enter Remote Command Mode}

When in data and connected mode, the host can force the remote device into a command and connected mode so that AT Commands can issue to the device remotely. The escape sequence guard time is specified by S Register 12 and is the same as per the ^^^ escape sequence. By default the guard time is 100 milliseconds. The remote device issues ATO as normal to return to data mode. For this command to be effective, S Register 536 must be set to 1.

Response: <cr,lf>OK<cr,lf>

2.14.5 ATO {Enter Data Mode} (letter 'o')

Return to data mode. Assume that the module is in data mode after OK is received. Responds with an error if there is no Bluetooth SSO connection.

Response: <cr,lf> CONNECT 123456789012,><cr,lf> (if incoming connection)
<cr,lf> CONNECT 123456789012,><cr,lf> (if outgoing connection)
Or <cr,lf>ERROR nn<cr,lf>

2.14.6 Dropping SSO Connections

In a conventional telephony modem, a call normally terminates by first sending a +++ character sequence enveloped by an escape sequence guard time (of the order of 100 to 1000 milliseconds) to enter local command and connected mode and then the ATH command.

Laird BTM devices provide a variety of ways to drop a connection. One method is similar to the above, but instead a ^^^ character sequence is used; this eliminates ambiguity when a data call is in progress via a mobile phone which was established using the mobile phone's Bluetooth AT modem. The second method involves the host dropping the DTR (DSR from the module's viewpoint) handshaking line.

Being able to drop a connection using the escape sequence ^^^ has a severe penalty on data throughput. In fact, the data rate is approximately 85 kbps instead of approximately 300 kbps. To cater for this performance hit, the device's connection drop capability is configurable to be in one of two modes. One mode allows a connection to drop using either method, and the other mode allows for a connection to drop using the DTR method only. By default, the device is in the first mode. Select this mode using the S507 register (Table 3-1).

To reiterate, the escape sequence is as follows:

```
<Guard time><Esc Chr><Guard time><Esc Chr><Guard time><Esc Chr><Guard time>
```

This means that even when a file transfer occurs and it happens to be full of <Esc Chr> characters, it is not going to drop into command mode because, when transferring a file, it happens as fast as possible and so the inter character gap is significantly shorter than the <Guard time>.

The <Esc Chr> character can change via the S2 register and the <Guard time> interval can be specified via the S12 register (Table 3-1).

2.14.7 SSO - Asynchronous Messages

RX<string>

This response is sent to the host when the unit is in online-command mode, S Register 531 is set to 3, and data arrives from a peer.

If the data from the string contains non-visual characters (for example ASCII 0 to 31 and ASCII 128 to 255), then those characters translate into a three character escape sequence starting with '\.

For example, the embedded <cr><lf> sequence is sent as the six character string \0D\0A.

If the data contains the character '"' then it is sent as \22.

If the data contains the character '\ then it is sent as \5C

2.14.8 SSO – S Registers

The following table lists S registers for SSO profiles.

Table 2-15: S Registers for SSO profiles

Register	Default	Range	Description
S2	94	32..126	Escape sequence character. It is not '+' by default as a Bluetooth serial link can be used to connect to a mobile phone which exposes an AT command set, which in turn uses '+' as default. So if both used '+', there is confusion. 94 is the character '^'.
S12	100	40..5000	Escape sequence guard time in milliseconds, with a granularity of 20 ms. New values round down to the nearest 20 ms multiple.

Register	Default	Range	Description
S507	0	0..2	<p>When set to 0, a connection can be dropped using ^^^ escape sequence only and the state of DSR line is ignored.</p> <p>When set to 1 a connection can be dropped using EITHER the ^^^ escape sequence OR the DSR handshaking line. When set to 2, a connection can only be dropped using a deassertion of DSR. Mode 2 provides for the highest data transfer rate.</p> <p>If the status of the DSR line is to be conveyed to the remote device as a low bandwidth signal then this register MUST be set to 0, otherwise a deassertion of DSR will be seen as a request to drop the Bluetooth connection.</p> <p>This register affects S Register 536 – see details of 536 below.</p>
S531	0	0..4	<p>Specifies the mode on connection establishment.</p> <p>0 – Normal. Data exchanges between UART and RF.</p> <p>1 – LOCAL_COMMAND. UART input is parsed by the AT interpreter and RF data discards.</p> <p>2 – REMOTE_COMMAND. RF input is parsed by the AT interpreter and UART data discards. If S Reg 536 is not 1, this register cannot be set to 2 and an ERROR returns.</p> <p>3 – LOCAL_COMMAND. UART input is parsed by the AT interpreter and incoming RF data sends to the host using the RX<string> asynchronous response.</p> <p>4 – LOCAL_COMMAND and on the RF side, the GPIO automatically sends when there is a change in input (digital I/O cable replacement mode).</p>
S536	0	0..1	<p>When set to 1, a remote device can ‘capture’ the AT parser of this unit by it sending this module an escape “!!!” sequence. The inter character timing is set via S Register 12.</p> <p>If S Register 507 is >= 2, then reading this register always returns 0 and writing 1 results in ERROR 33.</p>

2.15 AT Commands for a Selected Peer Device

This section describes AT commands to make the BTM Bluetooth device connectable for one particular remote device only or to connect to a particular remote device on reset or on power cycle automatically.

2.15.1 AT+BTP<bd_addr> {Make Device Discoverable and Selectively Connectable}

Make the BTM device discoverable (for all devices) and connectable for the device with the Bluetooth address <bd_addr> only. Connection requests from any other devices are rejected.

If <bd_addr> is 000000000000 then incoming connections accept from any device, as per AT+BTP without an address.

The setting remains valid until the next reset or power cycle (unless not changed by any other AT command subsequently). For permanent discoverable/connectable settings, please refer to S Register 512 in Table 3-1 and [Section 2.15.3](#).

Response: <cr,<lf>OK<cr,<lf>

2.15.2 AT+BTG<bd_addr> {Make Device Selectively Connectable Only}

Make the BTM device connectable for the device with the Bluetooth address <bd_addr> only. Connection requests from any other devices are rejected.

If the specified address is 000000000000 then incoming connections accept from any device, is as per AT+BTP without an address.

The BTM device is not discoverable.

The setting remains valid until next reset or power cycle (unless not changed by any other AT command subsequently). For permanent discoverable/connectable settings, please refer to S Register 512 in Table 3-1 and [Section 2.15.3](#).

Response: <cr,lf>OK<cr,lf>

2.15.3 AT+BTM<bd_addr> {Set Incoming Peer Address}

This command stores a peer address for incoming connections in non-volatile memory. Only the device with Bluetooth address <bd_addr> is permitted to make a connection to the BTM device. Connection requests from other devices are rejected.

The new setting applies immediately and retains over a power cycle (unless not changed by any other AT command subsequently).

When S register 512 = 3, 4, 6 or 7 then the BTM device waits for an incoming connection from the peer address specified. If <bd_addr> is 000000000000 then incoming connections from any devices are permitted.

Response: <cr,lf>OK<cr,lf>

2.15.4 AT+BTM {Delete Incoming Peer Address}

This command deletes the peer address previously stored using AT+BTM<bd_addr>.

If the BTM device was connectable for the selected device before this command, it is connectable for any device immediately after this command.

Response: <cr,lf>OK<cr,lf>

2.15.5 AT+BTM? {Read Incoming Peer Address}

This command displays the peer address stored in non-volatile memory, used to put the module in pure cable replacement mode.

Response: <cr,lf>12346789012
<cr,lf>OK<cr,lf>

If the location is empty the response is as follows:

Response: <cr,lf>000000000000
<cr,lf>OK<cr,lf>

2.15.6 AT+BTR<bd_addr> {Set Outgoing Peer Address}

This command stores a peer address for outbound connections in non-volatile memory.

This command sets up a module in pure cable replacement mode. If S register 512 equals 1 and the peer address is NOT 000000000000 then it periodically (time specified via S register 505) attempts to connect to the peer address specified. In this circumstance, all data from the host buffers in the receive buffer until a Bluetooth connection establishes with the peer device and it then sends the buffer across. This means that if the peer device is not in the vicinity and will never be there and S507 equals 1 or 2, the device effectively becomes useless, as in this circumstance the module is not listening for commands arriving on the UART.

In this circumstance, a recovery is possible by one of the following two methods:

- Method 1 – Assumes that the DTR from the host is connected to the DSR line of the module and S507 equals 1.
- Method 2 – Assumes that this connection is absent and S507 equals 1 or 2.

In the first method, it is enough to deassert the DTR line from the host to abort the autoconnect cycle. No "OK" is sent in response. Hence it is up to the host to send a character regularly (e.g. one per second) until the BTM device echoes all buffered characters to the host (provided echo is enabled). Once the BTM device echoes characters, it is in command mode.

The second method is initiated by resetting the device and then ensuring that the text string "AT+BT&BISM&<cr>" is sent (where <cr> is the carriage return character). There is special code which looks out for this magic command and terminates the autoconnect cycle if it sees it and confirms to the host of that fact by sending an "OK" response.

Response: <cr,
>OK<cr,
>

2.15.7 AT+BTR {Delete Outgoing Peer Address}

This command deletes the peer address previously stored using AT+BTR<bd_addr>.

Response: <cr,
>OK<cr,
>

2.15.8 AT+BTR? {Read Outgoing Peer Address}

This command displays the peer address stored in non-volatile memory, used to put the device in pure cable replacement mode.

Response: <cr,
>12346789012
<cr,
>OK<cr,
>

If the location is empty the response is as follows:

Response: <cr,
>000000000000
<cr,
>OK<cr,
>

2.16 Bluetooth Profiles

This section covers S-Registers and AT-Commands that relate to supported Bluetooth Profiles on BTM.

2.16.1 Profile Activation

In order to activate available profiles and advertise them to potential client devices, use S-Register 102. Per default, only SPP activates (value=1). Other supported profiles can be activated by setting the appropriate flag in S-Register 102. Once S-Register 102 is written, the changed value needs to be saved to non-volatile memory

("AT&W") and subsequently a reset ("ATZ") or power cycle is required. Please note that "AT&W" saves the content of all S Registers to non-volatile memory.

2.16.2 SPP (Serial Port Profile)

The SPP is for serial data transmission with a remote device in both directions. It behaves like a wireless replacement for a serial cable.

SSP belongs to the group of SSO profiles; please refer to [Section 2.14](#) for additional information.

In order to use SPP, the profile must be enabled in S102 (value=1). If it was not enabled earlier, set the S register accordingly and issue AT&W followed by ATZ.

2.16.3 SPP example

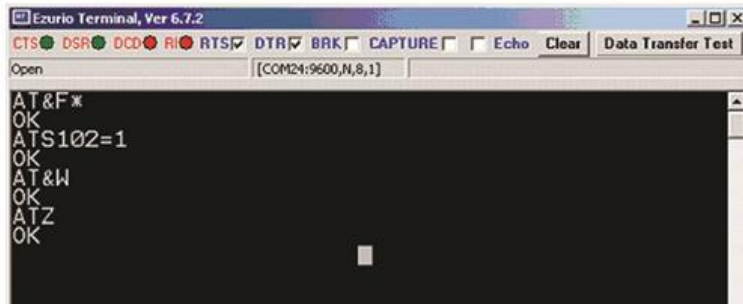
This section gives an example on how an SPP connection between two Laird BTM devices can be established. It is assumed that two devices (A and B) are connected to a terminal program, e.g. Laird (Ezurio) Terminal on a PC. The example sequence of AT commands is listed in [Table 2-16](#). Figures [Figure 2-2](#), [Figure 2-3](#), [Figure 2-4](#), and [Figure 2-5](#) present applicable screenshots with Laird (Ezurio) Terminal.

Table 2-16: SPP Example Command Sequence

Phase	Dev	AT Command	Comment
Preparation	A	AT&F*	Restore factory default settings
		ATS102=1	Enable Serial Port Profile (SPP)
		AT&W	Store settings
		ATZ	Reset
		AT&F*	Restore factory default settings
Preparation	B	AT&F*	Restore factory default settings
		ATS102=1	Enable Serial Port Profile (SPP)
		ATS0=1	Automatic response after one "RING"
		AT&W	Store settings
		ATZ	Reset
		AT+BTP	Make device temporarily connectable and discoverable
		ATI4	Query Bluetooth device address of local device <BdAddr_DevB>
Initiate connection	A	AT+SPD <BdAddr_DevB>	Initiate SPP connection from device A to device B. Asynchronous messages: "PAIR 0..." (pairing successful, A and B) "RING..." (B only) "CONNECT..." (connected, A and B)
Connected	A,B	<data>	Any character entered on one end is displayed at the other end.
Enter command mode	A or B	^^^	Response "OK" : Command mode confirmed, now AT commands are expected at the UART; UART data from host is not sent across to remote device
Disconnect		AT+SPH	Response "NO CARRIER..." (A and B): disconnection confirmed

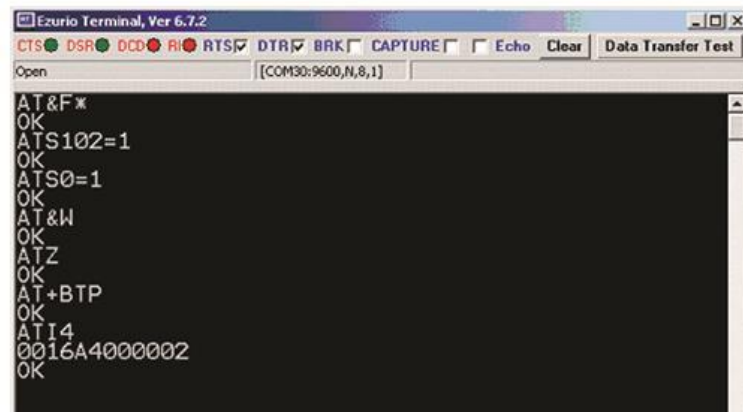
BTM410/411

Bluetooth® AT Data Module User Guide



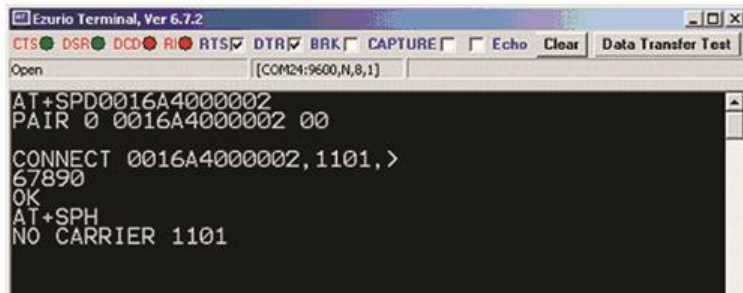
```
Ezurio Terminal, Ver 6.7.2
CTS DSR DCD RI RTS DTR BRK CAPTURE Echo Clear Data Transfer Test
Open [COM24:9600,N,8,1]
AT&F*
OK
ATS102=1
OK
AT&W
OK
ATZ
OK
```

Figure 2-2: SPP Example - Preparation of Device A



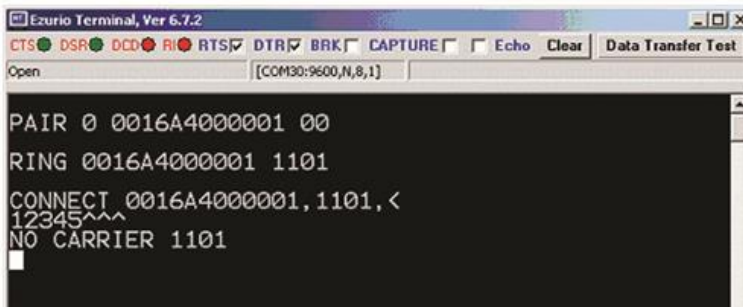
```
Ezurio Terminal, Ver 6.7.2
CTS DSR DCD RI RTS DTR BRK CAPTURE Echo Clear Data Transfer Test
Open [COM30:9600,N,8,1]
AT&F*
OK
ATS102=1
OK
ATS0=1
OK
AT&W
OK
ATZ
OK
AT+BTP
OK
ATI4
0016A4000002
OK
```

Figure 2-3: SPP Example – Preparation of Device B



```
Ezurio Terminal, Ver 6.7.2
CTS DSR DCD RI RTS DTR BRK CAPTURE Echo Clear Data Transfer Test
Open [COM24:9600,N,8,1]
AT+SPD0016A4000002
PAIR 0 0016A4000002 00
CONNECT 0016A4000002, 1101, >
67890
OK
AT+SPH
NO CARRIER 1101
```

Figure 2-4: SPP Example Device A - initiate connection, receiving data, command mode, disconnect



```
Ezurio Terminal, Ver 6.7.2
CTS DSR DCD RI RTS DTR BRK CAPTURE Echo Clear Data Transfer Test
Open [COM30:9600,N,8,1]
PAIR 0 0016A4000001 00
RING 0016A4000001 1101
CONNECT 0016A4000001, 1101, <
12345^^^
NO CARRIER 1101
```

Figure 2-5: SPP example Device B - Incoming connection, receiving data, disconnection

2.16.4 ATA {Accept Incoming SPP Connection Request}

Accept an incoming connection, which is indicated by the unsolicited string <cr,lf>RING 123456789012<cr,lf> every second (123456789012 is the Bluetooth address of the connecting device).

Response: <cr,lf>CONNECT 123456789012,1101,<<cr,lf>

2.16.5 AT+SPD<bd_addr> {Make Outgoing SPP Connection}

Initiate an SPP connection to a device with Bluetooth address <bd_addr> and SPP profile.

The timeout is specified by S register 505.

For backward compatibility, the following command fulfils the same purpose: ATD<bd_addr>.

Response: <cr,lf>CONNECT 123456789012,1101,><cr,lf>
Or <cr,lf>NO CARRIER<cr,lf>

Due to a known issue in the Bluetooth RFCOMM stack, it is not possible to make more than 65525 outgoing connections in a single power up session. Therefore, if that number is exceeded, the connection attempt fails with the following response:

Response: <cr,lf>CALL LIMIT
Or <cr,lf>NO CARRIER<cr,lf>

In that case, issuing an ATZ to reset the device resets the count to zero and more connections are possible.

2.16.6 AT+SPDL {Remake Connection}

Make a SPP connection with the same device as that specified in the most recent AT+SPD command. An error returns if the 'L' modifier is specified AND a Bluetooth address.

For backward compatibility, the following command fulfils the same purpose: ATDL

Response: <cr,lf>CONNECT 123456789012,><cr,lf>
Or <cr,lf>NO CARRIER<cr,lf>

2.16.7 AT+SPDR {Make SPP Connection to Peer Specified in AT+BTR}

Make a SPP connection with the device address specified in the most recent AT+BTR command. An error returns if the 'R' modifier is specified AND a Bluetooth address.

For backward compatibility, the following command fulfils the same purpose: ATDR

Response: <cr,lf>CONNECT 123456789012,><cr,lf>
Or <cr,lf>NO CARRIER<cr,lf>

2.16.8 AT+SPH {Drop SPP Connection}

Drop an existing SPP connection or reject an incoming connection indicated by unsolicited RING messages.

For backward compatibility, the following command fulfils the same purpose: ATH

Response: <cr,lf>NO CARRIER<cr,lf>

2.16.9 SPP – Incoming Connections

The Laird BTM device can be configured using the AT+BTP or AT+BTG command so that it scans for incoming connections from other Bluetooth devices. It can also be configured via S Register 512 to be in this mode by default on power up.

When the lower layers detect an SPP connection request, a RING 123456789012 string sends to the host every second. The command ATA is used to accept the connection and ATH to reject the request.

On connection, if the S0 Register is ≥ 0 then confirmation to the host is in the following format:

```
CONNECT 123456789012,1101,<
```

When S0 register is -1, neither RING nor CONNECT are sent to the host and the connection silently accepts.

If the S 100 register is non-zero, then after the ring indications specified by this register have been sent to the host, and the host fails to accept or reject the incoming connection, then an automatic 'hangup' is initiated.

2.16.10 SPP – Asynchronous Messages

RING

This string is sent to the host when a remote device initiates a serial port connection. The fully qualified string is in the form RING 012345678901, where 012345678901 is a 12 digit hexadecimal number which corresponds to the remote device's Bluetooth address. This response is sent to the host every two seconds until the host either accepts the connection using the ATA command or rejects it using the ATH command.

```
CONNECT 123456789012,1101,<
```

An SPP connection with Bluetooth device 123456789012 has been established successfully. The connection was initiated by the remote device (incoming).

```
CONNECT 123456789012,1101,>
```

An SPP connection with Bluetooth device 123456789012 has been established successfully. The connection was initiated by the local device (outgoing).

2.16.11 SPP – S Registers

S Registers for SPP are summarized in the following table:

Table 2-17: S Registers for SPP

Register	Default	Range	Description
S0	0	-1..15	Number of RING indication before automatically answering an incoming connection. A value of 0 disables autoanswer. If -1, then autoanswer on one RING and DO NOT send RING/CONNECT response to the host. This emulates a serial cable replacement situation. Setting values ≥ 0 resets S Register 504 to 0, and < 0 forces 504 to 1. If S0 $\neq 0$ and S100 $\neq 0$ then S0 must be $< S100$. If a value is entered which violates this rule, then ERROR 29 sends in response. If S504 = 1 then this register returns -1, regardless of the actual value stored in non-volatile memory.
S100	15	0..15	Number of RING indications before an auto disconnection initiates. A value of 0 disables this feature. If S0 $\neq 0$ and S100 $\neq 0$ then S0 must be $< S100$. If a value is entered which violates this rule, then ERROR 29 sends in response.

2.17 Hardware Units (BTM410 / 411)

This section covers S Registers and AT Commands that relate to hardware units of a BTM410 or BTM411 device. For this section, please refer to the Bluecore data sheet ([Reference 5](#)) for further information.

2.17.1 Codec Gain

The BTM410/411 can operate with an external PCM codec. Laird provides a number of different codec evaluation boards designed for use with the BTM410/411 development kit. For example, the ACC-05 is a codec evaluation board based around the Winbond W681360 codec [6]. The platform provides flexible support for different codec formats (μ -law, A-law and 13 bit linear). If 13 bit linear format is chosen, then the 13 bit sample transmits over the PCM interface as the MS 13 bits of a 16 bit word. The LS 3 bits may be used to control the output gain of the codec (for example on the Winbond W681360) and the AT software allows this output gain setting to be controlled using s-register 589 as described in [Table 2-18](#).

2.17.2 Hardware Units - S Registers

[Table 2-18](#) gives an overview on S Registers for hardware units except GPIO. For GPIO Registers please refer to [Table 2-19](#).

Table 2-18: S Registers for Hardware Units

Register	Default	Range	Description
S589	8	0..8	External codec output gain

2.17.3 GPIO (General Purpose Input/Output)

On a BTM410/411 device a number of digital I/Os can be used for general purposes. Each GPIO is assigned to an S-Register (S651 to S658) which is capable of both GPIO configuration (config mode) as well as single pin read/write access (r/w mode). The bitmask of the I/O pin for direct read/write access is 0x01. All configuration flags allocate to higher value bits. A bitmask for the I/O pin applies if S-Register 650 is set to 1. This will enable the user to access a GPIO-Pin directly by reading/writing 0 or 1. If the GPIO shall be configured, S650 must be set to 0 in order to obtain access to the GPIO configuration flags.

All logical GPIO lines can be read/written in one atomic step by new S-Register 670 at any time. Some GPIOs have an alternative function assigned. If the alternative function is enabled, the appropriate I/O Pin is not available as GPIO anymore. UART modem control functions are generally enabled per default. Wi-Fi coexistence functions are currently not used, but if they should be used or required in the future, the appropriate function cannot be moved to another I/O Pin. Hence it should be considered that no other user function is assigned to an I/O Pin if the coexistence functions are required. The following table lists all GPIOs and their alternative functions.

It is currently not possible to disable UART modem control functions (RI/DCD/DTR/DSR) in order to use these pins as GPIO. As a result, only four GPIOs (3..6) are actually available for free configuration.

Table 2-19: GPIO - Alternative Functions BTM410/411

GPIO Pin (BTM410/411)	Alternative Function	
	Modem Control Line ⁽¹⁾	Wi-Fi Coexistence ⁽²⁾
GPIO1	RI	-
GPIO2	DCD	-
GPIO3	-	BT_Priority / Ch_Clk

GPIO Pin (BTM410/411)	Alternative Function	
	Modem Control Line ⁽¹⁾	Wi-Fi Coexistence ⁽²⁾
GPIO4	-	BT_Active / BT_State
GPIO5	-	Wlan_Active
GPIO6	-	Rf_Active
GPIO7	DTR	-
GPIO8	DSR	-

(1) Alternative functions for modem control lines are fixed. A modem control line cannot be used as GPIO.

(2) Recommended pin assignment, not configurable by S-Registers, please contact Laird Technologies if coexistence is required.

Table 2-20: GPIO configuration register

Bit	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
	function mapping code							reserved		FMS	NEN	INV	DIR	PS		
Default	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

Table 2-21: GPIO Configuration Register Field Descriptions

Field	Description
0 – PS	I/O Pin State – returns the current state of the I/O pin (0/1) when read. A write affects the I/O pin directly if DIR=1 and FMS=0 (FMS_NONE).
1 – DIR	Direction – controls if the I/O pin is an input or an output. 0 input 1 output
2 – INV	Inversion – controls if the I/O pin is inverted or not. Applies to both pin directions (read and write). 0 not inverted 1 inverted
3 – NEN	Notification enable – sends a notification to the host via UART on each status change. Applies to both pin directions (input and output). AT&W and ATZ are required for a new setting to become effective. Notification format: “\r\nGPIOx,y\r\n” x=GPIO index [1..8]; y=new pin state [0..1] with INV flag applied 0 disable notification 1 enable notification
[4:5] – FMS	Function Mapping Select – Selects modem control function or Function Mapping Code 0 FMS_NONE – function mapping disabled 1 FMS_MODEMCTRL – use GPIO as modem control line ⁽¹⁾ 2 Reserved (attempt to write this value will cause ERROR 02) 3 FMS_MAPCODE – bits [8:15] specify Function Mapping Code
[6:7]	Reserved
[8:15] Function mapping code	A Function Mapping Code is set in this bit field. The pin carries out the assigned operation. A mapped function does not affect any other flag of the GPIO configuration register. So, DIR and INV must be set manually according to the selected function and hardware requirements. Valid only if FMS==3.

(1) read only

Value	Function Mapping Code – Input
0x00	Cable Replacement TX
0x01	RFC_RTC_TX ⁽¹⁾
0x02	RFC_RTR_TX ⁽¹⁾
0x03	RFC_IC_TX ⁽¹⁾
0x04	RFC_DV_TX ⁽¹⁾
0x05	Volume down single step ⁽²⁾
0x06	Volume up single step ⁽²⁾
0x07	Volume down multiple after short press ⁽²⁾
0x08	Volume up multiple after short press ⁽²⁾
0x09	Volume down multiple after medium press ⁽²⁾
0x0A	Volume up multiple after medium press ⁽²⁾

(1) disabled, reserved for future usage

(2) applies to SCO connection with external codec board

Value	Function Mapping Code – Output
0x00	Cable Replacement RX
0x01	RFC_RTC_RX ⁽¹⁾
0x02	RFC_RTR_RX ⁽¹⁾
0x03	RFC_IC_RX ⁽¹⁾
0x04	RFC_DV_RX ⁽¹⁾

(1) Disabled, reserved for future usage.

Table 2-22: GPIO S registers

Register	GPIO	Default	Range	Description
S650		0	0..1	Mode for GPIO Config Registers: 0 = no mask 1 = enable i/o pin state mask
S651	GPIO1	0x0000	0..0xFFFF	GPIO Configuration Registers S650 must be set to 0 to enable configuration access. Controls Pin State, Pin Direction, Pin Inversion, Function Mapping Enable, Function Mapping Select and Function Mapping Code. See Table 2-20 .
S652	GPIO2			
S653	GPIO3			
S654	GPIO4			
S655	GPIO5			
S656	GPIO6			
S657	GPIO7			
S658	GPIO8			
S669	GPIO1..8	0x0000	0..0xFF	Enable strong bias (=strong pull up / strong pull down) if GPIO is configured as input, bitmask: 0x0001: GPIO1; 0x0002: GPIO2; 0x0004: GPIO3; 0x0008: GPIO4 0x0010: GPIO5; 0x0020: GPIO6; 0x0040: GPIO7; 0x0080: GPIO8

Register	GPIO	Default	Range	Description
S670	GPIO1..8	0x0000 (depending on wiring and configuration)	0..0xFF	Read/Write all GPIOs in one atomic step (Write operation only affects GPIOs configured as outputs) 0x0001: GPIO1 0x0002: GPIO2 0x0004: GPIO3 0x0008: GPIO4 0x0010: GPIO5 0x0020: GPIO6 0x0040: GPIO7 0x0080: GPIO8

2.18 Miscellaneous

2.18.1 SCO / eSCO Audio Link

BTM modules provide an AT command to establish an SCO / eSCO audio connection between a pair of BTM modules (or BISM2). This enables the user to create bidirectional audio links independently from a particular Bluetooth profile. The only prerequisite is the existence of a RFCOMM link (SPP) between the modules. If this link doesn't exist, it can be created using AT+SPD<BdAddr>.

A SCO/eSCO link is intended for bidirectional transmission of speech. The sampling rate is fixed to 8 kHz, meaning a usable bandwidth of 3.5 kHz.

For SCO, there are three packet types defined in the Bluetooth specification [1]: HV1, HV2, HV3. Each occupies one slot. They differ in the level of bit error checking. We recommend that you enable all three packet types for SCO links; this will pass the final decision down to the baseband. There is no retransmission of erroneous SCO packets.

For eSCO and basic data rate, there are three packet types defined in the Bluetooth specification [1]: EV3, EV4, EV5. EV3 occupies one slot, EV4 and EV5 can occupy up to three slots each. They differ in the level of bit error checking. We recommend that you enable all three packet types for eSCO links. This will pass the final decision down to the baseband. eSCO packets involve a CRC code and retransmission of erroneous eSCO packets.

Packet types and link types (SCO or eSCO) are negotiated on link setup. A BTM can accept either incoming SCO or eSCO links (S register 584), but not both SCO and eSCO at one time. If the initiating side requests an unsupported link type, the audio link will fail. The initiating BTM module is supposed to request the remaining link type in that case.

Table 2-23 lists all AT commands and S-Registers for SCO/eSCO links.

Table 2-23: SCO/eSCO AT-commands and S-Registers

Task	AT-Command/S-Register	Comment
Initiate SCO link	AT+BTAx	x = packet type bitmask, recommended value = 7 1 = HV1 2 = HV2 4 = HV3
Initiate eSCO link	AT+BTA100x	x = packet type bitmask, recommended value = 7 1 = EV3 2 = EV4 4 = EV5

Task	AT-Command/S-Register	Comment
Release SCO/eSCO link	AT+BTA0 / AT+BTA	
Initiate SCO/eSCO link	AT+BTA8	Link type (SCO/eSCO) and packet types defined by S584.
Enable either SCO or eSCO for incoming requests and for AT+BTA8	S584 [0..1]	0 = SCO (HV1,HV2,HV3) enabled 1 = eSCO (EV3,EV4,EV5) enabled Only one link type can be enabled at one time.
Initiate SCO/eSCO link automatically on each SPP link	S532 [0..7]	The recommended value to enable this feature is 7. Value = bitmask for packet type. The link type (SCO/eSCO) is defined by S584. 0 : Feature disabled 1 : HV1 (S584=0) or EV3 (S584=1) 2 : HV2 (S584=0) or EV4 (S584=1) : HV3 (S584=0) or EV5 (S584=1)

2.18.2 SCO / eSCO Asynchronous Messages

The following asynchronous messages apply to SCO/eSCO connections.

AUDIO ON (SCO)

This response sends to the host when a SCO channel is established.

AUDIO ON (eSCO)

This response is sent to the host when a eSCO channel is established.

AUDIO OFF

This response is sent to the host when an existing SCO/eSCO channel closes.

AUDIO FAIL

This response is sent to the host when a SCO channel setup fails. This might be caused by the fact that the peer only accepts eSCO connections but a SCO connection was requested or vice versa. Please try to initiate the SCO connection with the remaining link type.

2.18.3 Link Key Management

On a BTM device, AT firmware manages link keys. Appropriate AT commands are described in [Section 2](#). There is a range of S Registers defining the behaviour of automatic link key storage on incoming/outgoing and dedicated/general bonding.

2.18.4 Dedicated Bonding

In BT2.1 specification, “dedicated bonding” is defined as the exchange of link keys between two devices without the intention of establishing a connection immediately.

Dedicated bonding is initiated by “AT+BTW<BdAddr>” (initiation of pairing).

2.18.5 General Bonding

In BT2.1 specification, “general bonding” is defined as the exchange of link keys between two devices with the intention of establishing a connection immediately. This is the case if a device tries to connect to another device without an existing link key. Hence, pairing (authentication and exchange of link keys) initiates automatically prior to the connection.

General bonding initiates by a connection requesting AT command if there is no link key for the peer device existing. Such AT commands are:

"AT+SPD<BdAddr>", "AT+APD<BdAddr>", "AT+AVD<BdAddr>", "AT+HSD<BdAddr>",
 "AT+HSGD<BdAddr>", "AT+HFD<BdAddr>", "AT+HFGD<BdAddr>", "AT+DUD<BdAddr>"

2.18.6 Automatic Storage of Link Keys

Four S Registers define the automatic storage of link keys in the trusted device list, depending on incoming/outgoing and general/dedicated bonding. See [Table 2-24](#).

Table 2-24: Automatic storage of link keys

Task	S-Register	Comment
Automatic link key storage on dedicated bonding outgoing (DBO)	S325 [0..1]	0 = do not store (cache only) 1 = store automatically (default) identical with S538
Automatic link key storage on general bonding outgoing (GBO)	S326 [0..1]	0 = do not store (cache only) 1 = store automatically (default)
Automatic link key storage on dedicated bonding incoming (DBI)	S327 [0..1]	0 = do not store (cache only) 1 = store automatically (default)
Automatic link key storage on general bonding incoming (GBI)	S328 [0..1]	0 = do not store (cache only) 1 = store automatically (default)

2.18.7 Profile Connection Status

The connection status of a profile can be queried by an AT-Command. This may help you decide whether to disconnect all connected profiles (via ATH*) or a certain one. For details, see

[Table 2-25](#).

Table 2-25: Profile connection status

Task	AT-Command	Comment
Get connection status of SPP	ATI60	0 = not connected 1 = connected (local command mode) 2 = connected (remote command mode) identical with ATI9
Get connection status of A2DP	ATI61	0 = not connected 1 = connected
Get connection status of AVRCP	ATI62	0 = not connected 1 = connected
Get connection status of HSP-Headset	ATI63	0 = not connected 1 = ACL connected 2 = audio connected
Get connection status of HSP-AG	ATI64	0 = not connected 1 = ACL connected 2 = audio connected
Get connection status of HFP-HF	ATI65	0 = not connected 1 = SLC connected 2 = audio connected 3 = in call, SLC

Task	AT-Command	Comment
		4 = in call, audio
Get connection status of HFP-AG	ATI66	0 = not connected 1 = SLC connected 2 = Audio connected 3 = in call - SLC 4 = in call – audio
Get connection status of DUN	ATI67	0 = not connected 1 = connected

2.18.8 Disconnecting Profiles

A connection to a profile can be released by "ATH<Profile-UUID>". For A2DP and AVRCP this provides a second way to disconnect. The response on a disconnect command is usually "NO CARRIER <profileUUID>" if a connection has existed and S329=0. If no connection has existed and S329=0, no profileUUID is appended. If all connections are to be released, ATH* may be used. See the following table.

Table 2-26: Profile release commands

Task	AT-Command	Comment
Disconnect SPP	ATH1101 or AT+SPH or ATH	Single "ATH" retained for backward compatibility, response "NO CARRIER" or "NO CARRIER 1101" depending on S329 and if a SPP connection has existed previously.
Disconnect A2DP	ATH110D or AT+APH	If A2DP connection released: response = "NO CARRIER 110D"; If no A2DP connection has existed: response = "NO CARRIER".
Disconnect AVRCP	ATH110E or AT+AVH	If AVRCP connection released: response = "NO CARRIER 110E"; If no AVRCP connection has existed: response = "NO CARRIER".
Disconnect HSG	ATH1112 or AT+HSGH	If AG(HSP) connection released: response = "NO CARRIER 1112"; If no HSP connection has existed: response = "NO CARRIER".
Disconnect HS	ATH1108 or AT+HSH	Must be enabled by S332 because it would result in a behaviour not defined in HSP specification. If HS(HSP) connection released: response = "NO CARRIER 1108"; If no HSP connection has existed: response = "NO CARRIER".
Disconnect HFG	ATH111F or AT+HFGH	If AG(HFP) connection released: response = "NO CARRIER 111F"; If no HSP connection has existed: response = "NO CARRIER"
Disconnect HF	ATH111E or AT+HFH	If HF(HFP) connection released: response = "NO CARRIER 111E"; If no HSP connection has existed: response = "NO CARRIER"
Disconnect all profiles listed in this table	ATH*	Response: NO CARRIER <ProfileUUID>" for each previously connected profile or NO CARRIER" if no existing connection found or HS connected but S332=0

2.18.9 Legacy Response Format (BISM2)

Some BISM2 responses have slightly changed on BTM modules in order to provide enhanced functionality. If required, a BISM2 compatible response format can be enabled by S Register 329.

Table 2-27 shows the implications of enabled/disabled legacy response format.

Table 2-27: Enabling/disabling legacy response format

Task	S-Register	Comment
Enable legacy response format (BISM2 compatible)	S329 [0..1]	0 = disabled (default) 1 = enabled

Table 2-28: Implications of S329

Command	Legacy response format enabled (S329=1)	Legacy response format disabled (S329=0)
"AT+SPH"; "ATH1101"	Response = "NO CARRIER"	If SPP is connected, response = "NO CARRIER 1101" If SPP is not connected, response = "NO CARRIER"
"AT+APH"; "ATH110D"	Response = "NO CARRIER"	If A2DP is connected, response = "NO CARRIER 110D" If A2DP is not connected, response = "NO CARRIER"
"AT+AVH"; "ATH110E"	Response = "NO CARRIER"	If AVRCP is connected, response = "NO CARRIER 110E" If AVRCP is not connected, response = "NO CARRIER"
"AT+HSH"; "ATH1108"	Response = "NO CARRIER"	If HS instance is connected, response = "NO CARRIER 110E" If HS instance is not connected, response = "NO CARRIER"
"AT+HSGH"; "ATH1112"	Response = "NO CARRIER"	If HSG instance is connected, response = "NO CARRIER 1112" If HSG instance is not connected, response = "NO CARRIER"
"AT+HFH"; "ATH111E"	Response = "NO CARRIER"	If HF instance is connected, response = "NO CARRIER 111E" If HF instance is not connected, response = "NO CARRIER"
"AT+HFGH"; "ATH111F"	Response = "NO CARRIER"	If HFG instance is connected, response = "NO CARRIER 111F" If HFG instance is not connected, response = "NO CARRIER"
"AT+DUH"; "ATH1103"	Response = "NO CARRIER"	If DUN is connected, response = "NO CARRIER 1103" If DUN is not connected, response = "NO CARRIER"

2.18.10 Page Scan / Inquiry Scan Interval and Window

Page scanning means being connectable; inquiry scanning means being discoverable. With the following S registers, the power consumption of the BTM can be influenced. However, lower power consumption means longer connection establishment time and longer time until a BTM is discovered by other devices.

The page scan window defines the time for the module to look out for incoming connection requests (paging). The inquiry scan window defines the time for the module to look out for incoming inquiry requests (device discovery). If the module is both connectable and discoverable (S12=4 or AT+BTP issued), it mutually does page scanning and inquiry scanning as shown in Figure 2-6. If connectable only, the module performs page scanning only (repeatedly) and if discoverable only, then the module performs inquiry scanning only.

S register 508 defines the page scan interval in ms, range is [11..2250].

S register 509 defines the page scan window in ms, range is [11..2250].

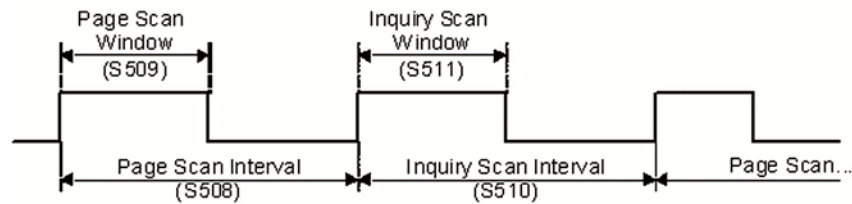


Figure 2-6: Page Scanning intervals

2.18.11 Sniff Mode

Bluetooth connections are master/slave in nature. A master sends packets and a slave must acknowledge that packet in the next timeslot. Timeslots in Bluetooth are 625 microseconds wide. This implies that a master always knows when packets are sent and received, which also means it is able to optimize power usage by switching on power hungry circuitry only when needed. A slave does NOT have prior knowledge of when a packet will be received and has to assume that a packet is received from a master on every receive slot. This means that it has to leave its receiving circuitry on for most of the receive slot duration. The result of this is high power consumption on the slave side. In general, a slave draws about five times the current of a master. This problem was identified very early in the evolution of Bluetooth (especially since headsets spend all their time as a slave in a Bluetooth connection) and it is solved by a mode called Sniff, with appropriate lower layer negotiating protocol.

Sniff mode during connection is an agreement between the slave and its master that data packets only exchange for N timeslots every M slots. The slave can then assume that it will never be contacted during M-N slots, and so can switch its power hungry circuitry off. The specification goes further by also specifying a third parameter called 'timeout' (T) which specifies 'extra' timeslots that the slave agrees to listen for after receiving a valid data packet. Put another way, if a slave receives a data packet, then it knows that it MUST carry on listening for at least T more slots. If within that T slot time period it receives another data packet, then the timer restarts. This mechanism ensures low power consumption when there is no data transfer – at the expense of latency. When there is a lot of data to transfer, it acts as if sniff mode is not enabled.

During sniff mode, a slave listens for N slots every M slots. The Bluetooth specification states that a master can have up to seven slaves attached to it with all slaves requesting varying sniff parameters. It may therefore be impossible to guarantee that each slave gets the M parameter it requests. In light of this, the protocol for enabling sniff mode mandates that a requesting peer specify the M parameter as a minimum and maximum value. This allows the master to interleave the sniff modes for all attached slaves.

For this reason, the sniff parameters are specified in the BTM module via four S registers. S Register 56 specifies 'N'; S Register 562 specifies 'T'; and S Registers 563/564 specifies minimum 'M' and maximum 'M' respectively. Although the specification defines these parameters in terms of timeslots, the S register values must be specified in units of milliseconds and the firmware does the necessary translation to timeslots.

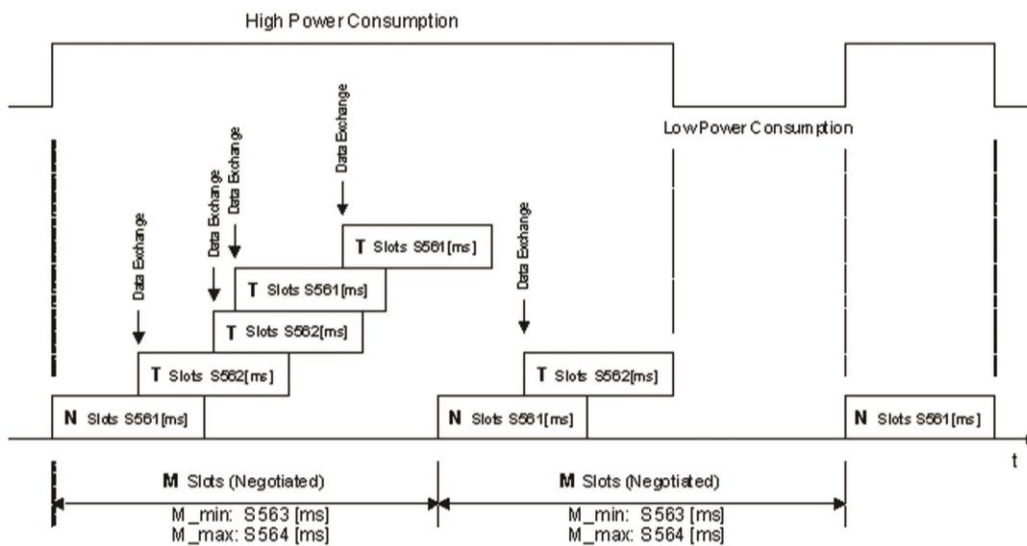


Figure 2-7: Sniff Mode example

Sniff Mode can be optimized for power savings. In general:

- Be aware that power savings trades off against data latency.
- If possible, always enable sniff mode, at least with a small sniff interval (20..50ms, e.g. AT564=20).
- Set the timeout value to about 30% to 50% of the sniff interval (e.g. AT562=5, see Section 2.18.13).
- Keep the attempt parameter at minimum (AT561=2).

Sample AT script (assuming factory default settings):

Comment	Sniff interval=30ms (recommended)	Sniff interval=100ms (recommended if longer latency acceptable)
Attempt	AT561=2	AT561=2
Timeout	AT562=5(*)	AT562=20(*)
Min. sniff interval	AT563=20	AT563=90
Max sniff interval	AT564=30	AT564=100
Save settings	AT&W	AT&W

(*) for firmware v16.1.3.1, see section 2.18.13.

For future firmware versions, please consult the firmware release notes for fixed bugs.

In addition, if more efforts can be spent on low power optimisation:

- Characterise the expected data: amount, timing, maximum acceptable delay.
- Derive maximum SSR latencies and SSR timeouts.
- Derive a sniff interval which is a whole numbered common factor of SSR latency.
- Use delayed sniff mode requests (S364>0) only if the remote's end sniff parameters are not suitable for the application. Avoid this feature if possible (it is experimental and has not been tested against other devices than BTM41x).
- Verify actual parameters using AT+I commands (see examples).
- Optimise settings iteratively by doing current measurements, as proposed by the examples of this document.

For further information, see *Application Note – BTM41x Low Power Modes* on www.lairdtech.com/bluetooth.

2.18.12 Sniff Sub Rating

The sniff mode configuration registers S561, S562, S563 and S364 have been assigned a mapping according to table 2-29. A value is written in units of 1 ms. Although any value in the range [0...1600] is accepted, internally any written value is rounded to the nearest column "Read (ms)". Hence, it is recommended to write only values of the "Read (ms)" column in order to prevent confusion. The resulting number of slots and the resulting actual time is shown in Table 13 1 as well. The duration of a Bluetooth slot is fixed at 0.625 ms. To convert a value from ms to slots, multiply the value by 1.6.

The sniff sub-rating (SSR) configuration registers S348, S349 and S350 have been assigned a mapping according to Table 13 2. A value is written in units of 0.1s. Although any value in the range [0..170] is accepted, internally any written value is rounded to the nearest of column "Read (ms)". Hence, it is recommended to write only values of the "Read (ms)" column in order to prevent confusion. The resulting number of slots and the resulting actual time is shown in Table 13 2 as well. The duration of a Bluetooth slot is fixed at 0.625 ms. To convert a value from ms to slots, multiply the value by 1.6.

Table 2-29: Sniff register mapping S [561...564]

Write (ms)	Read (ms)	No. of Slots	Actual ms	Write (ms)	Read (ms)	No. of Slots	Actual ms
[0, 1]	0	0	0	[95, 149]	100	160	100
[2, 3]	2	4	2.5	[150, 249]	200	320	200
[4, 6]	5	8	5	[250, 349]	300	480	300
[7, 8]	7	12	7.5	[350, 449]	400	640	400
[9, 11]	10	16	10	[450, 549]	500	800	500
[12, 13]	12	20	12.5	[550, 649]	600	960	600
[14, 16]	15	24	15	[650, 749]	700	1120	700
[17, 18]	17	28	17.5	[750, 849]	800	1280	800
[19, 24]	20	32	20	[850, 949]	900	1440	900
[25, 34]	30	48	30	[950, 1049]	1000	1600	1000
[35, 44]	40	64	40	[1050, 1149]	1100	1760	1100
[45, 54]	50	80	50	[1150, 1249]	1200	1920	1200
[55, 64]	60	96	60	[1250, 1349]	1300	2080	1300
[65, 74]	70	112	70	[1350, 1449]	1400	2240	1400
[75, 84]	80	128	80	[1450, 1549]	1500	2400	1500
[85, 94]	90	144	90	[1550, 1600]	1600	2560	1600

Table 30: Sniff sub-rating (SSR) register mapping S [348..350]

Write (0.1 s)	Read (0.1 s)	No. of Slots	Actual s	Write (0.1 s)	Read (0.1 s)	No. of Slots	Actual s
[0]	0	0	0	[38, 42]	40	6400	4
[1]	1	160	0,1	[43, 47]	45	7200	4,5
[2]	2	320	0,2	[48, 52]	50	8000	5
[3]	3	480	0,3	[53, 57]	55	8800	5,5
[4]	4	640	0,4	[58, 64]	60	9600	6
[5]	5	800	0,5	[65, 74]	70	11200	7
[6]	6	960	0,6	[75, 84]	80	12800	8
[7]	7	1120	0,7	[85, 94]	90	14400	9
[8]	8	1280	0,8	[95, 104]	100	16000	10
[9]	9	1440	0,9	[105, 114]	110	17600	11
[10, 12]	10	1600	1	[115, 124]	120	19200	12
[13, 17]	15	2400	1,5	[125, 134]	130	20800	13
[18, 22]	20	3200	2	[135, 144]	140	22400	14
[23, 27]	25	4000	2,5	[145, 154]	150	24000	15
[28, 32]	30	4800	3	[155, 164]	160	25600	16
[33, 37]	35	5600	3,5	[165, 170]	170	27200	17

For further information, see *Application Note – BTM41x Low Power Modes* on www.lairdtech.com/bluetooth.

2.18.13 S561 and S562 bug in firmware v16.1.3.1

Note: S561, S562: An issue was observed with firmware v16.1.3.1: Sniff parameters “Attempt” (S561) and “Timeout” (S562) result in double the expected value. For example, if set to 30 the actual time is 60 ms instead of 30 ms.

2.18.14 Maximum RF-Tx Power Level

The maximum RF transmit power level for all operation states (inquiring / connecting / in connection) is controlled by S541 / S542.

2.18.15 Manufacturing Info String

A string with manufacturing information can be retrieved by “ATi200”.

2.18.16 Bluetooth Version

The Bluetooth version can be queried by “ATi18”.

2.18.17 Legacy Issues (BT2.0)

There are some special cases if a legacy device (BT2.0 or earlier, e.g. BISM2) requests a connection to a BTM device (BT2.1).

General bonding does not work if initiated by the legacy device. Instead, the legacy device must initiate dedicated bonding first (=pairing, BISM2: "AT+BTW<BdAddr>"). After successful pairing, the connection can be initiated by the legacy device (BISM2: "ATD<BdAddr>").

2.18.18 Factory Default UART Baud Rate

BTM devices are capable of operating at a wide range of baud rates. S Registers 520 and 521 allow the baud rate to be set.

As long as the equation $BAUDRATE * 0.004096$ produces an integer value, then there is 0% error in clocking for that baud rate.

It is possible to set a baud rate that a PC cannot cope with; in that circumstance, communication is virtually impossible. In this circumstance, the BTM device comes out of reset using 9600,N,8,1 comms settings for exactly 750 milliseconds and then reverts to the communication parameters as per the S registers.

If the host sends the string !<BISM>!<cr> where <cr> is the carriage return character within the 750 ms period, the module remains at 9600,N,8,1 and configures itself using factory default S register values.

If connected to a PC using Laird (Ezurio) Terminal, the module can be reset to the factory default baud rate as follows:

- Right click in the Laird (Ezurio) Terminal window → Factory Default → Via BREAK/CMD @ 9600 (Tested with version 6.7.2 of Laird (Ezurio) Terminal).

2.18.19 RI dependent Start-up Mode

The UART_RI line can be configured as an input and on power up its state can be used to force the device into one of two modes, defining discoverability and connectability states. See description for S Registers 565 to 569 inclusive in [Table 3-1](#) for more details.

For example, the feature could allow a device to make an outgoing connection if RI is in one state and be ready for an incoming connection in the other.

2.18.20 Reset via BREAK

The module can be reset by sending a BREAK signal. A BREAK signal exists when the module's UART_RX input is in a non-idle state (0v) for more than 125 milliseconds.

Laird (Ezurio) Terminal provides a BREAK capability which is used to reset a connected BTM device by ticking and un-ticking the BRK field. See [Figure 2-8](#).

BTM410/411

Bluetooth® AT Data Module User Guide

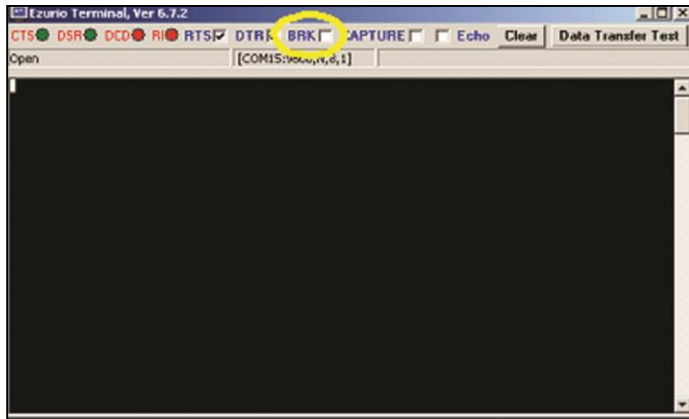


Figure 2-8: BREAK capability in Ezurio Terminal

2.18.21 Append Bluetooth Address to Friendly Name

If S Reg 593 is set to 1, then the last six hex digits of the Bluetooth address automatically appends to the friendly name. This allows the differentiation of multiple devices in the same neighbourhood with the same name.

3. APPENDIX

3.1 S Registers

The following table lists all S Registers.

Table 3-1: BTM41x - S Registers

Register	Default	Range	Category	Description
S0	0	-1..15	SPP	Number of RING indication before automatically answering an incoming connection. A value of 0 disables autoanswer. If -1, then autoanswer on one RING and DO NOT send RING/CONNECT response to the host. This emulates a serial cable replacement situation. Setting values ≥ 0 , resets S Register 504 to 0 and < 0 forces 504 to 1. If S0 $\neq 0$ and S100 $\neq 0$ then S0 must be $< S100$. If a value is entered which violates this rule, then ERROR 29 sends in response. If S504 = 1 then this register returns -1, regardless of the actual value stored in non-volatile memory.
S2	94	32..126	Misc.	Escape sequence character. It is not '+' by default as a Bluetooth® serial link can be used to connect to a mobile phone which exposes an AT command set, which in turn uses '+' as default. If both used '+', there will be confusion. 0x5e is the character '^'.
S12	100	40..5000	Misc.	Escape sequence guard time in milliseconds with a granularity of 20 ms. New values round down to the nearest 20 ms multiple.
S100	15	0..15	SPP	Number of RING indications before an auto disconnection initiates. A value of 0 disables this feature. If S0 $\neq 0$ and S100 $\neq 0$ then S0 must be $< S100$. If a value is entered which violates this rule, then ERROR 29 sends in response.
S101	\$1101	\$0..\$ffff	Misc.	UUID of default SPP based profile when not specified explicitly in the ATD command.
S102	\$0001	1..1	Misc.	Defines a set of bit masks for enabling profiles. Values can be ORed. A profile enables only if it is supported by the BTM variant. Issue AT&W and ATZ in order to make the new setting effective. As BTM41x supports SPP only, 0x0001 is the only possible value. 0x001: Serial Port Profile.
S103	1	1..4	Misc.	Boot Mode on cold boot. Boot modes are required to configure some low level device settings which cannot be configured by S registers and AT commands. Currently there are predefined settings defining the PCM data format to be used with certain codec ICs (applies mainly to BC04). 1 – normal. 2..4 – for future customization of the module.

Register	Default	Range	Category	Description
S319	0	0..1	SPP	SPP smart disconnect. 0 = disabled (default) 1 = enabled With this setting, BTM41x detects if there is any data pending in its internal buffers on an incoming disconnect notification. If so, then BTM41x delays the disconnection until all pending data is delivered to the UART first and then signals the disconnection on UART ("NO CARRIER") and on DCD line. This is an experimental feature which may have side effects in certain situations. It was created as the result of fixing bug [Ref. 2-19 / 285].
S320	2	1..3	SSP	Security Level: see Reference 1 , vol3, Generic Access Profile - Table 5.7 needs subsequent 'AT&W' and power cycle to take effect value = 3 overwrites S322
S321	1	0..4	SSP	Set IO capability: 0 – display only 1 – display yes/no 2 – keyboard only 3 – no input/no output 4 – reject IO-cap requests
S322	0	0..1	SSP	Force man-in-the-middle-protection (MITM): 0 – disabled 1 – enabled Referenced only if security level (S320) < 3
S323	0	0..1	SSP	Disable legacy (pre-BT2.1) Pairing: 0 – legacy pairing enabled 1 – legacy pairing disabled
S324	90	1..255	SSP	Secure Simple Pairing timeout in s. This value must be at least 60 in order to meet the recommendation of BT2.1 specification.
S325	1	0..1	Misc.	Store link key automatically on dedicated bonding outgoing (DBO).
S326	1	0..1	Misc.	Store link key automatically on general bonding outgoing (GBO).
S327	1	0..1	Misc.	Store link key automatically on dedicated bonding incoming (DBI).
S328	1	0..1	Misc.	Store link key automatically on general bonding incoming (GBI).
S329	0	0..1	Misc.	Enable legacy (BISM2) response format.
S330	1	1..31	Misc.	Configure inquiry response of AT+BTI (Bitmask): 1 - show device address 2 - show class of device 4 - show friendly name 8 - show extended inquiry data Values can be ORed.

Register	Default	Range	Category	Description
S331	2	0..2	Misc.	Direction indication style for "CONNECT" messages: 0 – Disabled. 1 – Character style: append 'I' to incoming and 'O' to outgoing CONNECT message, separated by a comma. 2 – Symbol style: append '<' to incoming and '>' to outgoing CONNECT message, separated by a comma. Applies only to role indicating UUID (e.g.HSP/HFP) and if S329=0.
S334	0	0..1	Misc.	Enable Extended SDP Error Codes: 0 - disable 1 – enable
S348		0..170	Sniff SSR	Sniff sub-rating (SSR) maximum listening interval. Unit – 0.1 seconds.
S349		0..170	Sniff SSR	Remote sub-rating (SSR) timeout. Unit – 0.1 seconds.
S350		0..170	Sniff SSR	Local sniff sub-rating (SSR) timeout. Time before changing from sniff mode to sniff sub-rating when no data is being transmitted. Unit – 0.1 seconds.
S356	0	0..3	Pairing	Identical to S358; not recommended for use due to consistency issue (different function of this SReg on BTM51x). Please use S358 instead.
S358	0	0..3	Pairing	Simple default PIN code (legacy pairing): 0 (default) = feature disabled 1 = "0000" 2 = "1234" 3 = "8888" This register only references on a PIN code request and if no persistent PIN code is stored in the module (see AT159 in Table 3-2). It allows catering for simple commonly used PIN codes by many BT2.0 devices. If the feature is disabled (value=0) and no persistent PIN code is available, then the PIN code request forwards to the module's host by the asynchronous "PIN?" message.
S359	3	0..3	SPP	Auto-BTX on SPP connection: 0 = do not change discoverable and connectable state when entering or exiting SPP connection. 1 = make the module not discoverable and not connectable when entering SPP connection (Bit 0). 2 = restore discoverable/connectable state according to S512 when exiting SPP connection (Bit 1). 3 = combination of both 1 and 2.
S364	0	0..31		Duration of initial power mode is s.

Register	Default	Range	Category	Description
				0 = indefinite (default)
S365		0..31		Duration of initial power mode in s. 0 = passive 1 = active Ignored if sniff mode is enabled (S561>0 and S364=0)
S366	0	0..1		Reboot on error 11 (error writing to PS store) 0 = Ignore error 11 1 = Reboot on error 11
S392	0	0..1		Delayed <i>NO CARRIER</i> message 0 – Send <i>NO CARRIER</i> immediately 1 = Send <i>NO CARRIER</i> delayed by 200 ms
S393	0	0..1		ACL release daemon 0 = Disable 1 = Enable
S394	0	0..15		System slowdown 0 = Disabled 1..15 = Enabled – The higher the number, the more the processor is kept busy
S395	0	0..7		Post connect lock (PCL) delay 0 = Disabled 1..7 = Additional delay (multiples of 100 ms) inserted after the <i>CONNECT</i> message before an incoming RFCOMM connection is permitted to send data.
S411	1400	200..1600	GPIO	Short press duration in ms; 200 ms granularity.
S412	2500	500..4000	GPIO	Component of medium press duration in ms, 500 ms granularity; actual value is this value plus S411; actual value is returned by AT+I412.
S413	2000	500..4000	GPIO	Component of long press duration in ms, 500 ms granularity; actual value is this value plus S411 + S412; actual value is returned by AT+I413.
S504	0	0..1	Misc.	Enable silent operation: Setting to 1 forces S0 to -1 and suppresses messages arising from connections or pairing. E.g. <i>CONNECT</i> , <i>NO CARRIER</i> , <i>RING</i> , <i>PAIR</i> etc. Suppressing connection based messages allows the device to configure in cable replacement mode.
S505	10	2..120	Misc.	Minimum delay before abandoning connection attempt as a master. Referenced by ATD. In units of seconds. See S Registers 530 and 543 in Table 3-1 . Please note that as disconnection time can vary, this register only guarantees the minimum delay. Note that for invalid addresses specified in the ATD command, the “ <i>NO CARRIER</i> ” response is immediate. See S register 560 in Table 3-1 for specifying disconnect max timeout

Register	Default	Range	Category	Description
S506	0	0..1	Misc.	Enable/Disable echoes. The ATEn command also affects this.
S507	0	0..2	Misc.	<p>When set to 0, a connection can be dropped using ^^^ escape sequence only and the state of DSR line is ignored. When set to 1 a connection can be dropped using EITHER the ^^^ escape sequence OR the DSR handshaking line. When set to 2, a connection can only drop using a deassertion of DSR. Mode 2 provides for the highest data transfer rate.</p> <p>If the status of the DSR line is conveyed to the remote device as a low bandwidth signal then this register MUST be set to 0, otherwise a deassertion of DSR is seen as a request to drop the Bluetooth® connection. This register affects S Register 536 – see details of 536 in Table 3-1.</p>
S508	640	11..2550	Misc.	Page Scan Interval in milliseconds. Minimum is 11.25ms so 10/11 ms gives 11.25 ms; see Section 2.18.10 .
S509	160	11..2550	Misc.	Page Scan Window in milliseconds. Minimum is 11.25 ms so 10/11 ms gives 11.25 ms; see Section 2.18.10 .
S510	640	11..2550	Misc.	Inquiry Scan Interval in milliseconds. Minimum is 11.25 ms so 10/11 ms gives 11.25 ms; see Section 2.18.10 .
S511	160	11..2550	Misc.	Inquiry Scan Window in milliseconds. Minimum is 11.25 ms so 10/11 ms gives 11.25 ms; see Section 2.18.10 .
S512	1	0..7	Misc.	<p>Specify power up state.</p> <p>When set to 0, AT+BTO is required to open the device for Bluetooth® activity.</p> <p>When set to 1, it proceeds to a state as if AT+BTO was entered.</p> <p>When set to 2, it is discoverable only, similar to issuing AT+BTQ.</p> <p>When set to 3, it is connectable but not discoverable; e.g. AT+BTG</p> <p>When set to 4, it is connectable and discoverable; e.g. AT+BTP.</p> <p>When set to 5, it is like 2, but all UART Rx traffic discards in absence of a connection while DSR asserts. If DSR does not assert, then it behaves exactly as per mode 2.</p> <p>When set to 6, it is like 3, but all UART Rx traffic discards in absence of a connection while DSR asserts. If DSR does not assert, then it behaves exactly as per mode 3.</p> <p>When set to 7, it is like 4, but all UART Rx traffic discards in absence of a connection while DSR asserts. If DSR is does not assert, then it behaves exactly as per mode 4.</p> <p>Note that by implication, a change to this can only be seen after a power cycle AND if AT&W was issued beforehand.</p>
S514	10	1..60	Pairing	Pairing Timeout in seconds. This includes the time a host takes to supply the PIN number when PIN? messages are indicated.

Register	Default	Range	Category	Description
S515	\$001F0 0	\$000000.. \$FFFFFF	Misc.	<p>Default Device Class Code. When queried, the value is always printed as a hexadecimal number.</p> <p>To change the device class of the module temporary and immediately without power cycle, use the command AT+BTC.</p> <p>To change the device class of the module permanently, write the new value to this S Register (ATS515=\$<devclasshex>), save the setting (AT&W) and initiate a power cycle (ATZ).</p>
S516	\$00000 0	0.. \$2FFFFFF	Misc.	<p>Default Device Class filter to be used with AT+BTI when it is not explicitly specified. When queried, the value is always printed as a hex number.</p> <p>The seventh most significant digit can be 0, 1, or 2, and is used to specify the type of device class filter.</p> <p>When 0, it specifies no filtering.</p> <p>When 1, it specifies an AND mask and all 24 bits are relevant.</p> <p>When 2, it specifies a filter to look for devices with matching major device class which occupies a 5 bit field from bits 8 to 12 inclusive (assuming numbering starts at bit 0). All other 19 bits MUST be set to 0.</p>
S517	20	2..61	Inquiry	Inquiry Length in units of seconds. This parameter is referenced by the AT+BTI command.
S518	8	0..255	Inquiry	<p>Maximum number of responses from an inquiry request. This parameter is referenced by the AT+BTI command. If this number is set too high, then AT+BTI returns ERROR 27. For a particular firmware revision, determine the effective maximum value by trial and error. That is, set to a high value, send AT+BTI and if ERROR 27 returns, then retry with a smaller value.</p> <p>This effective max value remains unchanged for that particular firmware build.</p>
S519	500	100.. 3000	Misc.	When S507>0, and in a connection, DSR can be used to change from data to command state by de-asserting the DSR line for less than the time specified in this register. This value is rounded down to the nearest 100 ms.
S520	9600	1200.. 115200	UART	<p>Change to a standard baud rate. The effect is immediate and in fact the OK is sent at the new baud rate. Only one of the following baud rates are accepted: 1200,2400,4800,9600,19200,28800,38400,5760,115200.</p> <p>If S register 525=1, then the maximum baud rate limits to 115200.</p>
S521	9521	1200.. 921600	UART	Change baud rate to non-standard value. BTM modules support any baud rate. The only limitation is the integer arithmetic involved, which may adjust the applied rate slightly. If the internally computed baud rate is more than 2% offset from the desired input value, then an ERROR

Register	Default	Range	Category	Description
				<p>returns and the old baud rate prevails. To inspect the actual baud rate, do AT+SM521?</p> <p>S521 should only be used for non-standard baud rates. For standard baud rates, use S520.</p> <p>The effect is immediate and the OK sends at the new baud rate.</p> <p>If S Register 525=1, then the max baud rate limits to 115200.</p> <p>In the event that a non-standard baud rate is requested, it is entirely possible that the host is not capable of generating such a baud rate. In this case the BTM device cannot communicate. If this happens, there is a procedure to recover from this situation which is described in Section 2.18.18.</p>
S523	1	1..2	UART	<p>Number of stop bits.</p> <p>See S Register 526 in Table 3-1 for further information.</p>
S524	0	0..2	UART	<p>Parity. 0=None, 1=Odd, 2=Even</p> <p>For the Go blue Activator variant of the module this register is read only.</p> <p>See S Register 526 in Table 3-1 for further information.</p>
S525	0	0..1	UART	<p>Apply multiplier of 8 to baud rate internally. This is set to 0 (disabled) by default. If S Register 521 > 115200 then this register cannot be set to 1.</p> <p>See S Register 526 in Table 3-1 for further information.</p>
S526	3	1..3	UART	<p>This register specifies a 2 bit mask used to qualify how S Registers 520 to 525 are actioned.</p> <p>If bit 0 is 1, the new communication parameters affect the UART immediately.</p> <p>If bit 1 is 1, the new communication parameters are stored in non-volatile memory.</p> <p>So for example, to change communication parameters but have them come into effect only after subsequent power cycles, then this register should be set to 2; and likewise to affect immediately and yet not have it persist over a power cycle, the value should be set to 1. Must be set before the baud rate change.</p>
S530	1000	100..1500 0	Misc.	<p>Reconnect delay when configured as master in pure-cable-replacement mode. This value rounds down to the nearest 100 ms. See S Register 505 in Table 3-1.</p>

Register	Default	Range	Category	Description
S531	0	0..4	Misc.	Specifies the mode on connection establishment. 0 = Normal, that data is exchanged between UART and RF. 1 = LOCAL_COMMAND. UART input is parsed by the AT interpreter and RF data is discarded. 2 = REMOTE_COMMAND. RF input is parsed by the AT interpreter and UART data discards. If S Register 536 is not 1 then this register cannot be set to 2 and an ERROR returns. 3 = LOCAL_COMMAND. UART input is parsed by the AT interpreter and incoming RF data is sent to the host using the RX<string> asynchronous response. 4 = LOCAL_COMMAND and on the rf side, the GPIO is automatically sent when there is a change in input. (digital I/O cable replacement mode)
S532	0	0..7	SCO	If non-zero, then on every connection, a SCO channel (audio) initiates. Bit 0 for HV1, Bit1 for HV2 and Bit2 for HV3. When the connection is lost, the SCO channel disappears along with it.
S535	20	0..41	Misc.	Link Supervision Timeout. If units go out of range, then a NO CARRIER message sends to the host after the time specified here.
S536	0	0..1	Misc.	When set to 1, a remote device can 'capture' the AT parser of this unit by sending this module an escape "!!!" sequence. The inter character timing is set via S Register 12. If S Register 507 is >= 2, then reading this register always returns 0, and writing 1 results in ERROR 33.
S539	0	0..1	UART	When set to 1, in idle mode (S512=1), UART Rx characters discard if DSR de-asserts.
S541	20	-43..20	Misc.	This sets the power level in dBm when inquiring or paging. Reading this register returns the value stored in non-volatile memory.
S542	4	-43..20	Misc.	As per S541, however reading this register returns the current power level as set in the base band. The read can be different from S541 because the actual power is set using a lookup table and the base band rounds down to the nearest value in the table.
S543	0	0..1	Misc.	If this is set to 1, then incoming pairing attempts are accepted (if a pin code has been pre-entered using AT+BTK) while in the wait phase of auto connect cycle initiated by the AT+BTR command. In addition to accepting pairing attempts, if the pairing is successful, then the new device automatically sets as the peer address for automatic connections (as if an explicit AT+BTR command was entered). See S Register 505 and 530 in Table 3-1 .
S544	1	0..1	UART	Configure UART for either high throughput or low latency:

Register	Default	Range	Category	Description
				0 = low latency, low throughput 1 = high latency, high throughput
S551	\$3211	\$0..\$ffff	SPP	<p>This register specifies in each 4 bit nibble, how the outgoing modem status bits to the remote peer gets its value. Bluetooth® allows for RTR, RTC, DV and IC bits to be exchanged over an RFCOMM connection.</p> <p>Nibble 0..3 specify the source for RTC. 4..7 specify the source for RTR. 8..11 specify the source for DV (i.e. DCD). 12..15 specify the source for IC (i.e. RI).</p> <p>Each nibble can take the following value:</p> <ul style="list-style-type: none"> 0 – Always set to 0. 1 – Always set to 1. 2 – If DCD (pin 8 on module connector) is output, then always 1. If DCD is input then 1 if DCD asserts, otherwise 0. 3 – If RI (pin 6) is output then always 0. If RI is input then 1 if RI asserts, otherwise 0. 4 – If DSR (pin 10) asserts then 1, otherwise 0. <p>In the event that a nibble specifies DSR as the source of its state, be aware that if S Register 507 is anything other than 0, a de-assertion of DSR causes the Bluetooth connection to drop. If bits 0..3 and 4..7 are set to 0, then some Bluetooth devices will use that as a signal to stop sending any data back.</p>
S552	\$0122	\$0..\$fff	SPP	<p>This register specifies in each 4 bit nibble, how the DTR, DCD, and RI output pins are controlled when in a Bluetooth connection.</p> <p>Nibble 0..3 specifies the source for DTR. 4..7 specifies the source for DCD. 8..11 specifies the source for RI.</p> <p>Each nibble can take the following value:</p> <ul style="list-style-type: none"> 0 – DO NOT touch the I/O. 1 – Always deassert. 2 – Always assert. 3 – If RTC bit in CONTROL_IND is 1 then assert, otherwise deassert. 4 – If RTR bit in CONTROL_IND is 1 then assert, otherwise deassert. 5 – If DV bit in CONTROL_IND is 1 then assert, otherwise deassert. 6 – If IC bit in CONTROL_IND is 1 then assert, otherwise deassert. <p>If this register changes while in command and connected mode, then on going back online using the ATO command, the modem output lines refresh.</p>

Register	Default	Range	Category	Description
S553	\$0201	\$0..\$fff	SPP	<p>This register specifies in each 4 bit nibble, how the DTR, DCD, and RI output pins are controlled when NOT in a Bluetooth connection.</p> <p>Nibble 0..3 specify the source for DTR. 4..7 specify the source for DCD. 8..11 specify the source for RI.</p> <p>In addition, it also refers to S Register 552 to see if the relevant pin is an input or not to be touched. If the nibble in 552 is 0, then the relevant pin is an input.</p> <p>Each nibble can take the following value:</p> <ul style="list-style-type: none"> 0 – Always deassert. 1 – Always assert. 2 – Assert if RING is being sent to the host.
S554	0	0..900	Misc.	<p>Post Reset Window: If S Register 512 ≥ 2 and ≤ 7, then this register specifies a time in seconds for which the device stays in the S512 mode after power up or reset. On timeout, it aborts the discoverable and/or connectable and fall back into S512=1 mode, when it is deaf and dumb (not connectable, not discoverable).</p> <p>Note: If AT+BTR is used to specify a peer device, then on reverting to mode 1, it attempts to make a connection to that peer device. A power cycle, reset via BREAK or ATZ is required to see the effects of change.</p>
S555	1	1..7	Misc.	<p>If S Register 554 is nonzero, then after the post reset (defined by S554) window expires, the mode will revert to the mode specified in this register. This allows, for example, the device to be discoverable and connectable on power up (mode 4 or 7) and on window timer expiry to revert to connectable only (mode 3 or 6).</p> <p>A power cycle, reset via BREAK or ATZ is required to see effects of a change. In some firmware builds, S Registers 565 to 569 inclusive are visible, which allows the start-up mode to depend on the state of RI line (Setting S Reg 565 forces the RI pin configure as an input). For this feature to be active, SReg 565 should be set to 1. In that case, on start-up and if RI is asserted, then the start-up mode is defined by S Reg 568; if de-asserted then S Reg 569.</p>
S558	0	0..1	Misc.	<p>When 1, the following responses; "RING", "NO CARRIER" and "CONNECT" are replaced by "BTIN", "BTDOWN" and "BTUP" respectively. This eliminates ambiguity when the module has a Bluetooth connection to an AT modem that also gives these responses.</p>
S559	0	0..3	Misc.	<p>This specifies a mask. When Bit 0 is 1, the response word "ERROR" is replaced by "BTERR" and "OK" is replaced by "ok".</p> <p>When Bit 1 is 1, then error responses do not include the error number and instead the error number is retrieved</p>

Register	Default	Range	Category	Description
				using AT112.
S560	15	15..120	Misc.	Disconnect timeout in seconds. This timer specifies how long to wait for confirmation from the peer device and/or the underlying stack that the connection is successfully torn down. There can be instances where a confirmation does not arrive and so in this case this timer is used to 'close off' the procedure and put the state machine back into a proper mode for new operations. Time is specified with 15 seconds intervals.
S561	0	0..1000	Sniff mode	Sniff Attempt Time in units of milliseconds. 0 means disable. See Section 2.18.11 .
S562	0	0..1000	Sniff mode	Sniff Timeout Time in units of milliseconds. 0 means disable. See Section 2.18.11 .
S563	0	0..1000	Sniff mode	Sniff Minimum Interval in units of milliseconds. 0 means disable. See Section 2.18.11 .
S564	0	0..1000	Sniff mode	Sniff Maximum Interval in units of milliseconds. 0 means disable. See Section 2.18.11 .
S565	0	0..1	Misc.	If set to 1, RI (Ring Indicate) line configures as an input and forces the start-up mode (SReg512) and post-timeout on Start-up mode (SReg555) to depend on the state of RI. The RI conditional modes are defined by S Registers 566 to 569 inclusive.
S566	1	1..7	Misc.	If S565=1, and RI is asserted, this is the mode the device starts up in.
S567	1	1..7	Misc.	If S565=1, and RI is de-asserted, this is the mode the device starts up in.
S568	1	1..7	Misc.	If S565=1, and RI is asserted, then this is the mode the device assumes after the post-start-up timeout defined in SReg 554, instead of mode defined in SReg555.
S569	1	1..7	Misc.	If S565=1, and RI is de-asserted, then this is the mode the device assumes after the post-start-up timeout defined in SReg 554 instead of mode defined in SReg555.
S584	0	0..1	Misc.	Enable/Disable eSCO.
S588	0	0..1	Misc.	After a disconnection, there is a cold reset.
S592	0	0..1	Misc.	Set this to 1 to reduce the trusted device database to just 1 record when auto saving of pairing is enabled via S reg 538.
S593	0	0..1	Misc.	Automatically append last 6 digits of local Bluetooth address to the Friendly name which was set via AT+BTN or AT+BTF.
S650	0	0..1	GPIO	GPIO pin state mask: 0 – No mask (enable configuration bit fields). 1 – Enable I/O pin state mask, disable configuration bit fields.
S651			GPIO1	GPIO Configuration Registers S650 must be set to 0 to

Register	Default	Range	Category	Description
S652	Depending on alternative GPIO usage and wiring	\$0..\$ffff	GPIO2	enable configuration access Controls Pin State, Pin Direction, Pin Inversion, Function Mapping Enable, Function Mapping Select and Function Mapping Code / av_operation_id. See Table 2-20 .
S653			GPIO3	
S654			GPIO4	
S655			GPIO5	
S656			GPIO6	
S657			GPIO7	
S658			GPIO8	
S669			\$0000	
S670	\$0000 (Depending on wiring and config)	\$0..\$ff	GPIO	Read/Write all GPIOs in one atomic step (write operation only affects GPIOs configured as outputs). 0x0001: GPIO1 0x0010: GPIO5 0x0002: GPIO2 0x0020: GPIO6 0x0004: GPIO3 0x0040: GPIO7 0x0008: GPIO4 0x0080: GPIO8
S1001 to S1010	0	0..2^32	Misc.	10 General Purpose 32 bit Registers for use by host. These are stored in non-volatile memory.

3.2 ATI Commands

The following table lists all ATI parameters supported by a BTM device. ATI commands provide general information about the BTM device and status information.

Table 3-2: BTM ATI Commands

Command	Information
AT10	The product name/variant.
AT11	The CSR firmware build number.
AT12	The AT firmware build number. For internal use only.
AT13	The AT firmware revision.
AT14	A 12 digit hexadecimal number corresponding to the Bluetooth address of the BTM device.
AT16	The maximum size of trusted device database.
AT17	The manufacturer of the Bluetooth chipset.
AT18	The chipset format.
AT19	SPP connection status: 0 – Not connected 1 – Connected in local command mode 2 – Connected in remote command mode
AT111	The reason why a “NO CARRIER” results in the most recent attempt at making an outgoing connection. The response values are as follows: 0 – No prior connection.

Command	Information
	1 – Connection timeout. 2 – Connection attempt cancelled. 3 – Normal disconnection. 4 – Peer device refused connection. 5 – Service profile <uuid> requested not available on remote device. 6 – Connection failed. 32 – ATH was entered. 33 – Incoming connection aborted because too many rings. 34 – Unexpected incoming connection. 35 – Invalid address. 36 – DSR is not asserted. 37 – Call limit of 65531 connections has been reached. 38 – Pairing in progress. 39 – No link key. 40 – Invalid link key. 255 – Unknown Reason.
ATI12	The last ERROR response number.
ATI13	The Sniff status is returned as follows: Response: <cr,lf>a:b,c,d,e<cr,lf> OK <cr,lf> Where: a: 0 when not online; 1 when online and sniff is enabled. b: Sniff attempt parameter. c: Sniff timeout parameter. d: Minimum sniff interval. e: Maximum sniff interval. All parameters 'b', 'c', 'd' and 'e' are given as Bluetooth slots which are 625 microseconds long converted from values of S Registers 561, 562, 563 and 564 respectively.
ATI14	The current boot mode.
ATI15	The maximum length of an AT command, not including the terminating carriage return.
ATI16	Codec Output Maximum Gain Range.
ATI17	Codec Input Maximum Gain Range.
ATI18	Bluetooth version.
ATI19	Audio connection status: 0 = Off 1 = On.
ATI20	Returns the number of bytes pending to send in the RF buffer when a connection is up.
ATI27	Current scan state: 0 = Not discoverable and not discoverable (not scanning). 1 = Discoverable (inquiry scanning). 2 = Connectable (page scanning). 3 = Discoverable and connectable (inquiry- and page-scanning).
ATI29	Maximum EIR data size in bytes.
ATI30	Current EIR RAM buffer length in bytes.
ATI31	Current EIR baseband buffer length in bytes.
ATI42	State information, where the response values are as follows:

Command	Information
	<p>13 = NotOpen 14 = OpenIdle 15 = Ringing 16 = OnlineCommand 172 to 177 = waiting for connectable and/or discoverable, where the lowest significant digit equates to the value stored in S Register 512 or 555.</p> <p>Note: When n=16, ATi9 returns 1.</p>
ATI43	<p>Query current role of SPP link: M = Master S = Slave ERROR 14 (incorrect mode) = No SPP link</p> <p>Normally, the initiating device becomes master of a link and the accepting device becomes the slave. If ATi144 returns the unexpected role, it is likely that a role change occurred.</p>
ATI44	<p>Query current power mode of SPP link (active/sniff/passive) and sniff interval. Response: <i><power_mode></i>, <i><sniff_interval_in_slots_decimal></i> <i><power mode></i>:</p> <p>0 = Active (highest power consumption, lowest latency) 1 = Sniff mode (power consumption and latency depend on sniff interval) 2 = Passive (the device will not initiate a change of the power mode)</p>
ATI45	<p>Query current sniff sub-rating (SSR) parameters of SPP link. Response: <i><flag></i>, <i><lfi></i>, <i><rli></i>, <i><lto></i>, <i><rto></i></p> <p><i><flag></i>: 1 = SSR Active; 0 = SSR Not Active <i><lfi></i>: Local listening interval, decimal integer, slots <i><rli></i>: Remote listening interval, decimal integer, slots <i><lto></i>: Local timeout, decimal integer, slots Time before changing from sniff mode to SSR when no data is being transmitted <i><rto></i>: Remote timeout, decimal slots Time before changing from sniff mode to SSR when no data is being transmitted</p>
ATI46	<p>Query current link policy power table. Response for each row: [<i><index></i>] <i><mode></i>, <i><time></i>, <i><min_int></i>, <i><max_int></i>, <i><attempt></i>, <i><timeout></i></p> <p><i><index></i>: Row index, starting with 0 <i><mode></i>: power mode, 0 = Active; 1 = Sniff; 2 = Passive <i><time></i>: duration of current row in s (switching to next row after this timeout) <i><min_int></i>, <i><max_int></i>: sniff mode intervals in slots, (S563 / S564, 'M') <i><attempt></i>: number of listening slots at sniff interval (S561, 'N') <i><timeout></i>: number of additional listening slots (S562, 'T')</p>
ATI59	<p>Returns '1' if a pre-set PIN code (by AT+BTK=" ... ") is available (legacy pairing). Returns '0' otherwise. The PIN code does display for security reasons.</p>
ATI60	<p>SPP connection status: 0 = Not connected 1 = Connected; identical with ATi9.</p>

Command	Information
ATI101	The RSSI value in dBm. If a connection does NOT exist, then a value of -32786 returns. A value of 0 means the RSSI is within the golden range. This is quite a large band, therefore RSSI is not always a useful indicator. Use ATI111 instead, which returns the bit error rate.
ATI111	Returns LinkQual which is defined in the CSR chipset as BER (bit error rate). This returns a value which is the number of bits in error out of 1 million. Hence a value of 0 is best, and larger values are worse. As the value approaches 1000 (BER = 0.1%) it is an indication that the link is very bad and a large number of Bluetooth packets are being lost.
ATI144	Like ATI44 but all values in ms rather than slots. Rounding indicated by!
ATI145	Like ATI45 but all values in ms rather than slots. Rounding indicated by!
ATI146	Like ATI46 but all values in ms rather than slots. Rounding indicated by!
ATI200	Manufacturing data (e.g. module serial number, manufacturing date).
ATI333	Full AT firmware version number.
ATI411	Short press duration in ms (S411).
ATI412	Medium press duration in ms (S411+ S412).
ATI413	Long press duration in ms (S411+ S412 + S413).
ATI1000	Available memory slots; diagnostic information to detect memory shortage or leaks.
ATI1001	Max. memory slot size; diagnostic information about maximum size of available memory slots.
ATI1003	Unique build number for BTM41x/BTM51x series.
ATI1005	Information related to write cycles left before flash defragmentation occurs.
ATI1006	Number of free bytes in current sink (UART or RFCOMM)
ATI1007	PSFlood only in debug mode
ATI1008	Similar to ATI1005 with different parameters
ATI1009	Similar to ATI1005 with different parameters
ATI1010	Similar to ATI1005 with different parameters

3.3 Error Responses

Table 3-3: BTM Error Responses

Error	Description
01	Register not recognized.
02	Value for register is out of range.
03	Incoming call NOT pending.
04	No call to connect to. This error code has meaning for ATO only.
05	Syntax error.
06	Empty string.
06	Device Class could not be stored.
08	Invalid Device Class code.
09	Invalid Bluetooth address.
10	Could not set Service or Friendly name.
11	PS Store Write.
12	PS Store Read.

Error	Description
13	Not idle.
14	Incorrect mode.
15	Already scanning.
16	Pairing is already in progress.
17	NOT USED.
18	NOT USED.
19	NOT USED.
20	Not safe to write to Non-volatile Store - Ongoing Bluetooth connection.
21	Link Key cache is empty.
22	Link Key database is full.
23	Malloc returned NULL - Resource issue.
24	Remote Address same as Local Address.
25	Connection setup fail, DSR not asserted.
26	Unauthenticated license.
27	Max responses too high (See S Register 518 in Table 3-1). Memory allocation error.
28	The length of Pin in AT+BTK is too long.
29	Invalid Ring count specified for S Register 0 or 100. If S0<>0 and S100<>0 then S0 must be < S100.
30	ADC error.
31	Analogue value cannot be read, as it is set for output.
32	Analogue value cannot be written, as it is set for input.
33	Invalid S register value.
34	Both L and R modifier cannot be specified in ATD command.
35	Invalid Major Device Class – valid value in range 0x00 to 0x1F inclusive.
36	Pairing in progress – command cannot be actioned – try again later.
37	Invalid sniff parameter specified. (E.g. new Attempt value greater than MinInterval. Solution is to first increase MinInterval and re-enter the Attempt value).
38	Get Remote Friendly name failed.
39	Failed to change mode to multipoint.
40	7 Bit mode requires parity to be even or odd.
41	Stream error.
42	Stream Pending error.
43	Unknown Audio Gateway command.
44	Busy; try later.
45	Command or operation not allowed.
46	N/A
47	N/A
48	N/A
49	N/A
50	N/A
51	N/A

Error	Description
52	N/A
53	N/A
54	No manufacturing information available.
55	Audio resource error.
56	Invalid UUID.
57	Maximum gain level reached.
58	Minimum gain level reached.
59	Profile or role not enabled.
60	Profile under construction.
61	Unknown Headset command.
62	Unknown Hands-free command.
63	Incorrect state.
64	Unknown DUN command.
65	UART resource error.
76	Memory allocation attempt was not successful.
79	Writing to modem control line is not permitted by GPIO S-register.
80	Attempt to write the pin state of a GPIO that is configured as input.
81	Maximum size of EIR data exceeded (AT129).

3.4 List of UUIDs

Table 3-4 gives a list of selected UUIDs. For a complete list, refer to the “Assigned Numbers – Service Discovery (SDP)” document (Reference 3) by the Bluetooth SIG.

Table 3-4: Selected UUIDs

UUID	Mnemonic / Profile	Role
0x1101	Serial Port Profile (SPP)	-
0x1102	LAN access using PPP	-
0x1103	Dial-up Networking (DUN)	-
0x1105	OBEX Object Push	-
0x1106	OBEX File Transfer	-
0x1108	Headset Profile (HSP)	Headset
0x110A	A2DP	Audio Source
0x110B	A2DP	Audio Sink
0x110C	AVRCP	Remote Target
0x110D	A2DP	-
0x110E	AVRCP	-
0x110F	AVRCP	Remote Controller
0x1112	Headset Profile	Audio Gateway
0x111E	Hands-free Profile (HFP)	Hands-free unit

BTM410/411

Bluetooth® AT Data Module User Guide

UUID	Mnemonic / Profile	Role
0x111F	Hands-free Profile (HFP)	Audio Gateway

3.5 References

1. "Bluetooth Specification Version 2.1 + EDR [vol3]", 26 July 2007
<https://www.bluetooth.org/Technical/Specifications/adopted.htm>
(click on "Core Specification v2.1 + EDR")
2. "Serial Port Profile" Specification
<http://www.bluetooth.com/Bluetooth/Technology/Works/SPP.htm>
(link at the bottom of page "Need more? View the Serial Port Profile (SPP)")
<https://www.bluetooth.org/Technical/Specifications/adopted.htm> (scroll down to section 'Traditional Profiles (Qualifiable)' -> SPP adopted version 1.1)
3. "Bluetooth Assigned Numbers"
<https://www.bluetooth.org/Technical/AssignedNumbers/home.htm>
Most interesting will be the links 'Baseband' and 'Service Discovery Protocol'
4. Class of Device Generator: this link might be helpful for creating a particular CoD
http://bluetooth-pentest.narod.ru/software/bluetooth_class_of_device-service_generator.html
Caution: this tool allows selection of more than one minor device classes, so make sure that only one minor device class is select and verify the result with [3] anyway.
5. "Bluecore 4 External" Data Sheet, Cambridge Silicon Radio (CSR)
<http://www.csrsupport.com> (log in or new account required)
6. "Winbond 681360 Codec Board User Guide", Ezurio Application Note
7. "FW_ReleaseNote_Btm41x_v16.1.3.0", Doc No: BTM41xv16.1.3.0
Information guide for Production and Engineering releases of firmware for part ~ BTM410 / BTM411.
8. "BTM411 Development Kit Quick Start SPP-v2" – SPP Quick Start Guide for BTM410 / BTM411.

BTM410/411

Bluetooth® AT Data Module User Guide

4. RELATED DOCUMENTS AND FILES

The following additional BTM410/411 technical documents are also available from the [Laird BTM41x Series product page](#) under the Documentation tab:

- Product Brief
- Hardware Integration Guide - Version 6.0
- Firmware Release Notes - Version 16.1.3.0
- BTM411 Development Kit Quick Start Guide SPP - Version 2
- Development Kit Schematics
- Quick Start Guide

For more information and support, visit the BTM41X series support page at https://laird-ews-support.desk.com/?b_id=1952.



Laird Technologies is the world leader in the design and manufacture of customized, performance-critical products for wireless and other advanced electronics applications. Laird Technologies partners with its customers to find solutions for applications in various industries such as:

- Network Equipment
- Telecommunications
- Data Communications
- Automotive Electronics
- Computers
- Aerospace
- Military
- Medical Equipment
- Consumer Electronics

Laird Technologies offers its customers unique product solutions, dedication to research and development, as well as a seamless network of manufacturing and customer support facilities across the globe.

LWS-GUIDE-BTM410-411

Copyright © 2013 Laird Technologies, Inc. All rights reserved. The information contained in this manual and the accompanying software programs are copyrighted and all rights are reserved by Laird Technologies, Inc. Laird Technologies, Inc. reserves the right to make periodic modifications of this product without obligation to notify any person or entity of such revision. Copying, duplicating, selling, or otherwise distributing any part of this product or accompanying documentation/software without the prior consent of an authorized representative of Laird Technologies, Inc. is strictly prohibited.

All brands and product names in this publication are registered trademarks or trademarks of their respective holders.

This material is preliminary. Information furnished by Laird Technologies in this specification is believed to be accurate. Devices sold by Laird Technologies are covered by the warranty and patent indemnification provisions appearing in its Terms of Sale only. Laird Technologies makes no warranty, express, statutory, and implied or by description, regarding the information set forth herein. Laird Technologies reserves the right to change specifications at any time and without notice. Laird Technologies' products are intended for use in normal commercial and industrial applications. Applications requiring unusual environmental requirements such as military, medical life-support or life-sustaining equipment are specifically not recommended without additional testing for such application.

Limited Warranty, Disclaimer, Limitation of Liability

global solutions: local support™