Bluetooth Location Tracker Protocol

CCC Camp 2003 / Congress 2003 (20C3)
Version 0.0.7

Authors:
Andreas "Steini" Steinhauser <steini@ccc.de>
Daniel Dorau <daniel.dorau@alumni.tu-berlin.de>
Collin Mulliner <collin@mulliner.org>

1 Introduction

Steini's Baustelle

2 BLT client protocol

2.1 Request

This message type instructs the BLT client to perform a specific action. Each request contains at least a command code (a ASCII string) followed by a message number.

2.1.1 Authentication

This command is used for requesting the client to authenticate.

Example:
req(authentication, 0)

2.1.2 Configuration

This command is used for configurating the basic Bluetooth functions of the BLT client. It contains the following parameters:

Inquiry Scan 1 to enable, 0 to disable Inquiry Scan on the BLT client

Page Scan 1 to enable, 0 to disable Page Scan on the BLT client

Page Timeout duration of a Page Scan in 1.28 second units

Device Name The Bluetooth device name of the BLT client, if empty don't change the current setting. The device name is enclosed in two ".

Example:
req(configuration, 1, 0, 0, 0x0A, "BLT_#1")

2.1.3 Inquiry

This command instructs the BLT client to perform an Bluetooth Inquiry. It contains the following parameters:

max. number of devices (as in HCI spec) the maximum number of devices that should be returned, should all ways be zero (0) to get all devices in range

max. inquiry time (as in HCI spec) the duration of the inquiry in 1.28 second units

Example:
req(inquiry, 2, 0, 0x30)

2.1.4 Name_Request

This command instructs the BLT client to request the Bluetooth Device Name of a given address. It contains the following parameter:

BD_ADDR the BD_ADDR (the Bluetooth device address) of the device to be queried.

Example:
req(name_request, 3, 00:11:22:33:44:55)

2.2 Confirmation

This is currently not used!
This message type confirms the reception of a request to the BLT server. The parameters are:

Request Name the request command name

Message Number the confirmed message number

Reason Code the HCI reason code

Example:
conf(name_request, 1, 0)

2.3 Indication

This message type asynchronously indicates events to the BLT server such as the completion of a command previously requested by the server.

2.3.1 Authentication

This message is send to the server to authenticate the current session. It the authentication is accepted nothing will happen, if the authentication is denied the connection will be closed by the server. It contains the following parameters:

Login the assigned login string

Password the assigned password

Example:
ind(authentication, 0, “blt_station_1“, “Hwas23a“)

2.3.2 Inquiry_Result_Event

This message is sent for each BD_ADDR discovered during a Bluetooth Inquiry. It contains the following parameters:

BD_ADDR The Bluetooth device address of the found device.

Class of device The Bluetooth class of the found device.

RSSI in dBm The signal quality.

Time stamp Time at which the device was found, the format is "MM.DD.YYYY HH:MM:SS".

Latitude The latitude part of the BLT clients GPS coordinate, multiplied with 100000.

Longitude The longitude part of the BLT clients GPS coordinate, multiplied with 100000.

Example:
ind(inquiry_result_event, 3, 00:12:34:56:78:90, 0xffd0, 0x123456, "07.22.2003 23:11:08", 3244214, 2361241)

2.3.3 Inquiry_Complete

This simple message is send to indicate that the inquiry procedure has been completed.

Example:
ind(inquiry_complete, 3)

2.3.4 Name_Request

This message contains the result of a Bluetooth Name Request. The parameters are:

BD_ADDR The Bluetooth device address.

Name The Bluetooth Device Name.

Normally the Name_Request is an answer to a Name_Request. But a Name_Request can also be triggered by a Bluetooth Device in field so it is valid (for the BLT client) to send this anytime he wants except during a running Inquiry.

Example:
ind(name_request, 1, 00:12:34:56:78:90, "JohnSmith")

3 BLT data protocol

3.1 Requests

3.1.1 Num_Total_Devices

This command is used to request a grand total number of currently seen devices.

The OUTPUT has the following parameter:

Number of Devices Total number of devices currently seen.

Example:
c: data(num_total_devices)
s: 532

3.1.2 Num_Devices_At

This command is used to request the number of devices seen by a specific cell.

The COMMAND has following parameters:

Latitude The latitude part of the BLT clients GPS coordinate, multiplied with 100000.

Longitude The longitude part of the BLT clients GPS coordinate, multiplied with 100000.

The OUTPUT as following parameters:

Number of Devices Number of devices currently seen by a specific cell.

Example:
c: data(num_devices_at, 2343243, 4323432)
s: 61

3.1.3 List_All_Devices

This command is used to request the position data of all devices. There can be more than one position for a single device, this normally means that this device is seen by more then one cell at the same time.

The OUTPUT has following parameters:

BD_ADDR The Bluetooth device address.

Device Name The name of the device.

Class of device The Bluetooth class.

RSSI in dBm The signal quality.

Time stamp Time at which the device was found, the format is "MM.DD.YYYY HH:MM:SS".

Latitude The latitude part of the BLT cell GPS coordinate, multiplied with 100000.

Longitude The longitude part of the BLT cell GPS coordinate, multiplied with 100000.

Example:
c: data(list_all_devices)
s: 00:11:22:33:44:55, "Heinz", 0xffd0, 0x143213, "07.25.2003 17:30:11", 3221332, 1321213
s: 00:99:88:77:66:55, "", 0xdfe0, 0x121231, "07.25.2003 17:30:23", 3244324, 4343232
s: data(list_end)

3.1.4 List_Devices_At

This command is used to request a list of all devices at a given position.

The COMMAND has the following parameters:

Latitude the latitude part of the BLT clients GPS coordinate, multiplied with 100000

Longitude the longitude part of the BLT clients GPS coordinate, multiplied with 100000

Example:
c: data(list_devices_at, 2343243, 2324332)
s: 00:11:22:33:44:55, "Heinz", 0xffd0, 0x143213, "07.25.2003 17:30:11", 2343243, 2324332
s: 00:99:88:77:66:55, "", 0xdfe0, 0x121231, "07.25.2003 17:30:23", 2343243, 2324332
s: data(list_end)

3.1.5 List_Device

This command is used to get the position of a unique device (selected by it's Bluetooth device address).

The COMMAND does have the following parameter:

BD_ADDR the BD_ADDR (the Bluetooth device address) of the device.

Example:
c: data(list_device, 00:11:22:33:44:55)
...
s: 00:11:22:33:44:55, "Fido", 0xffd0, 0x143213, "07.25.2003 17:30:11", 3221332, 1321213
s: 00:11:22:33:44:55, "Fido", 0xffd0, 0x143213, "07.25.2003 17:30:35", 3213213, 3221131

3.2 Push(Streaming)

3.2.1 Push_All_Devices

This command is used to tell the server that all device positions should be continually pushed to the client:

Example:
c: data(push_all_devices)
...
s: 00:11:22:33:44:55, "Heinz", 0xffd0, 0x143213, "07.25.2003 17:30:11", 3221332, 1321213
s: 00:99:88:77:66:55, "", 0xdfe0, 0x121231, "07.25.2003 17:30:23", 3244324, 4343232

3.2.2 Push_Devices_At

This command is used to tell the server that all device positions btw. all devices see at a distinct position should be pushed to the client.

The COMMAND does have the following parameters:

Latitude the latitude part of the BLT cells GPS coordinate, multiplied with 100000

Longitude the longitude part of the BLT cells GPS coordinate, multiplied with 100000

Example:
c: data(push_devices_at, 3221332, 1321213)
...
s: 00:11:22:33:44:55, "Fido", 0xffd0, 0x143213, "07.25.2003 17:30:11", 3221332, 1321213
s: 00:99:88:77:66:55, "Batman", 0xdfe0, 0x121231, "07.25.2003 17:30:23", 3221332, 1321213

3.2.3 Push_Device

This command is used to tell the server that only the position of a unique device (selected by it's hardware address) should be pushed to the client.

The COMMAND does have the following parameter:

BD_ADDR the BD_ADDR (the Bluetooth device address) of the device to follow.

Example:
c: data(push_device, 00:11:22:33:44:55)
...
s: 00:11:22:33:44:55, "Fido", 0xffd0, 0x143213, "07.25.2003 17:30:11", 3221332, 1321213
s: 00:11:22:33:44:55, "Fido", 0xffd0, 0x143213, "07.25.2003 17:30:35", 3213213, 3221131