# SonarPhone WiFi Communication

Jim McKeown

Last update: 23 December 2022


This document is based on observations of data sent between a mobile phone set as master and an SP200A SonarPhone. No other models were observed. The information in this document was verified by building an ESP32 microcontroller running as either a second master or stand-alone master client used to extract numerical depth data from from a SP-200A.

The Vexilar SP200A T-Box server communicates with the proprietary mobile phone application SonarPhone client via WiFi, SSID: T-BOX-720. UDP messages are initiated by the phone app client and are replied to by the T-Box server.

After a factory reset of the T-Box, the phone app is used to establish a single device as the master that controls the T-Box. Only the master can change settings such as max and min depth and beam width. Slave SonarPhone clients are able to view data from any T-Box server provided they have the WiFi password to join the T-Box device's network and the master client is already running. Slave clients are not able to change any settings.

The phone app requires the master client to enter a password to establish that device as the master client after a factory reset. However, the password is not actually used in authenticating communications between the master client and the T-Box server. Instead, the master client MAC address is stored in the SP200A server memory. Once a client is connected to the SP200A WiFi network, the master MAC address is the only information needed for any client to authenticate as the master client. A second master second master client may also authenticate while the actual phone app master is running.

The FX message is always exactly the same. Any client on the T-Box network can send this message to the T-Box server and get a reply.

FX request:

```
00 46 F
01 58 X
02 15 const
03 00 const
04 00 const
05 00 const
06 00 const
07 00 const
08 00 const
09 00 const
10 00 const
11 00 const
12 00 const
13 00 const
14 00 const
15 00 const

16 00 const
17 00 const
18 00 const
19 b3 179 checksum
20 00 const
21 00 const
22 00 const
23 00 const
24 00 const
25 00 const
26 00 const
27 00 const
28 00 const
```

This message is just ‘FX’ and some constants. Byte 19 (b3) is a checksum but it does not change because the other bytes do not change.

The server responds to the the FX message with a REDYFX reply. The REDYFX reply message contains the T-Box serial number and the master MAC address. If the master device has not yet been established since the last factory reset of the T-Box, the MAC address is reported as ‘11 11 11 11 11 11’.

Note that the T-Box may also respond to the FX message or any other message with a BUSY reply if the requested data is not immediately available.

BUSY:

```
00 ff const
01 00 const
02 ff const
03 00 const
04 0a const
05 00 const
06 42 B
07 55 U
08 53 S
09 59 Y
```

REDYFX:

```
00 ff const
01 00 const
02 ff const
03 00 const
04 20 const
05 00 const
06 52 R
07 45 E
08 44 D
09 59 Y
10 46 F
11 58 X
12 16 const
13 00 const
14 02 const
15 00 const

16 30 0--+
17 30 0  |
18 30 0  |
19 30 0  |
20 30 0  T-Box serial number
21 30 0  |
22 33 3  |
23 36 6  |
24 36 6  |
25 38 8--+
26 78 120 master mac address msb
27 62  98 master mac address 2nd msb
28 56  86 master mac address 3nd msb
29 6d 109 master mac address 3nd lsb
30 62  98 master mac address 2nd lsb
31 32  50 master mac address lsb
```

In this example the T-Box serial number is 0000003668 and the MAC address of the phone used to establish the master is 78:62:56:6d:62:32.

Using the master MAC address from the REDYFX reply, any client can construct a valid FC request. This message sets max and min depth, depth units and beam width and requests all data from the T-Box.

FC request:

```
00 46  70 F
01 43  67 C
02 15  21 const
03 00   0 const
04 f4 244 const
05 02   2 const
06 00   0 minimum depth, whole units, lower byte
07 00   0 minimum depth, whole units, upper byte
08 f0 240 maximum depth, whole units. lower byte, zero = auto range
09 00   0 maximum depth, whole units, upper byte
10 00   0 const
11 01   1 units, 0 = meters, 1 = feet
12 00   0 const
13 08   8 beam width. 08 = 20 degrees, 02 = 40 degrees
14 00   0 const
15 00   0 const

16 00   0 const
17 00   0 const
18 00   0 const
19 a7 167 checksum lower byte
20 01   1 checksum upper byte
21 78 120 master mac address msb
22 62  98 master mac address 2nd msb
23 56  86 master mac address 3nd msb
24 6d 109 master mac address 3nd lsb
25 62  98 master mac address 2nd lsb
26 32  50 master mac address lsb
27 00   0 const
28 00   0 const
```

The T-Box server responds to a valid FC request with a REDYFC message or BUSY if data is not yet available. The REDYFC message contains maximum and minimum depth, depth units (meters or feet), measured depth, measured temperature, measured battery voltage, beam width, part of the master MAC address, and 758 data points representing echo intensity over the maximum 80 meter depth range.

The REDYFC response is sent repeatedly by the T-Box server as fast as it can for at least 30 seconds after a FC request. Therefore, it is not necessary to send the FC request more than once every 30 seconds. Additional FC requests at intervals of less than 30 seconds will not result in any more data being sent by the T-Box server.

REDYFC response:

```
00 ff const
01 00 const
02 ff const
03 00 const
04 1c const
05 03 const
06 52 R
07 45 E
08 44 D
09 59 Y
10 46 F
11 43 C
12 12 const
13 03 const
14 f4 const
15 02 const

16 00 minimum range (lower byte) in whole units
17 00 minimum range (upper byte) in whole units (normally zero).
18 0a maximum range (lower byte) in whole units (0x0a = 9 dec) 00 = auto range.
19 00 maximum range (upper byte) in whole units (normally zero).
20 00 const
21 01 Depth units. 00 = meters, 01 = feet.
22 00 const
23 03 measured depth, whole units, lower byte
24 00 measured depth, whole units, upper byte
25 33 measured depth, fraction of units / 100. 0x33 = 51 dec = 0.51 units
26 12 measured temperature. always whole degrees C.
27 00 const
28 14 const
29 01 const
30 0e whole battery Volts (14 Volts)
31 4d fraction battery Volts / 100. 0x4d = 77 dec, 0.77 Volts

32 08 beam width 08 = 20 degrees, 02 = 40 degrees
33 62 master mac address 2nd msb
34 56 master mac address 3rd msb
35 6d master mac address 3rd lsb
36 62 master mac address 2nd lsb
37 32 master mac address lsb
38 e8 echo waveform. 758 data points over 80 meter maximum depth = 0.105540897
m/data point
39 e8 or 9.475 data points per meter
40 e8
41 e8
42 e8
43 e8
44 e8
45 e8
46 e8
47 e8
   .
   .
   .
795 01
```

There is also a FV message that is sent by the phone app client and replied to by the T-Box server with a REDYFV response. The purpose of this message is not clear but it is definitely not required for a stand-alone or second master to operate. It may be some kind of keep-alive or ping message. It does not seem to contain any useful information. A stand-alone and second master client has been successfully tested without using any FV message.  It is included here for completeness.

FV request:

```
00 46 F
01 56 V
02 15 const
03 00 const
04 00 const
05 00 const
06 00 const
07 00 const
08 00 const
09 00 const
10 00 const
11 00 const
12 00 const
13 00 const
14 00 const
15 00 const

16 00 const
17 00 const
18 00 const
19 b1 177 checksum
20 00 const
21 00 const
22 00 const
23 00 const
24 00 const
25 00 const
26 00 const
27 00 const
28 00 const
```

FV response:

```
00 ff const
01 00 const
02 ff const
03 00 const
04 10 const
05 00 const
06 52 R
07 45 E
08 44 D
09 59 Y
10 46 F
11 56 V
12 06 const
13 00 const
14 01 const
15 01 const
```