Modbus-RTU Master Protocol Documentation

Revision: 20.05
Date: 2020-05-04

www.iqhome.org

Contents

1. Introduction

IQ Home ModBus-RTU master device enables access to ModBus-RTU slave devices over IQRF Network. Using Modbus-RTU master device users are able to send Modbus RTU requests and receive Modbus RTU responses. The Modbus-RTU master device bridges the IQRF Network and the RS-485 communication Modbus-RTU network. The device implements slave role on IQRF Network side and Master role on RS-485 Modbus-RTU network side. ModBus-RTU master device can handle up to 31 slave devices on RS-485 Modbus-RTU network side.

1.1. IQRF DPA informations

RF Network	IQRF
IQRF OS	4.03D
IQRF DPA	4.11
IQRF RF Mode	STD + LP
Default RF Channel	Assigned at bonding time

HWPID															
15.	**14.**	**13.**	**12.**	**11.**	**10.**	**9.**	**8.**	**7.**	**6.**	**5.**	**4.**	**3.**	**2.**	**1.**	**0.**
Product code								Hardware revision				1	1	1	1

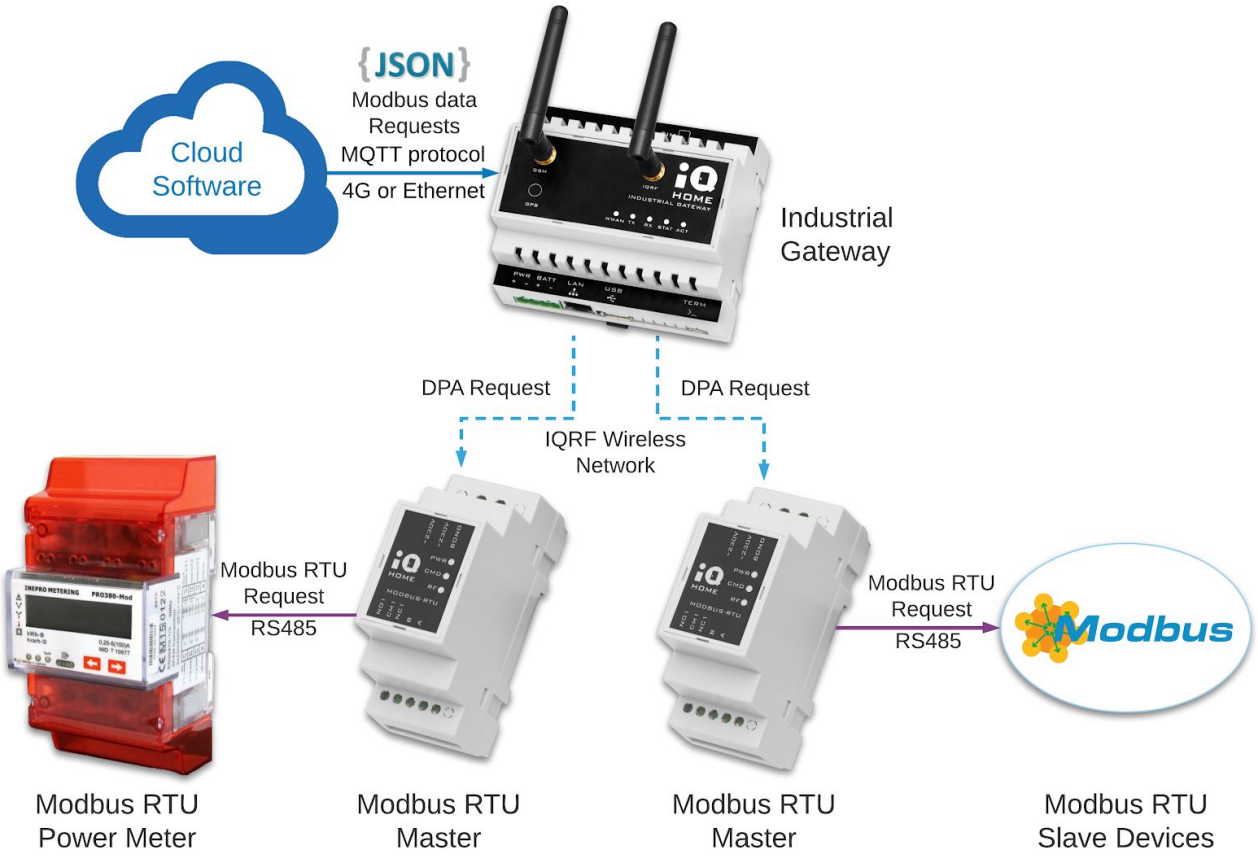
HWPIDver															
15.	**14.**	**13.**	**12.**	**11.**	**10.**	**9.**	**8.**	**7.**	**6.**	**5.**	**4.**	**3.**	**2.**	**1.**	**0.**
Year of build date							Month of build date				Day of build date				

1.2. Typical usage

With IQ Home ModBus-RTU master device the user can access and control ModBus-RTU devices from the cloud.

Typical request data flow:

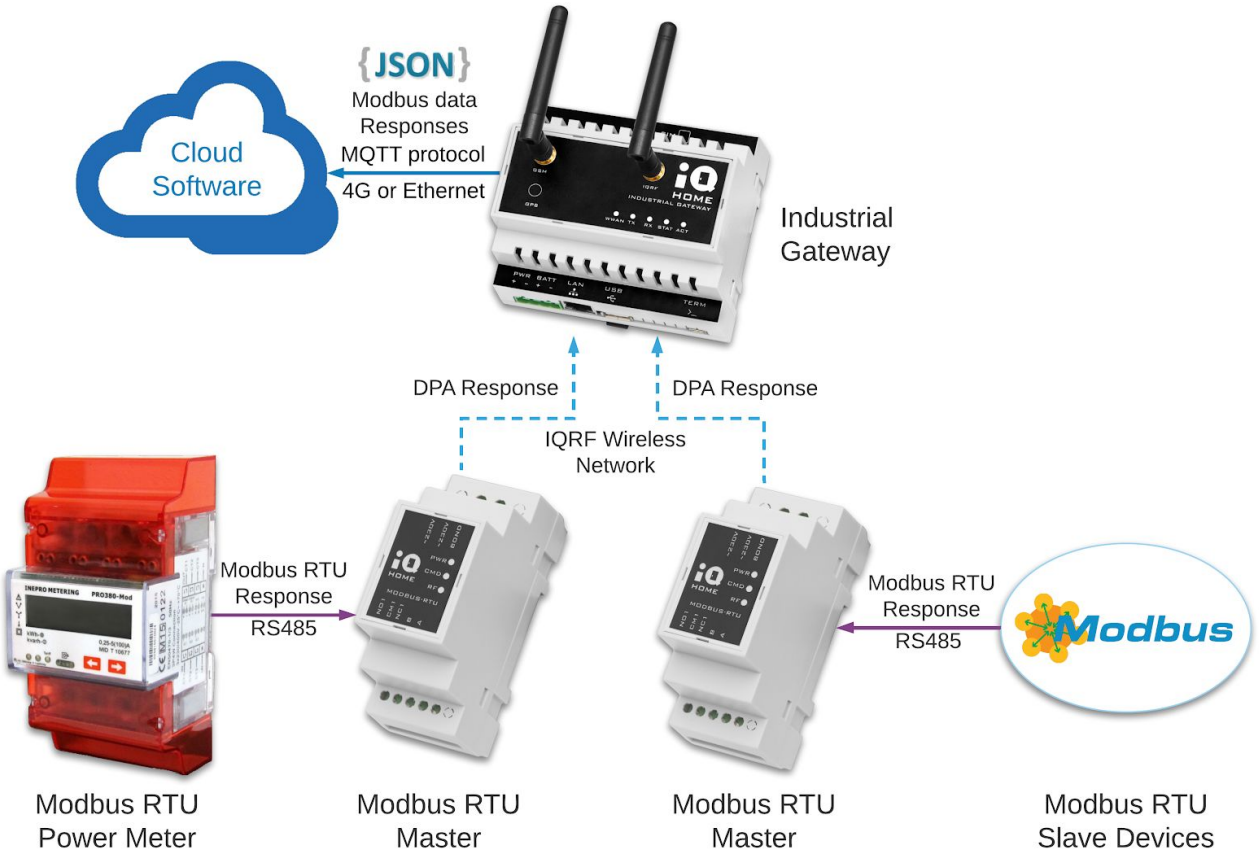
Cloud Software ➡ [Internet connection / MQTT protocol] ➡ **IQ Home Gateway** ➡ [IQRF Network] ➡ **IQ Home ModBus RTU Master** ➡ [Modbus RTU on RS485] ➡ **Modbus slave device**



Rerequest data flow

Typical response data flow:

Modbus slave device ➡ [Modbus RTU on RS485] ➡ **IQ Home ModBus RTU Master** ➡ [IQRF Network] ➡ **IQ Home Gateway** ➡ [Internet connection / MQTT protocol] ➡ **Cloud Software**



Response data flow

1.3. Main features

IQ Home Modbus-RTU master device main features:

- Modbus-RTU device calculates and checks the CRC-16 error check fields. Users don’t need to care about it.
- Modbus-RTU master device can address up to 31 slave devices. From slave device address 0x01 to 0x1F.
- Modbus-RTU master device can send broadcast messages. Broadcast address is 0x00.
- Automatic Time-Out control. Modbus-RTU master device generates time-out response, if the device doesn't receive any response from the slave device.
- Automatic Request resend mechanism. Modbus-RTU master device automatically re-sends the Modbus-RTU request, if the device doesn't receive any response or receives corrupted response from the slave device.
- Modbus-RTU master device communicate with two different mode:
    - 1 start bit
      8 data bits, least significant bit sent first
      1 bit for Even parity (default)
      1 stop bit

    - 1 start bit
      8 data bits, least significant bit sent first
      2 stop bits (no parity)

- Modbus-RTU master device can communicate with different Baud rates. Supported Baud rates:
    - 1200
    - 2400
    - 4800
    - **9600 (default)**
    - 19200
    - 38400
    - 57600
    - 115200

1.4. Modbus message structure

Modbus-RTU Message consists of three main parts:

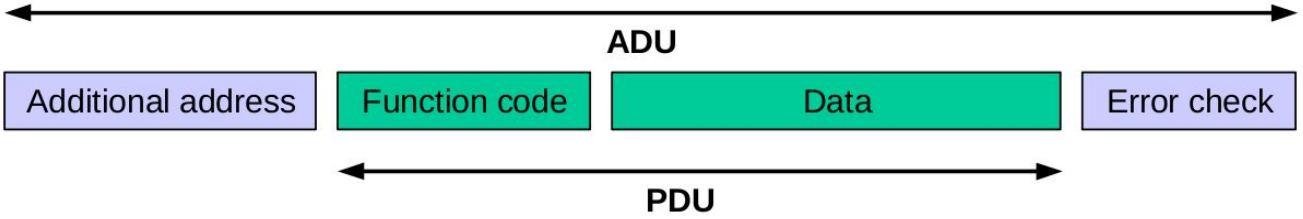
- Address field
- Protocol data unit (PDU)
- CRC-16 Error check

The full modbus-RTU Message is named application data unit (ADU) in official Modbus documentation.

Protocol data unit (PDU) consists of two main parts:

- Function code byte
- Data

Next picture shows the structure of Modbus-RTU Message:



With 0x38 PNUM code can user send and receive Modbus-RTU messages:

- PCMD byte contains the Modbus-RTU slave device address. The device address can be 0x01 to 0x1F
- PDATA contains the Modbus protocol data unit (PDU)

1.5. Additional information

More information about PDU data format, please read the offical MODBUS Protocol Specification: www.modbus.org/docs/Modbus_Application_Protocol_V1_1b3.pdf

IQ Home Modbus-RTU master device implements Modbus Serial Line Protocol and Implementation Guide V1.02: http://www.modbus.org/docs/Modbus_over_serial_line_V1_02.pdf

1.6. Compatible devices

Next table shows the devices which implement the protocol described in this document. The table contains the Product code and the product name.

Code	Product name	Product code	Input voltage	RS-485
MB-RTU-01/24	ModBus-RTU master	48	24V DC	✔
MB-RTU-01/230	ModBus-RTU master	49	230V DC	✔

2. Send and Receive Modbus-RTU message

PNUM	PCMD
0x38	0x01 to 0x1F

With the command user can send requests and receive responses from Modbus-RTU RS-485 network.

2.1. Request

Request				
NADR [2B]	**PNUM [1B]**	**PCMD [1B]**	**HWPID [2B]**	**PDATA [up to 56B]**
NADR	0x38	Modbus-RTU save address 0x01 to 0x1F	HWPID or 0xFFFF	Modbus protocol data unit (PDU) request

After receiving the IQRF DPA command the Master unit sends out the Modbus-RTU data unit created from the content of the PDATA field to RS-485 network.

- PCMD byte contains the Modbus-RTU slave device address. The device address can be 0x01 to 0x1F.
- PDATA contains the Modbus protocol data unit (PDU) request lika binary string.
- Modbus-RTU device calculates and checks the CRC-16 error check fields automatically.
- Modbus-RTU master device automatically re-sends the Modbus-RTU request, if the device doesn't receive any response or receives corrupted response from the slave device.

2.2. Response

Response						
NADR [2B]	**PNUM [1B]**	**PCMD [1B]**	**HWPID [2B]**	**ErrN [1B]**	**DpaValue [1B]**	**PDATA [up to 56B]**
NADR	0x38	Modbus-RTU save address + 0x80 0x81 to 0x9F	HWPID	0x00 or error codes: 0x20 0x21 0x22	?	Modbus protocol data unit (PDU) response

The addressed node response with received Modbus protocol data unit (PDU) response.

- PCMD byte contains the Modbus-RTU slave device address + 0x80.

- PDATA contains the Modbus protocol data unit (PDU) response lika binary string.
- Modbus-RTU device checks the received CRC-16 message integrity.

The Modbus-RTU master device can response with this error codes:

- 0x00 - Modbus response received successfully
- 0x20 - No Modbus response received (time-out)
- 0x21 - Received contains frame error (CRC or parity bit error)
- 0x22 - Received Modbus response is to long, can not send in DPA message

2.2.1. Modbus command example

Example: Reading value of two consecutive register starting from address 0x6000 from slave with slave address #1. Registers in Modbus are 16 bit wide.

Request:

Request				
NADR [2B]	**PNUM [1B]**	**PCMD [1B]**	**HWPID [2B]**	**PDATA [up to 56B]**
NADR	0x38	**0x01** save address	HWPID or 0xFFFF	"**0360000002**" Modbus protocol data unit (PDU) request

PDATA contains 5 bytes. Meaning of PDATA (PDU) bytes:

- 03 - Function code is: (0x03) Read Holding Registers
- 6000 - Starting Address is 0x6000
- 0002 - Quantity of Registers is 0x0002

> **NOTE:**
>
> Please note Modbus-RTU protocol has different endianness from IQRF DPA protocol.
> - Numbers in **IQRF DPA** are represented in **big-endian** data format.
> - Numbers in **Modbus-RTU** are represented in **little-endian** data format.
>
> In **PDATA (PDU message part)** the numbers are represented in **little-endian** data format.

More information about Holding registers, please see Chapter 6.3 "03 (0x03) Read Holding Registers" in MODBUS Protocol Specification:
www.modbus.org/docs/Modbus_Application_Protocol_V1_1b3.pdf

Response:

Response						
NADR [2B]	**PNUM [1B]**	**PCMD [1B]**	**HWPID [2B]**	**ErrN [1B]**	**DpaValue [1B]**	**PDATA [up to 56B]**
NADR	0x38	0x81 Modbus-RTU save address 0x81 = 0x01 + 0x80	HWPID	0x00	?	"**030412345678**" Modbus protocol data unit (PDU) response

Response PDATA contains 6 bytes. Meaning of PDATA (PDU) bytes:

- 03 - Function code is: (0x03) Read Holding Registers
- 04 - Byte count (number of following bytes)
- 1234 - Value of register located on address 0x6000 is 0x1234
- 5678 - Value of register located on address 0x6001 is 0x5678

NOTE:

Please note Modbus-RTU slave device can respond with error code. Error response is represented with modified response function code. The error response code equals with request response code plus 0x80. For example at 0x03 the error response PDU message starts with 0x83. The second byte contains the exception code.
Typical exceptions codes are:

- 0x01 - Function code is not supported
- 0x02 - Address error
- 0x03 - Quantity error
- 0x04 - Request processing error

More information about the response and the exception code at Holding registers, please see Chapter 6.3 "03 (0x03) Read Holding Registers" in MODBUS Protocol Specification: www.modbus.org/docs/Modbus_Application_Protocol_V1_1b3.pdf

3. Send Broadcast Modbus-RTU message

PNUM	PCMD
0x38	0x00

With the command user can send broadcast messages to Modbus-RTU RS-485 network.

3.1. Request

Request				
NADR [2B]	**PNUM [1B]**	**PCMD [1B]**	**HWPID [2B]**	**PDATA [up to 56B]**
NADR	0x38	Modbus-RTU Broadcast address 0x00	HWPID or 0xFFFF	Modbus protocol data unit (PDU) request

After receiving the IQRF DPA command the Master unit sends out the Modbus-RTU broadcast data unit created from the content of the PDATA field to RS-485 network.

- PCMD byte contains the Modbus-RTU broadcast address. The Modbus-RTU broadcast address is 0x00.
- PDATA contains the Modbus protocol data unit (PDU) request lika binary string.
- Modbus-RTU device calculates and checks the CRC-16 error check fields automatically.

> **NOTE:**
>
> Please note Modbus-RTU broadcast message types can be only write or modification commands. Broadcast messages do not have an acknowledgement process on the RS-485 side.

3.2. Response

Response						
NADR [2B]	**PNUM [1B]**	**PCMD [1B]**	**HWPID [2B]**	**ErrN [1B]**	**DpaValue [1B]**	**PDATA [0B]**
NADR	0x38	Modbus-RTU save address + 0x80 0x81 to 0x9F	HWPID	0x00	?	-

The addressed node acknowledges the request with a empty response (PDATA is empty, DPA Data length equal with zero).

3.3. Modbus broadcast command example

Example: Sets ON output (coil) address 0x0001 at all slave devices.

Request:

Request				
NADR [2B]	**PNUM [1B]**	**PCMD [1B]**	**HWPID [2B]**	**PDATA [up to 56B]**
NADR	0x38	**0x00** broadcast address	HWPID or 0xFFFF	"**050001FF00**" Modbus protocol data unit (PDU) request

PDATA contains 5 bytes. Meaning of PDATA (PDU) bytes:

- 05 - Function code is: (0x05) Write Single Coil
- 0001 - Output address is 0x0001
- FF00 - Set ON

Response:

Response						
NADR [2B]	**PNUM [1B]**	**PCMD [1B]**	**HWPID [2B]**	**ErrN [1B]**	**DpaValue [1B]**	**PDATA [0B]**
NADR	0x38	0x80	HWPID	0x00	?	-

Response contains empty PDATA.

4. Read and write configuration registers

PNUM	PCMD
0x38	0x3E

With the command user can set-up basic configuration registers. Configuration registers are stored in internal EEPROM. Values of configuration registers will remain after power down.

4.1. Configuration registers

With configuration registers can be set-up:

- RS-485 communication speed and byte data format
- Timeout value for no response received from RS-485 network
- Request send number at no response, or response containing integrity error

All tree registers are 1 byte wide register.

4.1.1. RS-485 communication speed and byte data format

Communication register is 1 byte wide. With a communication register can be set-up the RS-485 communication speed and byte data format. Next table shows the usable register value combinations.

RS-485 communication register		
Register value	**Communication speed [baud]**	**Parity**
0x00	1200	Even parity
0x01	2400	Even parity
0x02	4800	Even parity
0x03 (default)	**9600**	**Even parity**
0x04	19200	Even parity
0x05	38400	Even parity
0x06	57600*	Even parity
0x07	115200*	Even parity
0x08	1200	No parity - two stop bits
0x09	2400	No parity - two stop bits
0x0A	4800	No parity - two stop bits
0x0B	9600	No parity - two stop bits

0x0C	19200	No parity - two stop bits
0x0D	38400	No parity - two stop bits
0x0E	57600*	No parity - two stop bits
0x0F	115200*	No parity - two stop bits

** Test purpose only, it is not recommended to use in real application.*

Modbus-RTU master device communicate with two different mode base on communication register value:

- Register value is between 0x00 - 0x07:
  1 start bit
  8 data bits, least significant bit sent first
  1 bit for Even parity
  1 stop bit

- Register value is between 0x8 - 0x0F:
  1 start bit
  8 data bits, least significant bit sent first
  2 stop bits (no parity)

4.1.2. Timeout register

Timeout register is 1 byte wide register. With a timeout register can be set-up the timeout value for no response received from RS-485 network. Timeout can be calculated with this equation:

$$Timeout\ [ms]\ = Register\ Value\ \times 10\ [ms]$$

- Minimum register value is 1 (10 ms).
- Maximum register value is 255 (2.55 s).
- **Default register value is 50 (0.5 s)**

4.1.3. Request counter

Request counter register is 1 byte wide register. With a request send number register can be set-up the number of attempts to send out Modbus requests. If the device does not receive any response or response containing integrity error, then the device will resend the request. For example: If the register value is 3, then the device will send out the modbus request 3 times at communication error. After the third time the device responds with an error value to the IQRF request.

- Minimum register value is 1.
- Maximum register value is 15.
- **Default register value is 3.**

4.2. Read register values

4.2.1. Request

Request				
NADR [2B]	**PNUM [1B]**	**PCMD [1B]**	**HWPID [2B]**	**PDATA [0B]**
NADR	0x38	0x3E	HWPID or 0xFFFF	-

Request does not contain PDATA. DPA Data length has to be zero.

4.2.2. Response

Response								
NADR [2B]	**PNUM [1B]**	**PCMD [1B]**	**HWPID [2B]**	**ErrN [1B]**	**DpaValue [1B]**	**PDATA 1. byte**	**PDATA 2. byte**	**PDATA 3. byte**
NADR	0x38	0xBE	HWPID	0x00	?	RS-485 communication register	Timeout register	Request send number

4.3. Write register values

4.3.1. Request

Request						
NADR [2B]	**PNUM [1B]**	**PCMD [1B]**	**HWPID [2B]**	**PDATA [3B]**		
NADR	0x38	0x3E	HWPID or 0xFFFF	RS-485 communication register	Timeout register	Request send number

4.3.2. Response

Response of write register write request equals to response of read request described in chapter 4.2.2. Response.

5. Read product information

PNUM	PCMD
0x3E	0x00

The command is usable to get basic information about the product.

5.1. Request

The request does not contain any PDATA information.

Request			
NADR [2B]	**PNUM [1B]**	**PCMD [1B]**	**HWPID [2B]**
NADR	0x3E	0x00	HWPID or 0xFFFF

5.2. Response

The addressed node response with all basic product information.

Response						
NADR [2B]	**PNUM [1B]**	**PCMD [1B]**	**HWPID [2B]**	**ErrN [1B]**	**DpaValue [1B]**	**PDATA [16B]**
NADR	0x3E	0x80	0x15AF	0x00	?	Product information

5.2.1. PDATA structure of the response

Response PDATA array contains 20 byte long product information string.

PDATA					
1. byte - 15. byte	16. byte	17. byte	18. byte	19. byte	20. byte
Product String	Hardware and software revision				

- Product Code = Main product code of the product stored in ASCII characters.
- Hardware and software revision = Internal information about the hardware revision.

6. FRC - 1 Byte long product code

PNUM	PCMD	FRC command
0x0D	0x00 or 0x02	0xDE

This FRC command is used to collect product code information of IQ Home's products.
Maximum numbers of devices

- Maximum 63 device can send response to one data collection request.

6.1. Request

Next table shows the structure of request FRC command.

Request								
NADR [2B]	**PNUM [1B]**	**PCMD [1B]**	**HWPID [2B]**	**FRC Command**	**User data 1. byte**	**User data 2. byte**	**User data 3. byte**	**User data 4. byte**
0x0000 Coordi-nator	0x0D	0x00	0xFFFF	0xDE	Don't care	Don't care	Don't care	Don't care

- At FRC Commands the addressable node have to be coordinator (0x00).
- 1st byte of PDATA = FRC Command.
  0xDE: 1 Byte product code collection

6.2. Response

Response							
NADR [2B]	**PNUM [1B]**	**PCMD [1B]**	**HWPID [2B]**	**ErrN [1B]**	**DpaValue [1B]**	**PDATA 1. byte**	**PDATA 2… n. byte**
0x0000 Coordi-nato	0x0D	0x80	?	0x00	?	Status	FRC Data

- Status:
  Return code of the sendFRC IQRF OS function. See IQRF OS documentation for more information.
- FRC data:
  Data collected from the nodes. Because the current version of DPA cannot transfer the whole FRC output buffer at once (currently only up to 55 bytes), the remaining bytes of the buffer can be read by the next described Extra result command. (More information: IQRF DPA Framework - Technical Guide.)

6.2.1. Response - Product codes

Product	Value
MB-RTU-01/24	48
MB-RTU-01/230	49
MB-RTU-02/24*	50
MB-RTU-02/230*	51

** These products are not released, these product code has been reserved for future use.*

7. FRC - 2 Bit long RF mode

PNUM	PCMD	FRC command
0x0D	0x00 or 0x02	0x7E

This FRC command is used to collect current RF mode information of IQ Home's products.
Maximum numbers of devices

- Maximum 239 devices can send responses to one data collection request.

7.1. Request

Next table shows the structure of the request FRC command.

Request								
NADR [2B]	**PNUM [1B]**	**PCMD [1B]**	**HWPID [2B]**	**FRC Command**	**User data 1. byte**	**User data 2. byte**	**User data 3. byte**	**User data 4. byte**
0x0000 Coordi-nator	0x0D	0x00	0xFFFF	0x7E	Don't care	Don't care	Don't care	Don't care

- At FRC Commands the addressable node has to be coordinator (0x00).
- 1st byte of PDATA = FRC Command.
  0x7E: 2 bit RF Mode collection

7.2. Response

Response							
NADR [2B]	**PNUM [1B]**	**PCMD [1B]**	**HWPID [2B]**	**ErrN [1B]**	**DpaValue [1B]**	**PDATA 1. byte**	**PDATA 2… n. byte**
0x0000 Coordi-nato	0x0D	0x80	?	0x00	?	Status	FRC Data

- Status:
  Return code of the sendFRC IQRF OS function. See IQRF OS documentation for more information.
- FRC data:
  Data collected from the nodes. Because the current version of DPA cannot transfer the whole FRC output buffer at once (currently only up to 55 bytes), the remaining bytes of the buffer can be read by the next described Extra result command. (More information: IQRF DPA Framework - Technical Guide.)

7.2.1. Response - RF Mode

RF communication mode	Value
Fast communication mode* - IQRF RF Mode: STD - Routing on	1
Extreme Low Power communication mode* - IQRF RF Mode: LP - Routing off	2
Low Power communication mode - IQRF RF Mode: LP - Routing on *Default RF Mode*	3

** These RF Modes are not used at the moment, these values have been reserved for future use.*

9. Release Notes

Property	Value
IQRF OS version	4.03D
IQRF DPA version	4.11
Date of release	27/04/2020
Notes	• HWPID and HWPIDver has been modified • Response length of Read product information command (PNUM=0x3E) has been extended to 20 byte. • FRC - 1 Byte long product code (0xDE) has been added. • FRC - 2 Bit long RF mode (0x7E) has been added. **Caution: Devices with protocol version OS version 4.03D and 4.02D are not RF compatible.**

Property	Value
Protocol version	1.0.xx
IQRF OS version	4.02D
IQRF DPA version	3.02
Date of release	18/07/2018
Notes	First revision of IQ Home Modbus-RTU Master protocol.