Qi: Communications Protocol Specifications

qi-v13-standards/Qi-v1.3-comms-protocol.pdf

Extended vs Baseline Protocol

General Overview

- When a user places a Power Receiver within the Operating Volume of a Power Transmitter, the two start to communicate with the aim to configure and control the power transfer.
  - The Power Signal provides the carrier for all communications.

Figure 2. Protocol phases

- Ping Phase
  - The Power Transmitter tries to establish communications with a Power Receiver. Before
    doing so, it typically performs measurements to determine if there are objects such as bankcards, coins or other metals, which can damage or heat up during the power transfer.
  - These measurements proceed
    without waking up the Power Receiver
- Configuration Phase

  - Power Receiver sends basic identification and configuration data to the Power Transmitter. Both sides use this information to create a baseline Power Transfer Contract.
  - Power Transmitter and Power Receiver decide whether to continue with the Baseline Protocol or the Extended Protocol.
- <u>Negotiation Phase</u>
  - This phase is not present in the Baseline Protocol. The Power Transmitter and Power
    Receiver establish an extended Power Transfer Contract containing additional settings and limits. The
  - Power Receiver provides design information to the Power Transmitter, which the latter can use to complete FOD before switching to the power transfer phase.
- <u>Power Transfer Phase</u>
  - This is the phase in which the power transfer to the Power Receiver's Load occurs.
    In the Extended Protocol, the Power Transmitter and Power Receiver perform a system calibration at the start of this phase.
  - Occasional interruptions of this phase may occur to renegotiate an element of the Power Transfer Contract. The power transfer continues during such renegotiations.

- After the ping phase the power receiver initiates all further data packet communications
- 4 Kinds of packets the power receiver can send
  - <u>Status update</u>: the Power Transmitter does not reply to these data packets.
  - <u>Power control</u>: the Power Transmitter adjusts the power level in response to these data packets.
  - <u>Simple query</u>: invites the Power Transmitter to reply with a Response Pattern (ACK, NAK, ND, ATN).

- Data request: invites the Power Transmitter to reply with a full data packet.

The Power Transmitter should not respond to data packets that suffer from communications errors. The reason is that data packet corruption could result in the Power Transmitter providing the wrong type of response, confusing the Power Receiver.

The purpose of most communications in the protocol is to configure and control the power transfer. However, the Extended Protocol also supports data transport streams, which can pass high-level messages (often unrelated to the power transfer) between the Power Transmitter and Power Receiver. Examples of such messages include the authentication messages that the Power Transmitter and Power Receiver can use to verify each other's credentials in a tamper-resistant manner

The power receiver can initiate a data transport stream at anytime during the power transfer phase

Conversely, when a Power Transmitter has a high-level message to send to the Power Receiver—and has ensured that the latter can process that message—it can draw the Power Receiver's attention by responding with an ATN Response Pattern to an incoming simple-query data packet in the power transfer phase. This signals the Power Receiver to transmit a series of data-request data packets enabling the Power Transmitter to send a data transport stream

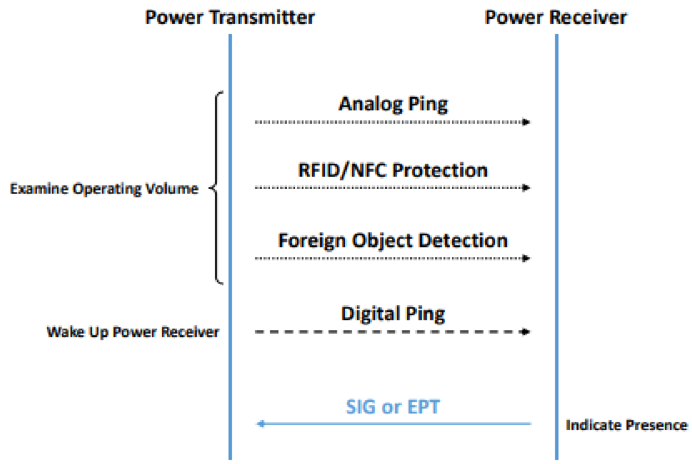
this could be useful for attacking - you would need to respond with an ATN response pattern in order to get the victim device to accept data from the "power transmitter"

Ping Phase

- At the beginning of this phase, neither the power transmitter or the power receiver are aware of each other
    - the power transmitter does not know if their is a receiver within its operating volume
    - the power receiver is not receiving a power signal so its systems are typically inactive

- The power transmitter is not trying to "wake up" the power receiver during this phase

Figure 4. Stages of the ping phase



- Begins with Foreign Object Detection (FOD)
- After FOD and determining that there potentially is a Power Receiver in its operating Volume, the Power Transmitter initiates a Digital Ping to solicit a response from the Power Receiver, which is either a Signal Strength (SIG) data packet or an End Power Transfer (EPT) data packet. If there is no such response, the Power Transmitter stays in the ping phase and should repeat the above steps.

Table 11. Timing constraints in the ping phase

Parameter	Side	Symbol	Minimum	Target	Maximum	Unit
Detection time window	PTx	t_{detect}	N/A	N/A	5,000	ms
Wake-up window	PRx	t_{wake}	19	40	64	ms
Digital Ping timeout	PTx	t_{ping}	65	65	70	ms
Power termination window	PTx	$t_{terminate}$	N/A	N/A	28	ms
Reset window	PRx	t_{reset}	N/A	25	28	ms
No Power Signal window	PTx	$t_{nopower}$	32	N/A	N/A	ms
Next Digital Ping window	PTx	$t_{nextping}$	See Table 25 in section 8.7, *End Power Transfer—EPT (0x02; power control)*			

Configuration Phase

During the Configuration Phase:

- The Power Receiver identifies itself to the Power Transmitter.
- The Power Receiver and Power Transmitter establish a baseline Power Transfer Contract.
- The Power Receiver and Power Transmitter determine the protocol variant to use in the power transfer.
- Data packets are sent during this phase
- consecutive data packets are able to be sent
- can trigger an illegal value timeout if the data packet is detected to contain an illegal value

Figure 12. Data flow in the configuration phase

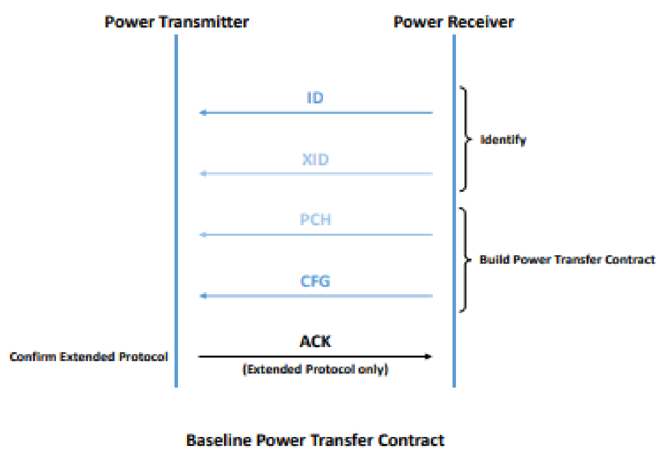


Figure 13. State diagram of the configuration phase

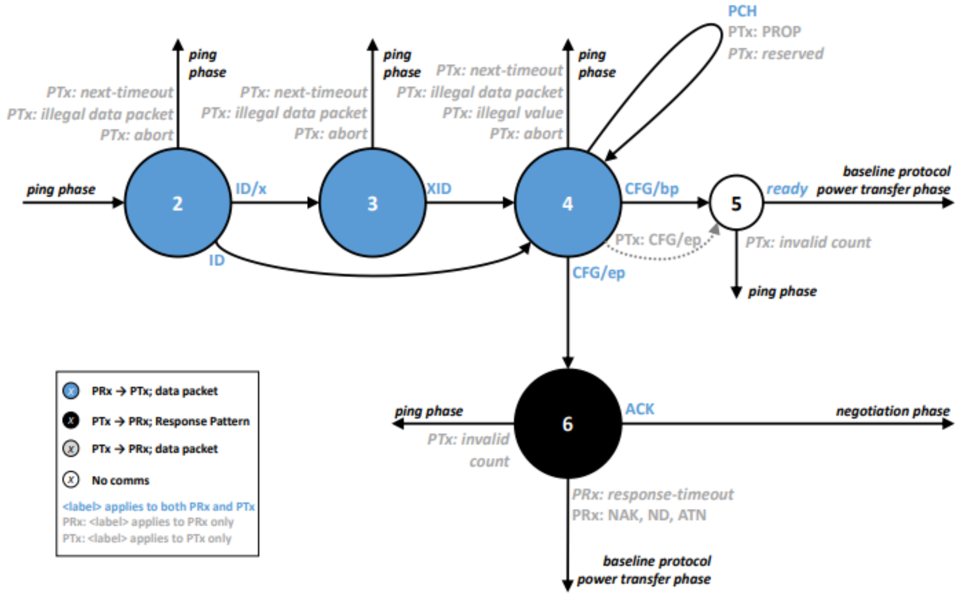
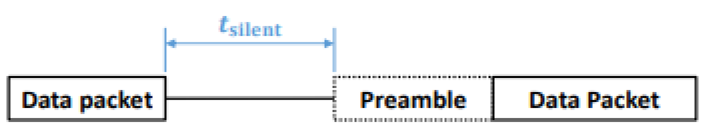


Figure 16. Generic timing constraints



Negotiation Phase

*Only exists within the extended protocol

- phase where the power transmitter and power receiver can make changes to the power transfer contract

Negotiation phase

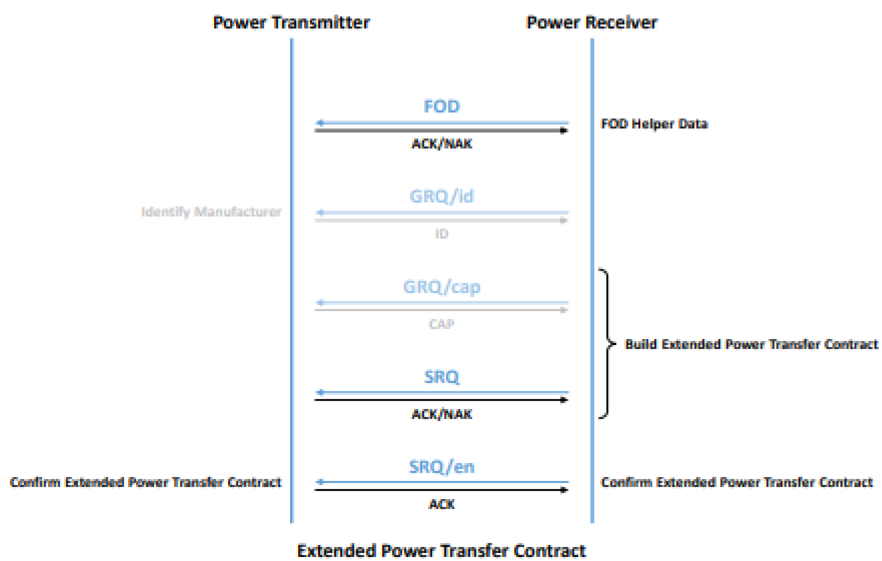
- directly follows the configuration phase and creates the initial extended power transfer
- unrestricted length for this phase

Renegotiation phase

- may interrupt the power transfer phase multiple times and typically serves to adjust a single element of the power transfer contract

- changes are negotiated by the power receiver using a question and answer approach
- power receiver will send a simple-query data packet and the power transmitter replies with a response pattern
- if negotiation is unsuccessful it will revert to the power transfer phase and use the baseline protocol if the negotiation phase is aborted

Figure 22. Data flow in the negotiation phase



Negotiable elements of the power transfer contract

- Reference Power
    - at most 5W
- FSK Polarity and modulation depth
- Received Power reporting data packet
    - extended protocol uses a 16 bit received power resolution (default is 8 bit)

- Guaranteed (load) Power
- Re-ping delay

Both the Power Receiver and the Power Transmitter shall keep track of the elements of the Power Transfer
Contract that have changed.

- Wireless Power ID transfer (proprietary?)

Power Transfer Phase

- The power transfer phase is the part of the protocol in which actual power transfers to the Power Receiver’s Load.
    - The power transfer proceeds subject to the conditions in the Power Transfer Contract created in the negotiation phase.
    - The Power Receiver controls the power level by sending control error data, which is a
      measure for the deviation between the Power Receiver’s target and actual operating points. The Power Transmitter and Power Receiver aim to drive the control error data to zero, at which point the system is operating at its target power level.
- In addition to control error data, the Power Transmitter and Power Receiver exchange information intended to facilitate FOD.
    - The Power Receiver regularly reports the amount of power it receives—the Received Power level—and the Power Transmitter can signal whether it has detected a Foreign Object.
    - The recommended method for FOD in the power transfer phase is power-loss accounting. In this approach, the Power Transmitter compares the Received Power level as reported by the Power Receiver with the amount of power it transmits—the Transmitted Power level—and signals the Power Receiver when the difference exceeds a threshold

- If circumstances so require, the Power Transmitter or the Power Receiver may request renegotiation of the
  Power Transfer Contract. Examples of such changed circumstances include:
  ▪ The Power Receiver requires (substantially) more power than previously negotiated.
  ▪ The Power Transmitter has detected that it is operating at a low efficiency.
  ▪ The Power Transmitter is no longer able to sustain the current power level because of an increased operating temperature (or vice versa, it allows the Power Receiver to operate at a higher power level after cooling down sufficiently).

- The Power Transmitter and Power Receiver can exchange application-level data throughout the power transfer phase by initiating data transport streams. An important common application is authentication, where both sides can verify their counterpart's credentials in a tamper resistant manner.

  - For example, a Power Receiver may want to verify the credentials of a Power Transmitter to ensure that it can trust the latter to operate safely at elevated power levels—having the proper credentials implies having passed compliance testing.

  - Accordingly, a recommended approach to the power transfer is to start at a low power level (e.g. at a Load Power of $P_L \leq 5$ W), and control the power to a higher level only after successfully completing the authentication protocol.

Figure 41. Data flow in the negotiation phase (Baseline Protocol)

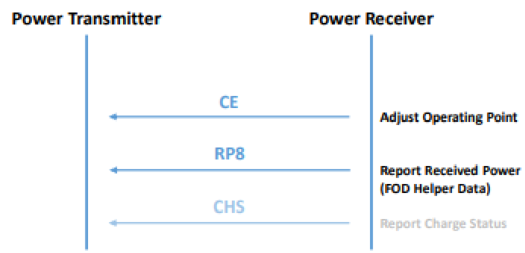
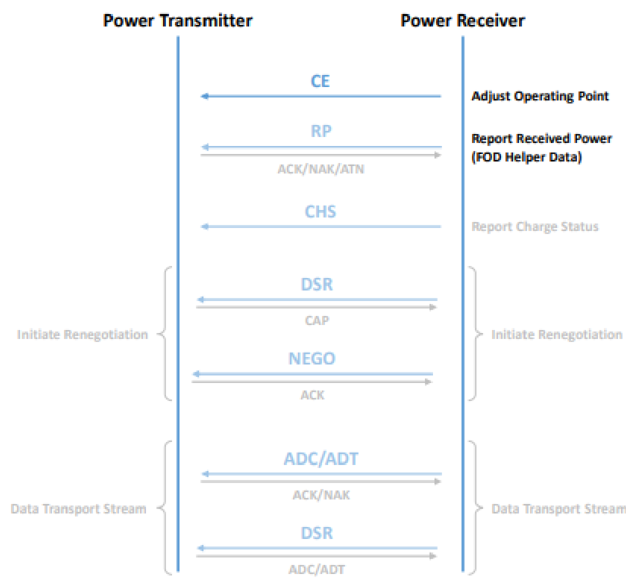


Figure 42. Data flow in the negotiation phase (Extended Protocol)



- The Power Receiver typically sends Control Error (CE) data packets several times per second. It sends Received Power data packets (RP8 in the Baselines Protocol and RP in the Extended Protocol) typically once every 1.5 second.
- In the Extended Protocol, the Power Receiver may reply to an RP data packet with an Attention (ATN) Response Pattern to request permission to send a data packet. The Power Transmitter and Power Receiver may use Data Stream Response (DSR), Power Transmitter Capability (CAP), and Renegotiate (NEGO) data packets to initiate renegotiation of an element in the Power Transfer Contract (typically the Guaranteed Load Power). Finally, they may use Auxiliary Data Control (ADC),

Auxiliary Data Transport (ADT), and DSR data packets to exchange application-level data.

Data Transport Stream

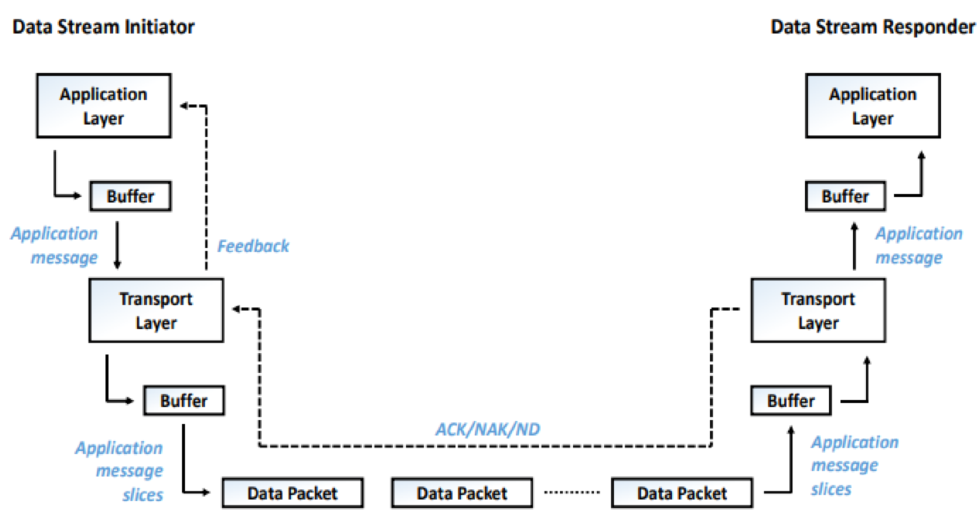
- Data transport streams serve to pass application-level data from a Data Stream Initiator to a Data Stream Responder Version 1.3 of the Qi Specification supports two applications, namely
  - Authentication, as defined in the Qi Specification, Authentication Protocol.
  - Proprietary (general-purpose) applications
- An initial ADC data packet opening the stream.
  - The type of the message contained in the stream.
  - The number of data bytes in the stream.
  - A sequence of ADT data packets containing the actual message.
  - A final ADC/end data packet closing the stream.

NOTE Other data packets, such as CE data packets, may intermix with those of a data transport stream. These data packets are not part of the transport data stream.

NOTE Max number of data bytes in a data transport stream = 2047

- Power transmitter/receiver can have at most 1 incoming and 1 outgoing data transport stream at a time

Figure 48. Data model



- The authentication protocol starts with the Power Receiver opening a data transport stream to send a GET_CERTIFICATE message to the Power Transmitter. After closing this stream, at position (a) the Power Receiver sends a DSR/poll data packet, inviting the Power Transmitter to send its certificate chain. If the Power Transmitter is not ready to send its certificate data at this time, it may respond with a NULL data packet. In this case, the Power Receiver should repeat its DSR/poll data packet later. Alternatively, the Power Receiver may wait until the Power Transmitter sends an ATN Response Pattern, which serves as a trigger for the Power Receiver to send a DSR/poll data packet.

2.4 Packet structure

The Power Receiver shall communicate to the Power Transmitter using data packets. As shown in Figure 4, a packet consists of four parts, namely a preamble, a header, a message, and a checksum. The preamble consists of a minimum of 11 and a maximum of 25 bits, all set to ONE, and encoded as defined in Bit encoding scheme. The preamble enables the Power Transmitter to synchronize with the incoming data and accurately detect the start bit of the header.

The header, message, and checksum consist of a sequence of three or more bytes encoded as defined in Header, Message, and Checksum.

Preamble	Header	Message	Checksum

Figure 4. Packet structure

Table 5: Message size

Header	Message Size*	Comment
0x00…0x1F	1 + (Header – 0) / 32	1 ×32 messages (size 1)
0x20…0x7F	2 + (Header – 32) / 16	6 × 16 messages (size 2…7)
0x80…0xDF	8 + (Header – 128) / 8	12 × 8 messages (size 8…19)
0xE0…0xFF	20 + (Header – 224) / 4	8 × 4 messages (size 20…27)

*Values in this column are truncated to an integer.

2.3 Data packet types

Whereas the Power Transmitter starts the communications protocol by applying a Digital Ping (at the end of the ping phase), the Power Receiver drives the execution of the remaining phases of the protocol. This means that the Power Receiver initiates all data packet communications, and that the Power Transmitter waits to send a data packet or Response Pattern until explicitly invited to do so.

NOTE Although it is the Power Receiver that drives the communications protocol, the Power Transmitter may adjust the power level or stop the power transfer completely at any time if it considers that necessary to ensure safe system operation. For additional information, see the *Qi Specification, Power Delivery*.

The Power Receiver can send four kinds of data packets:

- *Status update*—the Power Transmitter does not reply to these data packets.
- *Power control*—the Power Transmitter adjusts the power level in response to these data packets.
- *Simple query*—invites the Power Transmitter to reply with a Response Pattern (ACK, NAK, ND, ATN).
- *Data request*—invites the Power Transmitter to reply with a full data packet.

NOTE The Baseline Protocol uses status update and power-control data packets only.

The Power Transmitter should not respond to data packets that suffer from communications errors. The reason is that data packet corruption could result in the Power Transmitter providing the wrong type of response, confusing the Power Receiver. The lack of a response is a clear signal to the Power Receiver that something went wrong and that it should resend the data packet.

2.4.3 Checksum

The checksum consists of a single byte that enables the Power Transmitter to check for transmission errors. The Power Transmitter shall calculate the checksum as follows:

$$C := H \oplus B_0 \oplus B_1 \oplus \ldots \oplus B_{\text{last}}$$

where C represents the calculated checksum, H represents the header byte, and B_0, B_1,..., B_{last} represent the message bytes.

If the calculated checksum C and the checksum byte contained in the data packet are not equal, the Power Transmitter shall determine that the checksum is inconsistent.

Power Receiver Data Packets

Header* Mnemonic Name Type Size
0x01 SIG Signal Strength Status update 1
0x02 EPT End Power Transfer Power control 1
0x03 CE Control Error Power control 1
0x04 RP8 Received Power (8 bit) Status update 1
0x05 CHS Charge Status Status update 1
0x06 PCH Power Control Hold-off Status update 1
0x07 GRQ General Request Data request 1
0x09 NEGO Renegotiate Simple query 1
0x15 DSR Data Stream Response Data request 1
0x16 ADT/1e Auxiliary Data Transport (even) Simple query 1
0x17 ADT/1o Auxiliary Data Transport (odd) Simple query 1
0x18 PROP/1e Proprietary Multiple 1
0x19 PROP/1o Proprietary Multiple 1
0x20 SRQ Specific Request Simple query 2
0x22 FOD FOD Status Simple query 2
0x25 ADC Auxiliary Data Control Simple query 2
0x26 ADT/2e Auxiliary Data Transport (even) Simple query 2
0x27 ADT/2o Auxiliary Data Transport (odd) Simple query 2
0x28 PROP/2e Proprietary Multiple 2
0x29 PROP/2o Proprietary Multiple 2
0x31 RP Received Power (16 bit) Simple query 3
0x36 ADT/3e Auxiliary Data Transport (even) Simple query 3
0x37 ADT/3o Auxiliary Data Transport (odd) Simple query 3
0x38 PROP/3 Proprietary Multiple 3
0x46 ADT/4e Auxiliary Data Transport (even) Simple query 4
0x47 ADT/4o Auxiliary Data Transport (odd) Simple query 4
0x48 PROP/4 Proprietary Multiple 4
0x51 CFG Configuration Simple query 5
0x54 WPID Wireless Power ID (most significant bits) Multiple 5
0x55 WPID Wireless Power ID (least significant bits) Simple query 5
0x56 ADT/5e Auxiliary Data Transport (even) Simple query 5
0x57 ADT/5o Auxiliary Data Transport (odd) Simple query 5

0x58 PROP/5 Proprietary Multiple 5

0x66 ADT/6e Auxiliary Data Transport (even) Simple query 6

0x67 ADT/6o Auxiliary Data Transport (odd) Simple query 6

0x68 PROP/6 Proprietary Multiple 6

0x71 ID Identification Status update 7

0x76 ADT/7e Auxiliary Data Transport (even) Simple query 7

0x77 ADT/7o Auxiliary Data Transport (odd) Simple query 7

0x78 PROP/7 Proprietary Multiple 7

0x81 XID Extended Identification Status update 8

0x84 PROP/8 Proprietary Multiple 8

0xA4 PROP/12 Proprietary Multiple 12

0xC4 PROP/16 Proprietary Multiple 16

0xE2 PROP/20 Proprietary Multiple 20