Introduction

This application note describes the FDCAN protocol used in the STM32 microcontroller bootloader, providing details on each supported command.

This document applies to STM32 products embedding any bootloader version, as specified in application note *STM32 system memory boot mode (AN2606)*, available from [www.st.com](http://www.st.com). These products are listed in Table 1.

For more information about the FDCAN hardware resources and requirements for their device bootloader, users are advised to refer to application note AN2606.

<table>
<thead>
<tr>
<th>Table 1. Applicable products</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
</tr>
<tr>
<td>Microcontrollers</td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>
1 Bootloader code sequence

The 32-bit microcontrollers in the STM32H7 Series and STM32L5 Series are based on the Arm® Cortex® processor. They are referred to as STM32 in this document. Figure 1 presents the global sequence for the STM32 bootloader with FDCAN.

Figure 1. Bootloader for STM32 with FDCAN

Once the system memory boot mode is entered and the STM32 device is configured, (refer to application note AN2606 for additional details), the bootloader code waits for a frame on the FDCANx_Rx pin.

Note: Arm is a registered trademark of Arm Limited (or its subsidiaries) in the US and/or elsewhere.
In this application, the FDCAN settings are:

- Frame format: FD mode with Bit Rate Switching
- Mode: Normal mode
- AutoRetransmission: Enabled
- TransmitPause: Disabled
- Standard identifier (not extended)
- Time quantum = NominalPrescaler × (1 / fdcan_ker_ck)
  - fdcan_ker_ck = 20 MHZ
  - Nominal Pre-scaler = 0x1
- Synchronisation Jump Width = 0x10
- Nominal Time Segment1 = 0x3F
- Nominal Time Segment2 = 0x10
- Data Prescaler = 0x1
- Data Sync Jump Width = 0x4
- Data Time Segment1 = 0xF
- Data Time Segment2 = 0x4
- Standard Filters Number = 1
- Extended Filters Number = 0

Filter settings are:

- ID Type = 0
- Filter Index = 0
- Filter Type = 2 (classic filter)
- Filter Config = FDCAN_FILTER_TO_RXFIFO0
- Filter ID1 = 0x111
- Filter ID2 = 0x7FF

Transmit settings (from the STM32 to the host) are:

- Identifier = 0x111
- Id Type = 0
- Frame Type = FDCAN_DATA_FRAME
- Data Length = FDCAN_DLC_BYTES_64
- ErrorStateIndicator = FDCAN_ESI_ACTIVE
- BitRateSwitch = FDCAN_BRS_ON
- FDFormat = FDCAN_FD_CAN
- TxEventFifoControl = FDCAN_NO_TX_EVENTS
- MessageMarker = 0

Note: 1. The CAN bootloader firmware supports only one node at a time. This means that it does not support CAN Network Management.
2. For acceptance, MessageID and FilterID1 must match exactly.
3 Bootloader command set

Table 2 lists the supported commands, each of them being described in the corresponding sub-section.

<table>
<thead>
<tr>
<th>Command</th>
<th>Command code</th>
<th>Sub-section</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Get(1)</td>
<td>0x00</td>
<td>Section 3.1</td>
<td>Gets the version and allowed commands supported by the current version of the bootloader.</td>
</tr>
<tr>
<td>Get Version(1)</td>
<td>0x01</td>
<td>Section 3.2</td>
<td>Gets the bootloader version and the read protection status of the Flash memory.</td>
</tr>
<tr>
<td>Get ID(1)</td>
<td>0x02</td>
<td>Section 3.3</td>
<td>Gets the chip ID.</td>
</tr>
<tr>
<td>Read Memory(2)</td>
<td>0x11</td>
<td>Section 3.4</td>
<td>Reads up to 256 bytes of memory starting from an address specified by the application.</td>
</tr>
<tr>
<td>Go(2)</td>
<td>0x21</td>
<td>Section 3.5</td>
<td>Jumps to user application code located in the internal Flash memory or SRAM.</td>
</tr>
<tr>
<td>Write Memory(2)</td>
<td>0x31</td>
<td>Section 3.6</td>
<td>Writes up to 256 bytes of RAM or Flash memory starting from an address specified by the application.</td>
</tr>
<tr>
<td>Erase Memory(2)</td>
<td>0x44</td>
<td>Section 3.7</td>
<td>Erases from one to all the Flash memory sectors.</td>
</tr>
<tr>
<td>Write Protect</td>
<td>0x63</td>
<td>Section 3.8</td>
<td>Enables the write protection of some sectors.</td>
</tr>
<tr>
<td>Write Unprotect</td>
<td>0x73</td>
<td>Section 3.9</td>
<td>Disables the write protection of all Flash memory sectors.</td>
</tr>
<tr>
<td>Readout Protect(1)</td>
<td>0x82</td>
<td>Section 3.10</td>
<td>Enables read protection.</td>
</tr>
<tr>
<td>Readout Unprotect(1)</td>
<td>0x92</td>
<td>Section 3.11</td>
<td>Disables read protection.</td>
</tr>
</tbody>
</table>

1. Read protection: When the RDP (read protection) option is active, only this limited subset of commands is available. All other commands are NACK-ed and have no effect on the device. Once the RDP is removed, the other commands become active.

2. Refer to STM32 product datasheet and application note AN2606 to know about the valid memory spaces for this command.

Communication safety

Each packet is either accepted (ACK answer) or discarded (NACK answer):
- ACK message = 0x79
- NACK message = 0x1F
3.1 Get command

The Get command allows the host to get the version of the bootloader and the supported commands. When the bootloader receives the Get command, it transmits the bootloader version and the supported command codes to the host.

Figure 2. Get command (host side)

Start Get command

Send message with ID = 00h and DataLength = 0000h

Wait for ACK or NACK

Receive 1 message: number of bytes

Receive 1 message: bootloader version

Receive 12 messages (message by message): command opcodes

Wait for ACK

End of Get command
Based on the host command, the device answers as shown in Figure 3.

**Figure 3. Get command (device side)**

- Start Get command
- Received message with ID = 00h?
  - Yes: Send ACK message
  - No: Send NACK message
- Send 1 message: number of bytes
- Send 1 message: bootloader version
- Send 12 messages (message by message): command opcodes
- Send ACK message
- End of Get command

All data sent from the device on this command are sent using DataLength = 0000h (one byte).
The data are received as per the following order:
1. Number of commands (11)
2. FDCAN bootloader version (0x10)
3. Get command opcode (0x00)
4. Get Version command opcode (0x01)
5. Get ID command opcode (0x02)
6. Read Memory command opcode (0x11)
7. Go command opcode (0x21)
8. Write Memory command opcode (0x31)
9. Erase Memory command opcode (0x44)
10. Write Protect command opcode (0x63)
11. Write Unprotect command opcode (0x73)
12. Readout Protect command opcode (0x82)
13. Readout Unprotect command opcode (0x93)
3.2 Get Version command

The Get Version command is used to get the bootloader version. When the bootloader receives the command, it transmits the information to the host as described in Figure 4 (version and two dummy bytes having the value 0x00).

Figure 4. Get Version command (host side)

Start Get Version command

Send message with ID = 01h

Wait for ACK or NACK

ACK

Receive 1 message: bootloader version

NACK

Receive 1 message: 2 dummy bytes = 00h

Wait for ACK or NACK

End of Get Version command
The host receives first the bootloader version (one byte), and then two dummy bytes equal each to 00h.

Figure 5. Get Version command (device side)
3.3 Get ID command

The Get ID command is used to get the version of the STM32 product ID (identification). When the bootloader receives the command, it transmits the product ID to the host.

Figure 6. Get ID command (host side)

- Start Get ID command
- Send message with ID = 02h
- Wait for ACK or NACK
  - ACK
    - Receive one 2-byte message: STM32 product ID
  - NACK
- Wait for ACK or NACK
  - ACK
    - End of Get ID command
  - NACK
The host receives the STM32 product ID (two bytes) sent by the device as shown in Figure 7. The LSB (byte) is sent first.

**Figure 7. Get ID command (device side)**

1. **Start Get ID command**
2. **Received message with ID = 02h?**
   - **No**: Send NACK message
   - **Yes**: Send ACK message
3. **Send 1 message: STM32 product ID (2 bytes - MSB first)**
4. **Send ACK message**
5. **End of Get ID command**
3.4 Read Memory command

The Read Memory command is used to read data from any valid memory address: RAM, Flash memory, and information block (System memory or Option Byte areas).

Running the Read Memory command is only possible when the read protection is not set and the address to read from is valid. For this reason, the bootloader software performs the following checks in sequence:
1. Is the ID of the command correct or not?
2. Is the read protection disabled or not?
3. Is the address to read from valid or not?
If all checks pass, the Read Memory command proceeds with reading the data, otherwise NACK is sent to the host.

Note: The bootloader sends the data as 64-byte messages. The host takes only the number of data needed.

Figure 8. Read Memory command (host side)
Together with the message ID for the Read Memory command (11h), the address and number of bytes are sent to the device. The message content is as follows:

1. ID = 0x11, DLC = 0x05
2. data[0] = 0xXX (MSB of the address)
3. data[1] = 0xYY
4. data[2] = 0xZZ
5. data[3] = 0xTT (LSB of the address)
6. data[4] = N (number of bytes to be read minus one; 0 < N ≤ 255)

The data are always sent to the host by multiples of 64 bytes. The host must filter the needed data based on the number of data requested.
3.5 Go command

The Go command is used to execute downloaded code or any other code by branching to an address specified by the application. When the bootloader receives the Go command, it starts only if the message contains valid information and passes the following checks:

- Is the ID of the command correct?
- Is the read protection disabled?
- Is the address to jump to valid?

If the message content is correct, the Go command transmits an ACK message; Otherwise, it transmits a NACK message.

After sending an ACK message to the application, the bootloader firmware:

- Resets the registers of the peripherals used by the bootloader to their default values
- Initializes the main stack pointer of the user application
- Jumps to the memory location programmed in the received “address + 4”, which is the address of the application reset handler.

For example, if the received address is 0x0800 0000, the bootloader jumps to the memory location programmed at address 0x0800 0004. The host must send the base address where the application to jump to is programmed.

Note:

1. The jump to the application works only if the user application sets the vector table correctly to point to the application address.
2. The valid addresses for the Go command are in RAM or Flash memory. All other addresses are considered not valid and are NACK-ed by the device.
3. Not all addresses in the RAM are considered valid. The application to jump to must consider an offset to avoid overlapping with the first RAM memory used by the bootloader firmware.

Figure 10. Go command (host side)
The message content sent to the device, including the Go command ID (21h), is as follows:
1. ID = 0x21, DLC = 0x04
2. data[0] = 0xXX (MSB of the address)
3. data[1] = 0xYY
4. data[2] = 0xZZ
5. data[3] = 0xTT (LSB of the address)

Figure 11. Go command (device side)

3.6 Write Memory command

The Write Memory command is used to write data to any valid memory address of the RAM, Flash memory, or Option Byte area. When the bootloader receives the Write Memory command, it starts only if the message contains valid information and passes the following checks:
- Is the ID of the command correct?
- Is the read protection disabled?
- Is the address to write to valid?

If the message content is correct, the Go command transmits an ACK message and continues the job; Otherwise, it transmits a NACK message and exits the command.

For the Option Byte area, the start address must be the base address of the Option Byte area to avoid writing inopportune in this area.

When the address is valid, the bootloader:
- Receives the user data (N bytes). This means that the device receives N/64 messages, each message being composed of 64 data bytes.
- Programs the user data into the memory starting from the received address
- Transmits the ACK message at the end of the command if the write operation was successful; Otherwise it transmits a NACK message to the application and aborts the command.
Note:

1. The maximum length of the block to be written for the STM32 is 256 bytes.
2. No error is returned when performing write operations on write protected sectors.

**Figure 12. Write Memory command (host side)**

- **Start Write Memory command**
- Send message ID = 31h and 4-byte address (MSB first)
- Wait for ACK or NACK
  - ACK
  - NACK
  - Send data messages (packets of 64 bytes)
  - Wait for ACK or NACK
    - ACK
    - NACK
  - End of Write Memory command
Together with the message ID for the Write Memory command (31h), the address and number of bytes are sent to the device. The message content is as follows:

1. ID = 0x31, DLC = 0x05
2. data[0] = 0xXX (MSB of the address)
3. data[1] = 0xYY
4. data[2] = 0xZZ
5. data[3] = 0xTT (LSB of the address)
6. data[4] = N (number of bytes to be written minus one; 0 < N ≤ 255)

The host sends N / 64 messages.

3.7 Erase Memory command

The Erase Memory command allows the host to erase Flash memory pages. When the bootloader receives the Erase Memory command and RDP is disabled, it transmits the ACK message to the host.
After the transmission of the ACK message, the bootloader checks the first two bytes of data received in an MSB format and constructs a value called \textit{PageNumber}, which controls the execution of the Erase Memory command as follows:

- \textit{PageNumber} = 0xFFFF: mass erase is requested
- \textit{PageNumber} = 0xFFFE: Bank1 erase is requested (if supported)
- \textit{PageNumber} = 0xFFFD: Bank2 erase is requested (if supported)
- Otherwise, \textit{PageNumber} represents the number of pages to erase

If the \textit{PageNumber} value indicates mass or bank erase, an ACK message is sent upon completion. Otherwise, the bootloader starts erasing the memory pages as defined by the host, and then sends an ACK message when all the requested pages are erased.

\textbf{Erase Memory command specifications:}

1. The bootloader receives one message that contains \textit{N}, the number of pages to be erased.
2. The bootloader receives \textit{N} bytes, each byte containing the page number to be erased.

\textbf{Note:}

1. \textit{The ACK message sent after the erase operation only indicates that the command is finished. It does not guarantee that the erase operation has succeeded.}
2. \textit{No error is returned when performing erase operations on write-protected sectors.}
The `PageNumber` value sent from the host is MSB first:

- `PageNumber = (data[0] << 8) | (data[1])`
- Page numbers sent for the erase are sent on a 64-byte frame format, of which only `PageNumber` is read by the bootloader (the padding bytes in the 64-byte frame are not read)
Start Erase Memory command

Received message with ID = 44h?

RDP active?

Send ACK message

Receive 2-byte messages and construct PageNumber (MSB first)

PageNumber = 0xFFFF or PageNumber = 0xFFFE or PageNumber = 0xFFFD

Mass/Bank erase

Send ACK message

Receive page numbers to erase

Page(s) erase

Send ACK message

End of Erase Memory command

Send NACK message
3.8 **Write Protect command**

The Write Protect command is used to enable the write protection for some or all Flash memory sectors. When the bootloader receives the Write Protect command, it transmits an ACK message to the host if RDP is disabled. Otherwise, it transmits a NACK message.

After the transmission of the ACK byte, the bootloader waits to receive the Flash memory sector codes from the application.

At the end of the Write Protect command, the bootloader transmits the ACK message.

**Note:**

1. If a second Write Protect command is executed, the Flash memory sectors protected by the first command become unprotected, and only the sectors passed within the second Write Protect command become protected.

2. The total number of sectors and the sector numbers to be protected are not checked. This means that no error is returned when a command is passed with a wrong number of sectors to be protected, or a wrong sector number.

![Figure 16. Write Protect command (host side)](image)

The sector code is sent on one byte. The number of sectors and the codes are sent together with the command ID of the Write Protect command.
3.9 Write Unprotect command

The Write Unprotect command is used to disable the write protection of all the Flash memory sectors. When the bootloader receives the Write Unprotect command, it transmits an ACK message to the host if RDP is disabled. Otherwise, it transmits a NACK message. After the transmission of the ACK message, the bootloader disables the write protection of all the Flash memory sectors.
**Figure 18. Write Unprotect command (host side)**

1. Start Write Unprotect command
2. Send message ID = 73h
3. Wait ACK or NACK
4. ACK
5. Wait ACK
6. NACK
7. End of Write Unprotect command

**Figure 19. Write Unprotect command (device side)**

1. Start Write Unprotect command
2. Received message with ID = 73h?
   1. Yes
   2. No
3. RDP active?
   1. Yes
   2. No
4. Send ACK message
5. Send NACK message
6. End of Write Unprotect command
3.10 Readout Protect command

The Readout Protect command is used to enable the Flash memory read protection. When the bootloader receives the Readout Protect command, it transmits an ACK message to the host if RDP is disabled. Otherwise, it transmits a NACK message. After the transmission of the ACK message, the bootloader enables the read protection of the Flash memory.

Figure 20. Readout Protect command (host side)
3.11 Readout Unprotect command

The Readout Unprotect command is used to disable the Flash memory read protection. When the bootloader receives the Readout Unprotect command, it transmits an ACK message to the host. After the transmission of the ACK message, the bootloader deactivates the RDP.
Figure 22. Readout Unprotect command (host side)

1. Start Readout Unprotect command
2. Send message ID = 92h
3. Wait ACK
4. Wait ACK
5. End of Readout Unprotect command

Figure 23. Readout Unprotect command (device side)

1. Start Readout Unprotect command
2. Received message with ID = 92h?
   - Yes: Send ACK message
   - No: Send NACK message
   - No: Send ACK message
3. End of Readout Unprotect command
Revision history

**Table 3. Document revision history**

<table>
<thead>
<tr>
<th>Date</th>
<th>Version</th>
<th>Changes</th>
</tr>
</thead>
<tbody>
<tr>
<td>14-Nov-2019</td>
<td>1</td>
<td>Initial release.</td>
</tr>
</tbody>
</table>
List of tables

Table 1. Applicable products ................................................................. 1
Table 2. FDCAN bootloader commands ............................................... 4
Table 3. Document revision history ...................................................... 26
List of figures

Figure 1. Bootloader for STM32 with FDCAN ...................................................... 2
Figure 2. Get command (host side) ............................................................. 5
Figure 3. Get command (device side) ........................................................... 6
Figure 4. Get Version command (host side) ..................................................... 7
Figure 5. Get Version command (device side) .................................................. 8
Figure 6. Get ID command (host side) ........................................................... 9
Figure 7. Get ID command (device side) ....................................................... 10
Figure 8. Read Memory command (host side) ............................................... 11
Figure 9. Read Memory command (device side) ........................................... 12
Figure 10. Go command (host side) ............................................................ 13
Figure 11. Go command (device side) ........................................................... 14
Figure 12. Write Memory command (host side) .......................................... 15
Figure 13. Write Memory command (device side) ....................................... 16
Figure 14. Erase Memory command (host side) .......................................... 18
Figure 15. Erase Memory command (device side) ...................................... 19
Figure 16. Write Protect command (host side) ......................................... 20
Figure 17. Write Protect command (device side) ....................................... 21
Figure 18. Write Unprotect command (host side) ..................................... 22
Figure 19. Write Unprotect command (device side) ................................... 22
Figure 20. Readout Protect command (host side) ...................................... 23
Figure 21. Readout Protect command (device side) .................................... 24
Figure 22. Readout Unprotect command (host side) .................................. 25
Figure 23. Readout Unprotect command (device side) .............................. 25