AN3156
Application note

USB DFU protocol used in the STM32™ bootloader

Introduction

This application note describes the USB DFU protocol used in STM32 microcontroller bootloader. It details each supported command. For more information about the USB hardware resources and requirements for your device bootloader, please refer to the “STM32 system memory boot mode” application note (AN2606).

Related documents

Available from www.st.com:

AN2606 “STM32 system memory boot mode”

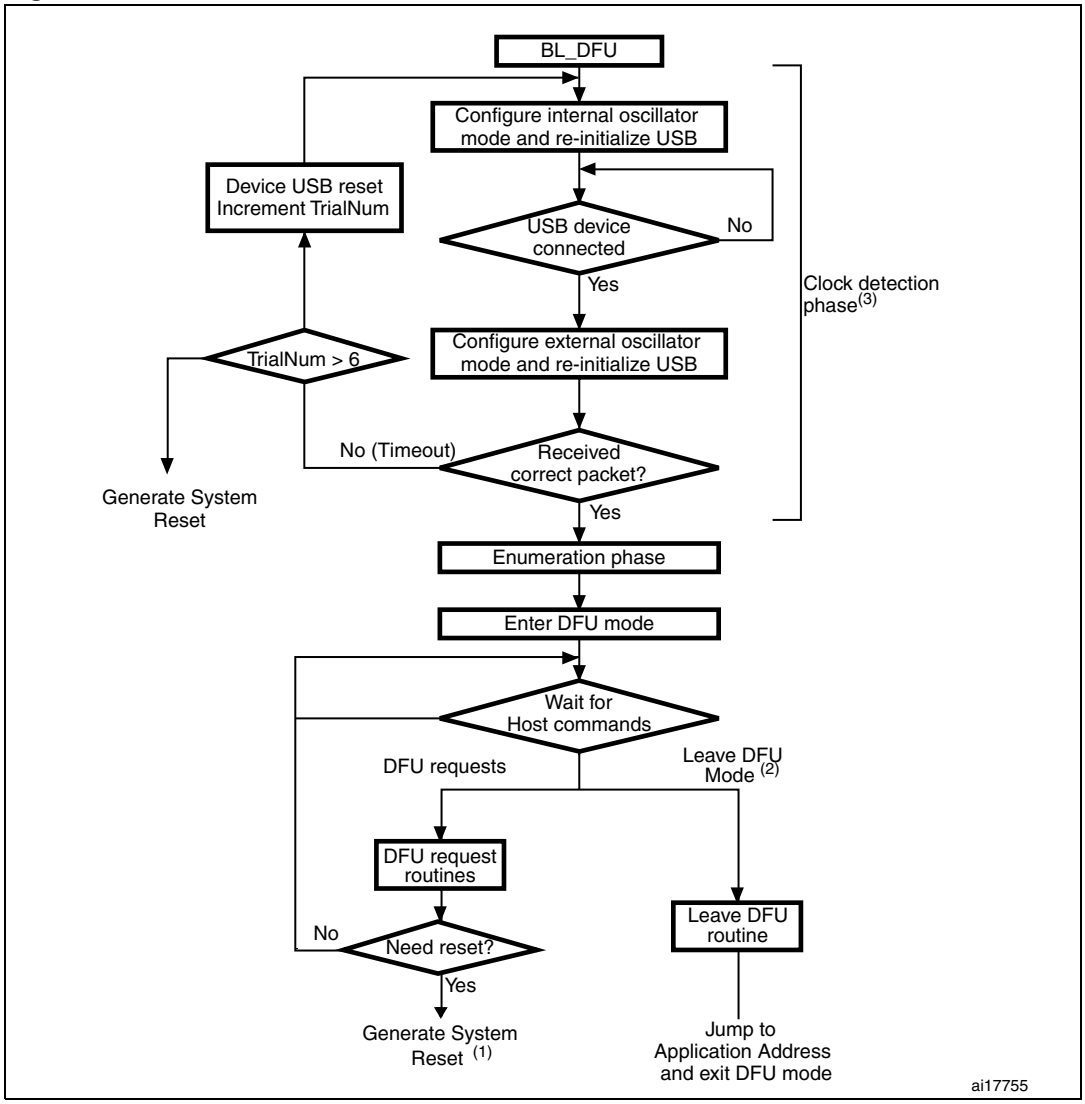
Contents

List of tables

List of figures

1 Bootloader code sequence

Figure 1. Bootloader for STM32 with USB DFU



1. After system reset, the device may return to the BL_DFU loop or execute code from Flash memory/RAM depending on the connection states and the boot pin status.
2. Leave DFU is achieved by a 0 Data Download request followed by GetStatus request and Device Reset.
3. After six trials (the three clock configurations are tested twice), a System Reset is generated.

Once the system memory boot mode is entered and the STM32 device has been configured (for more details refer to application note AN2606 “STM32 system memory boot mode”), the bootloader code configures the USB and its interrupts, and waits for the “enumeration done” interrupt.

Once this interrupt is detected (a host is present, has connected to the device and enumerated it), the system is configured in External oscillator mode and the USB device is re-initialized.

The device first tries the 25 MHz configuration, then, if it fails, the 14.7456 MHz configuration, and finally, if it fails, the 8 MHz configuration. If it fails, this operation is repeated with a large timeout value (the three configurations are retested). If the second trial also fails, a system reset is generated.

The USB enumeration is performed as soon as the USB cable is plugged (or immediately if the cable is already plugged). If you do not want the STM32 to enter the USB DFU bootloader application, the USB cable has to be unplugged before reset.

The bootloader version is returned in the device descriptor in the MSB of the bcd Device field (example: 0x2000 = Version 2.0).

2 USB DFU bootloader requests

USB DFU bootloader supports the DFU protocol and requests compliant with the “Universal Serial Bus Device Upgrade Specification for Device Firmware Upgrade” Version 1.1, Aug 5, 2004. For more details concerning these requests, refer to the specification.

Table 1 and *Table 2* enumerate the DFU Class-Specific requests and their parameters.

Table 1. DFU class requests

Request	Request code	Request description
DFU_DETACH	0x00	Requests the device to leave DFU mode and enter the application.
DFU_DNLOAD	0x01	Requests data transfer from Host to the device in order to load them into device internal Flash. Includes also erase commands.
DFU_UPLOAD	0x02	Requests data transfer from device to Host in order to load content of device internal Flash into a Host file.
DFU_GETSTATUS	0x03	Requests device to send status report to the Host (including status resulting from the last request execution and the state the device will enter immediately after this request).
DFU_CLRSTATUS	0x04	Requests device to clear error status and move to next step.
DFU_GETSTATE	0x05	Requests the device to send only the state it will enter immediately after this request.
DFU_ABORT	0x06	Requests device to exit the current state/operation and enter idle state immediately.

Note: The Detach request is not meaningful in the case of the bootloader. The bootloader is started by a system reset depending on the boot mode configuration settings, which means that no other application is running at this time.

Table 2. Summary of DFU class-specific requests

bmRequest	bRequest	wValue	wIndex	wLength	Data
00100001b	DFU_DETACH	wTimeout	Interface	Zero	None
00100001b	DFU_DNLOAD	wBlockNum	Interface	Length	Firmware
10100001b	DFU_UPLOAD	Zero	Interface	Length	Firmware
00100001b	DFU_GETSTATUS	Zero	Interface	6	Status
00100001b	DFU_CLRSTATUS	Zero	Interface	Zero	None
00100001b	DFU_GETSTATE	Zero	Interface	1	State
00100001b	DFU_ABORT	Zero	Interface	Zero	None

Communication safety

The communication between host and device is secured by the embedded USB protection mechanisms (CRC checking, Acknowledgements, etc.). No further protection is performed for transferred data or for bootloader specific commands/data.

3 DFU bootloader commands

The DFU_DNLOAD and DFU_UPLOAD requests are mainly used to perform simple Write Memory and Read Memory operations. They are also used to initiate the integrated bootloader commands (write, read unprotect, erase, set address, etc.). The DFU_GETSTATUS command then triggers the command execution.

In the DFU download request the command is selected through the **wValue** parameter in the USB request structure. If **wValue** = 0 then the data sent by the host after the request is a bootloader command code. The first byte is the command code and the other bytes (if any) are the data related to this command.

In the DFU upload request the command is selected through the **wValue** parameter in the USB request structure. If **wValue** = 0 then Get Command is selected and performed.

Table 3. DFU bootloader commands

DFU request	Bootloader command	Write protection disabled Read protection disabled	Write protection enabled Read protection disabled	Read protection enabled
DFU_UPLOAD	**Read Memory**	Allowed	Allowed	Not allowed
	Get	Allowed	Allowed	Allowed
DFU_DNLOAD	**Write Memory**	Allowed	Allowed(1)	Not allowed
	Erase	Allowed	Allowed**(1)**	Not allowed
	Read Unprotect	NA(2)	NA**(2)**	Allowed(3)
	Set Address Pointer	Allowed	Allowed	Allowed
	Leave DFU mode	Allowed	Allowed	Allowed

1. This operation is allowed but not effective: the bootloader does not return an error but the operation is not executed since the sectors are write-protected. This applies only to the Flash memory. It does not apply to the RAM memory or the option byte area.
2. This operation is allowed but has no meaning since the memory is not protected.
3. In this case, both the Flash memory (from 0x0800 0000) and the RAM are erased. The option byte area is reset to default values.

If you perform a Read Unprotect operation while the memory is not protected, the entire RAM memory is cleared by the bootloader firmware and the Flash memory is not erased (since it was not previously read-protected).

There are no commands for the Write Protect, Write Unprotect and Read Protect operations. These operations should be performed through the Write Memory and Read Memory commands used for the option byte area.

3.1 Device-dependent bootloader parameters

While the DFU bootloader protocol's command set and sequences are the same for all the STM32 devices, some parameters are device-dependent. For a few commands, the value of some parameters may depend on the device used. The concerned parameters are listed below:

- PID (product ID), which changes with the device
- Valid memory addresses (RAM, Flash memory, system memory, option byte areas) accepted by the bootloader when the Read Memory, Go and Write Memory commands are executed.
- Size of the Flash memory sector used when executing the Write Protect command.

For more details about the value of these parameters for the device you are using, please refer to the "Device-dependent bootloader parameters" section in the "STM32 system memory boot mode" application note (AN2606).

4 DFU_UPLOAD request commands

The upload request allows different commands to be performed. The command selection is done through the value of parameter **wValue** in the USB request structure. The operations described in *Section 4.1* to *Section 5.5* are supported.

4.1 Read memory

The Read memory operation is selected when **wValue** > 1.

The host requests the device to send a specified number of data bytes (**wLength**) from valid memory address (see note) of the internal Flash memory, embedded RAM, system memory or from the option bytes.

Note: Refer to Section 3.1: Device-dependent bootloader parameters for more details about the valid memory addresses for the device you are using.

The allowed number of bytes to be read depends on the memory target:

- For the internal Flash memory, embedded RAM and system memory: read size can be from 2 to 2048 bytes.
- For the option bytes: read size should be 16 bytes.

The address, from which the host requests to read data, is computed using the value of wBlockNumber (**wValue**) and the address pointer according to the following formula:

Address = ((wBlockNum – 2) × wTransferSize) + Address_Pointer, where:

– wTransferSize is the length of the requested data buffer.

The address pointer should be previously specified through a Set Address Pointer command (using a DFU_DNLOAD request). Otherwise (if no address was previously specified) the device assumes that it is the internal Flash start address (0x08000000).

If the Flash Read Protection is enabled, the Read operation is not performed and the returned device status is (Status = dfuERROR, State = errVENDOR) whatever the target (internal Flash memory, embedded RAM, system memory or option bytes).

4.2 Get command

This command is selected when **wValue** = 0.

The host requests to read the commands supported by the bootloader. After receiving this command, the device returns N bytes representing the command codes.

The STM32 sends bytes as follows (N = 4):

Byte 1: 0x00 - Get command

Byte 2: 0x21 - Set Address Pointer

Byte 3: 0x41 - Erase

Byte 4: 0x92 - Read Unprotect

The processing of the DFU_UPLOAD command is shown in *Figure 2* and *Figure 3*.

Figure 2. DFU_UPLOAD request: Device side

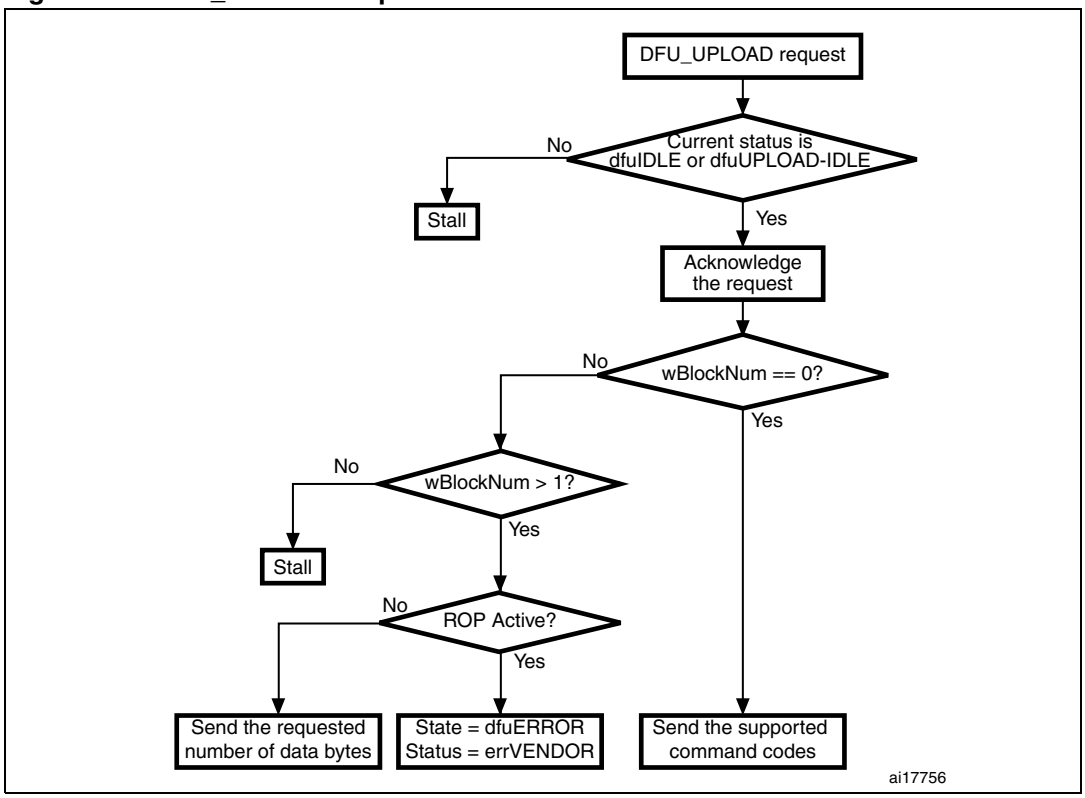
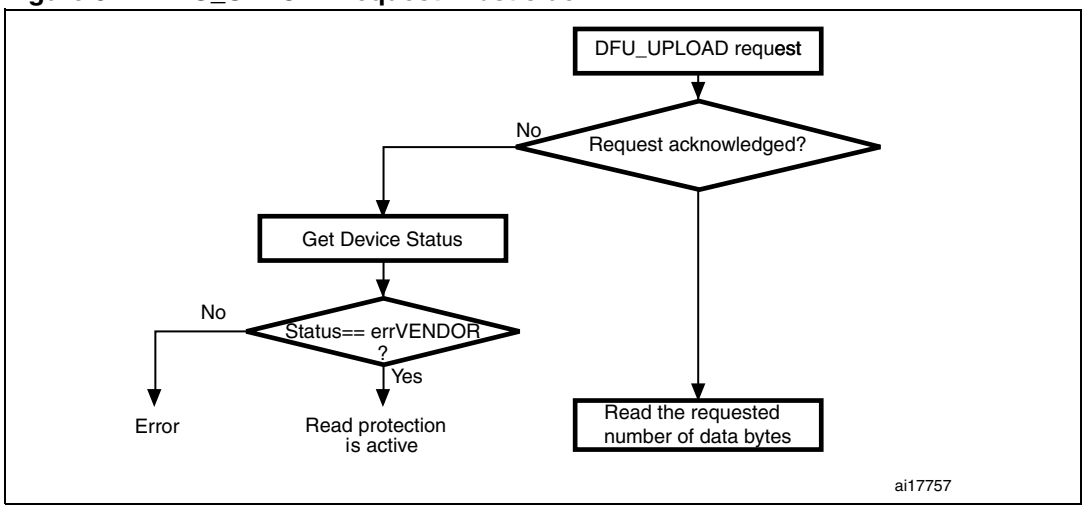


Figure 3. DFU_UPLOAD request: Host side



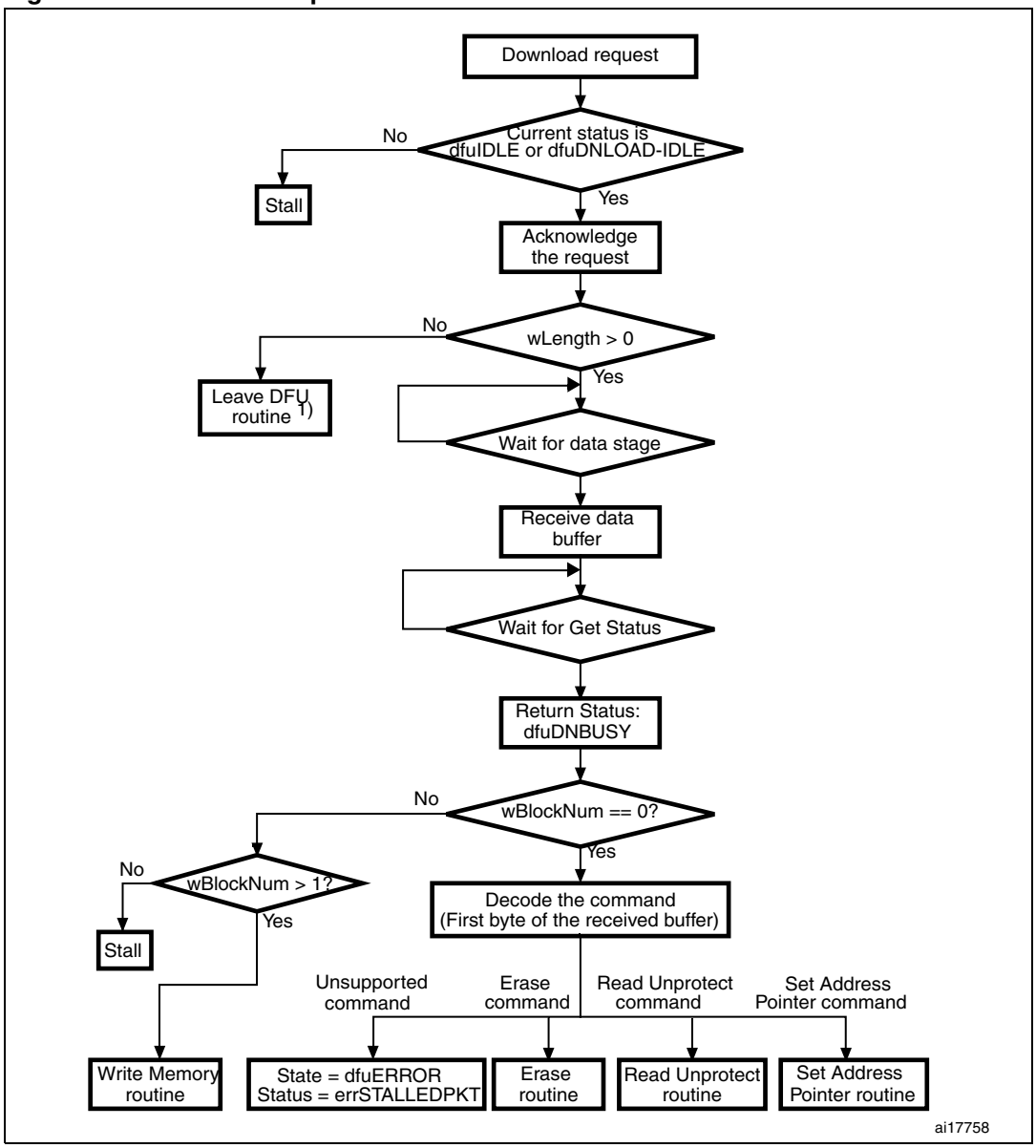
Note: Before issuing an Upload request, the host has to check that the device is in a correct state (dfuIDLE or dfuUPLOAD-IDLE state) and that there is no error reported in the status. If the device is not in the required state/status, the host has to clear any error (DFU_CLRSTATUS request) and get the new status until the device returns to dfuIDLE state.

5 DFU_DNLOAD request commands

The download request is used to perform different commands. The command selection is done through the value of parameter **wValue** in the USB request structure. The following operations are supported:

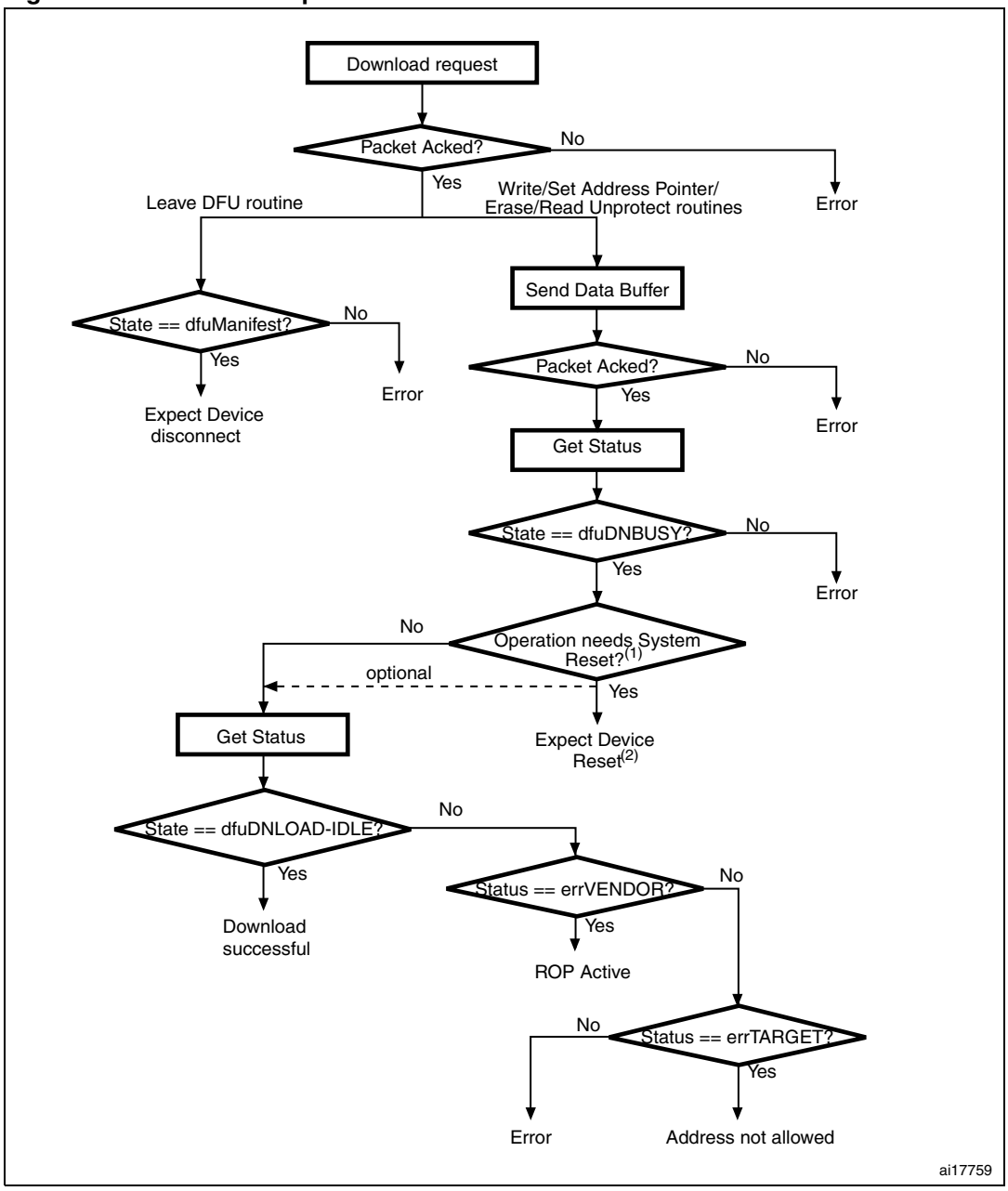
- Write Memory (**wValue** > 1)
- Set Address Pointer (**wValue** = 0 and first byte = 0x21)
- Erase (**wValue** = 0 and first byte = 0x41)
- Read Unprotect (**wValue** = 0 and first byte = 0x92)
- Leave DFU (leave DFU mode and Jump to application)

Figure 4. Download request: Device side



1. This routine can be used to reset the device or to jump to the application.

Figure 5. Download request: Host side



1. Operations needing System Reset are: Read Unprotect command and Write operations to the option bytes.
2. After returning to the dfuDNBUSY state, the device executes the requested operation and performs a system reset. The host may simply wait for the next enumeration or perform Get status again but the device will not be able to respond, unless it fails to execute the requested operation.

Note: Before issuing a Download request, the host has to check that the device is in a correct state: dfuIDLE or dfuDNLOD-IDLE, and that there is no error reported in the status. If the device is not in the required state/status, the host has to clear any error (DFU_CLRSTATUS request) and get the status again until the device returns to the dfuIDLE state.

5.1 Write memory

The Write memory operation is selected when **wValue** > 1.

The host requests the device to receive a specified number of data bytes (**wLength**) to load them into valid memory addresses (see note) in internal Flash memory, embedded RAM or option bytes.

Note: Refer to Section 3.1: Device-dependent bootloader parameters for more details about the valid memory addresses for the device you are using.

The allowed number of bytes to be written depends on the memory target:

- For the internal Flash memory and embedded RAM: write size can be from 2 to 2048 bytes.
- For the option bytes: write size should be 16 bytes.

Note: A different write size is possible for the option bytes but it is recommended to write the entire block (16 bytes) at a time in order to ensure data integrity. When the target is the option byte area, the address pointer must always be the start address of the option bytes, otherwise, the request is not performed.

The Write memory operation is effectively executed only when a DFU_GETSTATUS request is issued by the host. If the status returned by the device is not dfuDNBUSY, then an error has occurred.

A second DFU_GETSTATUS request is needed to check if the command has been correctly executed, except when the destination is the option byte area (in this case the device is immediately reset after the write operation completion). If the received address is wrong or unsupported, the device status is then (Status = dfuERROR, State = errTARGET).

The address, to which the host requests to write data, is computed using the value of wBlockNumber (**wValue**) and the address pointer according to the same formula as for an upload request:

Address = ((wBlockNum – 2) × wTransferSize) + Addres_Pointer, where:

- wTransferSize: length of the data buffer sent by the host
- wBlockNumber: value of the **wValue** parameter

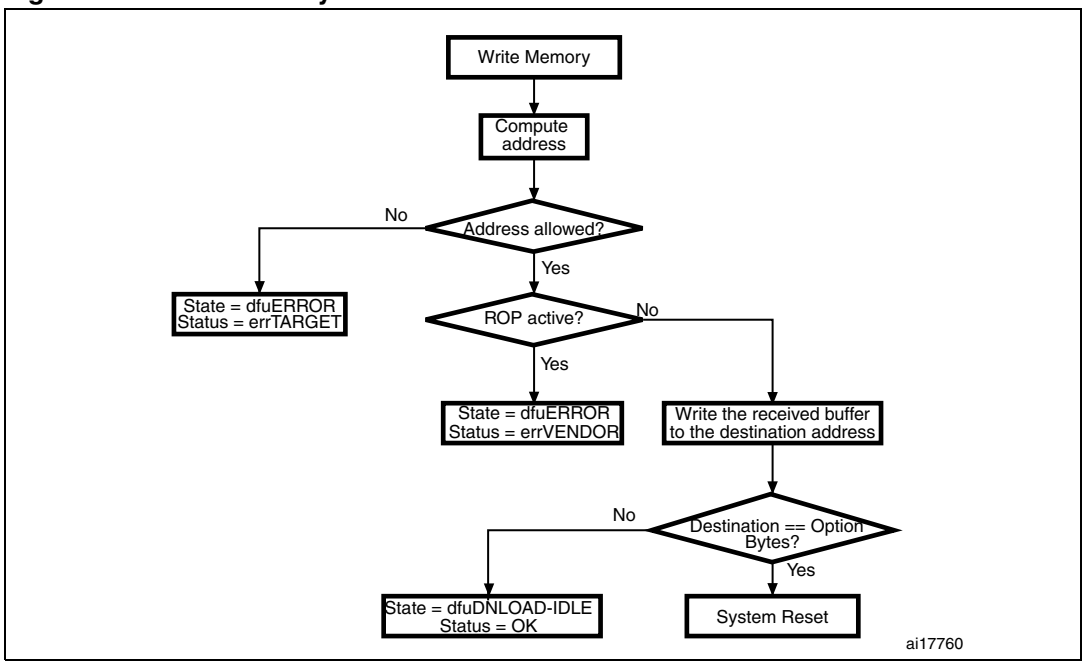
If the Flash Read Protection is enabled, the Write memory operation is not performed and the returned device status is (Status = dfuERROR, State = errVENDOR) whatever the target (internal Flash, embedded RAM or option bytes).

If the Write memory command is issued to the option byte area, all options are erased before writing the new values, and at the end of the command the bootloader generates a system reset to take into account the new configuration of the option bytes.

Note: 1 When writing to the RAM, you should take care not to overlap the first RAM memory used by the bootloader firmware.

2 No error is returned when performing write operations on write protected sectors.

Figure 6. Write Memory: Device side



5.2 Set Address Pointer command

The Set Address Pointer command is selected when **wValue** = 0 and the first byte of the buffer sent by the host is 0x21. The buffer length should be 5 (the four remaining bytes are the address bytes, LSB first (32-bit address format)).

The host sends a DFU_DNLOAD request with the above mentioned parameters to set the address pointer value used for computing the start address for Read and Write memory operations.

The STM32 receives bytes as follows:

Byte 1: 0x21 - Set Address Pointer command

Byte 2: A[7:0] - LSB of the address pointer

Byte 3: A[15:8] - Second byte of the address pointer

Byte 4: A[22:16] - Third byte of the address pointer

Byte 4: A[31:23] - MSB of the address pointer

After sending the Set Address Pointer command, the host has to send the DFU_GETSTATUS request.

The Set AddressPointer command is effectively executed only when a DFU_GETSTATUS request is issued by the host. If the status returned by the device is not dfuDNBUSY, then an error has occurred.

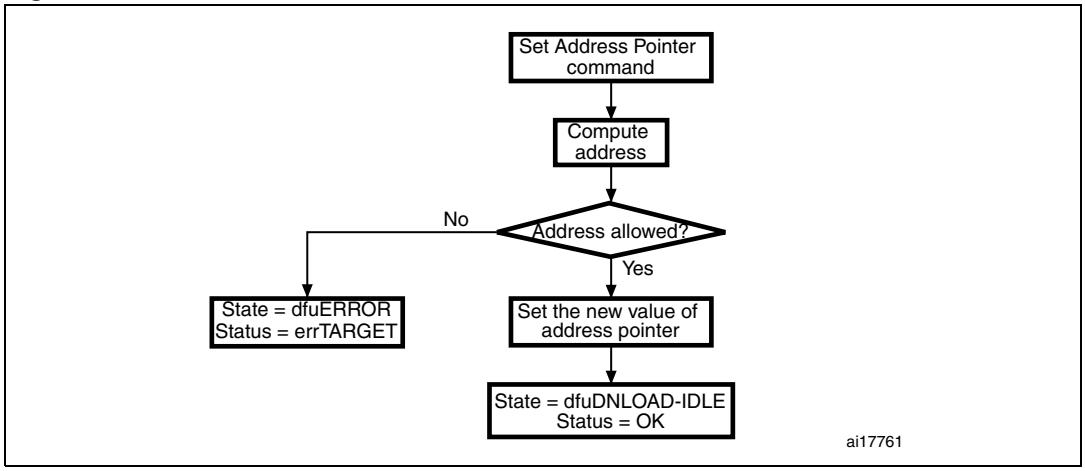
A second DFU_GETSTATUS request is needed to check if the command has been correctly executed. If the received address is wrong or unsupported, the device status is then (Status = dfuERROR, State = errTARGET).

The allowed locations for address pointer values are valid memory addresses (see note) in the internal Flash memory, embedded RAM, system memory and option bytes.

Note: 1 Refer to Section 3.1: Device-dependent bootloader parameters for more details about the valid memory addresses for the device you are using.

2 The Set Address Pointer command is allowed and executed when the Flash Read Protection is enabled or disabled.

Figure 7. Set Address Pointer command: Device side



5.3 Erase command

The Erase command is selected when **wValue** = 0 and the first byte of the buffer sent by the host is 0x41. The buffer length may be 5 bytes (the four remaining bytes are the address bytes, LSB first) for the page erase operation or only 1 byte (only the command byte) for the Mass erase operation.

The host sends a DFU_DNLOAD request with the above parameters to erase one page of the internal Flash memory or to perform a mass erase of this Flash memory.

The device receives the bytes as follows (page erase):

Byte 1: 0x41 - Erase command

Byte 2: A[7:0] - LSB of the page address

Byte 3: A[15:8] - Second byte of the page address

Byte 4: A[22:16] - Third byte of the page address

Byte 4: A[31:23] - MSB of the page address

Or, if a 1-byte command is received:

The STM32 receives the bytes as follows (Mass Erase):

Byte 1: 0x41 - Erase command

After sending an Erase command, the host has to send a DFU_GETSTATUS request.

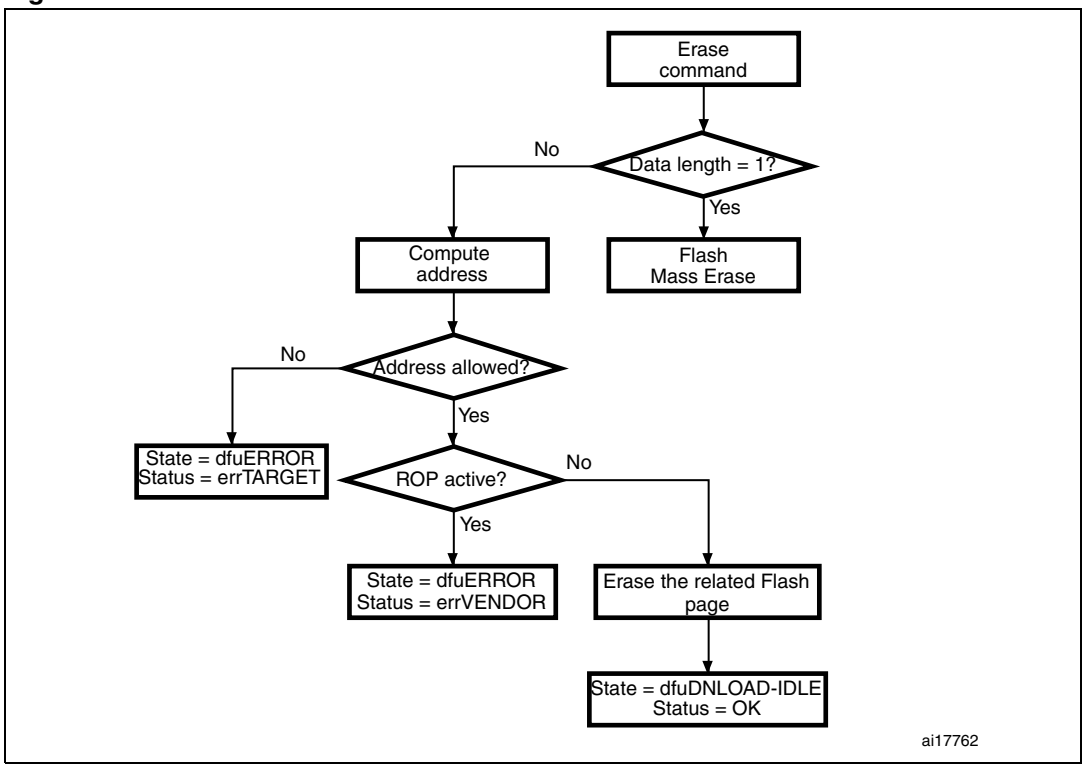
The Erase command is effectively executed only when a DFU_GETSTATUS request is issued by the host. If the status returned by the device is not dfuDNBUSY, then an error has occurred.

A second DFU_GETSTATUS request is needed to check if the command has been correctly executed. If the received page address is wrong or unsupported, the device status is then (Status = dfuERROR, State = errTARGET). If the Flash Read Protection is active, then the device returns the status (Status = dfuERROR, State = errVENDOR) and the erase operation is ignored by the device.

The allowed Erase page addresses are internal Flash memory addresses.

Note: No error is returned when performing Erase operations on write protected sectors.

Figure 8. Erase command: Device side



5.4 Read Unprotect command

The Read Unprotect command is selected when **wValue** = 0 and the first byte of the buffer sent by the host is 0x92. The buffer length should be only 1 byte (only the command byte).

The host sends a DFU_DNLOAD request with the above parameters to remove the read protection of the internal Flash memory.

The device receives the byte as follows:

Byte 1: 0x92 - Read Unprotect command

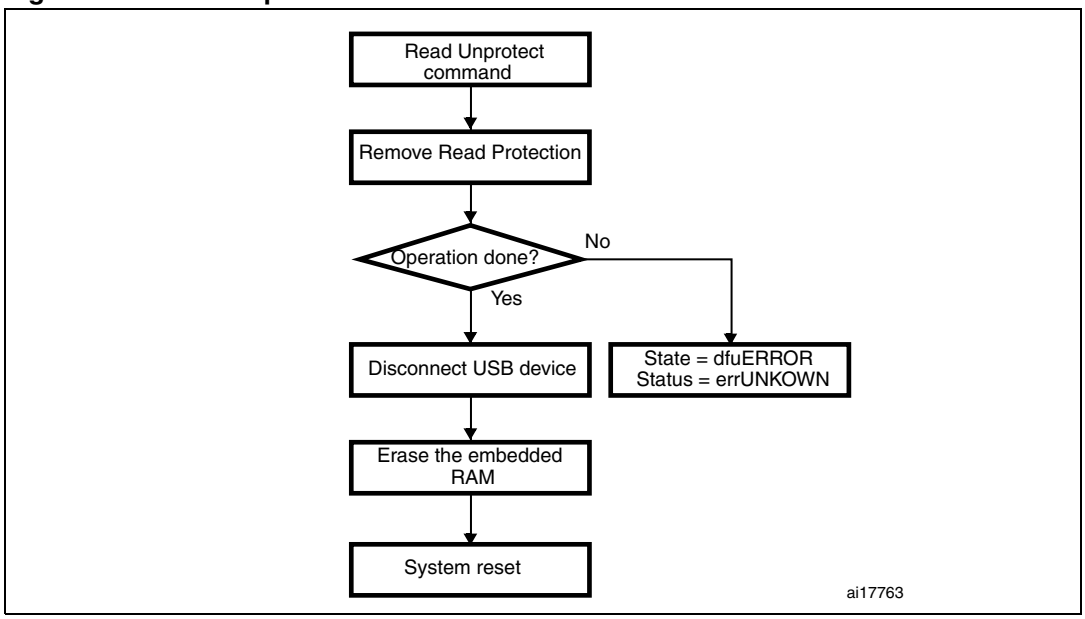
After sending a Read Unprotect command, the host has to send a DFU_GETSTATUS request.

The Read Unprotect command is effectively executed only when a DFU_GETSTATUS request is issued by the host. If the status returned by the device is not dfuDNBUSY, then an error has occurred. After this operation, the device removes the Read Protection and, consequently, both the internal Flash and the embedded RAM are fully erased.

Hence, just after executing this command, the device disconnects itself and executes a system reset. In this case, the device is not able to respond to a second Get Status request. And the host has to wait until the device is enumerated again.

A second DFU_GETSTATUS request may also be issued (if the device is still connected) to check if the command has been correctly executed. If the device fails to execute the command it returns an error status (depending on the error type).

Figure 9. Read Unprotect command: Device side



5.5 Leave DFU mode

It is possible to exit DFU mode (and bootloader) and jump to a loaded application (in the internal Flash or in the embedded RAM) using the DFU download request.

The Host sends a DFU_DNLOAD request with 0 data length (no data stage after the request) in order to inform the device that it will have to exit DFU mode. The device acknowledges this request if the current state is dfuDNLOAD-IDLE or dfuIDLE.

The DFU Leave operation is effectively executed only when a DFU_GETSTATUS request is issued by the host. If the status returned by the device is not dfuMANIFEST, then an error has occurred. After this operation, the device performs the following:

- it disconnects itself
- it initializes the registers of the peripherals used by the bootloader to their default reset values
- it initializes the user application's main stack pointer
- it jumps to the memory location programmed in the received 'address pointer + 4', which corresponds to the address of the application's reset handler
  For example if the received address is 0x0800 0000, the bootloader will jump to the memory location programmed at address 0x0800 0004.
  In general, the host should send the base address where the application to jump to is programmed.

The address pointer has to be set (using the Set Address Pointer command) before launching the Leave DFU routine, otherwise, the bootloader will jump to the default address (internal Flash memory start address: 0x08000000).

The address pointer can also be set through the last Write Memory operation: if a download operation is performed, the address pointer used for this download will be stored and used later for the jump.

Note: If the address pointer points to an address that does not contain executable code, then the device is reset and, depending on the state of the boot pins, may re-enter the bootloader mode.

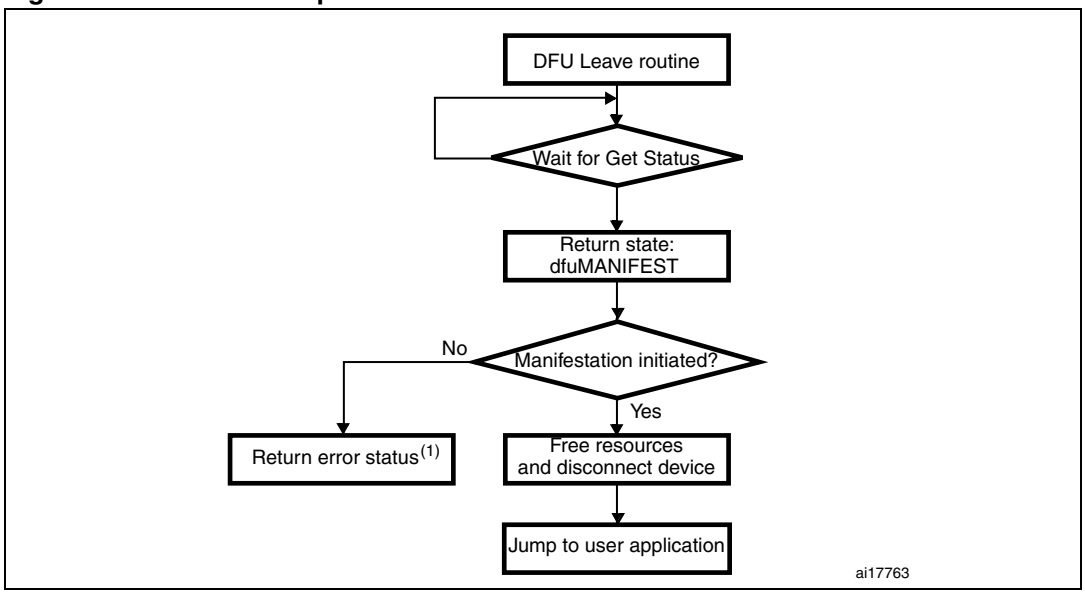
Since the bootloader DFU application is not manifestation-tolerant, the device will not be able to respond to host requests after a manifestation phase is completed.

A second DFU_GETSTATUS request may also be issued (if the device is still connected) to check if the command has been correctly executed. If the device fails to execute the command it returns an error status (depending on the error type).

Note: 1 The Jump to application works only if the user application sets the vector table correctly to point to the application address.

2 When performing a jump from the bootloader to a loaded application code which uses the USB IP, the user application has to disable all pending USB interrupts and reset the core before enabling interrupts. Otherwise, a pending interrupt (issued from the bootloader code) may interfere with the user code and cause a functional failure. This procedure is not needed after exiting the system memory boot mode.

Figure 10. Leave DFU operation: Device side



1. This status depends on the error origin and the current status.

6 Bootloader protocol version evolution

Table 4 lists the bootloader versions.

Table 4. Bootloader protocol versions

Version	Description
V2.0	Initial bootloader version.

7 Revision history

Table 5. Document revision history

Date	Revision	Changes
09-Mar-2010	1	Initial release.