



Software Updating

Teldat-Dm 835-I

Copyright© Version 11.00 Teldat SA

Legal Notice

Warranty

This publication is subject to change.

Teldat offers no warranty whatsoever for information contained in this manual.

Teldat is not liable for any direct, indirect, collateral, consequential or any other damage connected to the delivery, supply or use of this manual.

Table of Contents

Chapter 1	Software Updating Via FTP	1
1.1	Introduction	1
1.2	Updating Process.	1
1.2.1	Distributing with BIOS, C.I.T and FWs files.	1
1.2.2	Distributing with the C.I.T Image file (IMG)	3
1.3	FTP Features	4
1.3.1	INTEGRITY Test	4
1.3.2	CHECK Mode	5
1.4	Known Problems	6
1.4.1	Error writing file (550)	6
1.4.2	Connection closed by remote host	6
1.4.3	File transfer has stopped	7
1.4.4	Unable to open file (550).	7
1.4.5	Unix Clients (ASCII mode)	7
1.5	Information required for updating	8
1.5.1	How to determine the appropriate distribution and the appropriate binary.	8
1.5.2	How to determine the necessary firmware	10
1.6	FTP clients	10
1.6.1	FileZilla Client	10
1.6.2	WinSCP Client	14
1.6.3	FTP client through Linux console	19
Chapter 2	Appendix A. Backup Systems	20
2.1	Distributing with BIOS, CIT and FWs files	20
2.1.1	Two CIT codes loaded in the Flash disk	20
2.1.2	Flash Backup System	21
2.2	Distributing with the CIT image file (IMG)	24
2.2.1	Introduction	24
2.2.2	Operating a system with double image in flash	24

Chapter 1 Software Updating Via FTP

1.1 Introduction

Teldat routers execute software known as C.I.T. (Código Integrado Teldat – Teldat Integrated Code). This is made up of various elements:

- **BOOT**

This is a small start up program recorded in a read-only device. Losing this program is practically impossible, and recouping a device is also possible in extreme cases. This element cannot be updated via software.

- **BIOS FLASH**

This is the basic interface to the router's underlying hardware and is responsible for abstracting much of the hardware from the C.I.T. In this way, the variations produced in the hardware (e.g., changing the integrated circuit used to control PSTN) are transparent to the C.I.T.

- **C.I.T. (Código Integrado Teldat – Teldat Integrated Code)**

This is the part of the code that handles the internetworking processes (IP routing, X.25, IPSec, ATM, etc) as well as the configuration and monitoring console. This is also known as "application".

- **Auxiliary Files (*.BFW, ...)**

To simplify the modular updating of Teldat routers and reduce the size of the C.I.T, certain blocks are provided as isolated files. The need for these depends on the available hardware. E.g., Teldat devices support various ADSL chipsets and, depending on the type of chipset available in your device, one firmware (BFW) or another will be used.

- **Image file(*.img)**

In some devices, the BIOS, C.I.T and FWs are distributed in a single file with extension img.

The process of updating Teldat router software consists of substituting one or several of the previously mentioned elements. This manual explains the updating process via FTP.

1.2 Updating Process

Teldat routers have an FTP server to which files can be transferred for device software updating. This server is only accessible if the device has started up correctly (application being executed).

1.2.1 Distributing with BIOS, C.I.T and FWs files

The steps to execute updating are as follows:

- (1) Extract the distribution content to a directory; if this is successful, the content will not be altered.
- (2) Connect to the device's FTP server(you need a user and password: default is user "root" without password).

```
ftp 192.168.1.100
Connected to 192.168.1.100.
220 FTP server ready, 1 active clients of 1 simultaneous clients allowed.
Name (192.168.1.100:admin): root
331 User name accepted, need password.
Password: 230
User login complete.
Remote system type is UNIX.
ftp>
```

- (3) Configure the binary mode through the "bin" command, and, optionally, HASH marking through the "hash" command.

```
ftp> bin
200 TYPE is set to IMAGE.
ftp> hash
Hash mark printing on (1024 bytes/hash mark).
ftp>
```

- (4) Transfer the BIOS FLASH through the "put <bxxx.bin>" command.

```
ftp> put bxxxx.bin
```

```

local: bxxxxx.bin remote: bxxxxx.bin
200 PORT is set to IP ADDR = 192.168.1.50 PORT = 58804
150 Data connection open, checked file transfer in process...
#####
226 STOR completed, 268160 bytes processed, data connection is closed.
268160 bytes sent in 0.22 secs (1172.4 kB/s)
ftp>

```

- (5) Once the transfer has finalized, execute the recording command by entering `quote site savebuffer`.

```

ftp> quote site savebuffer
200 SAVEBUFFER completed O.K.
ftp>

```

- (6) Transfer the application through the “`put <application.bin>`” command.

```

ftp> put xxxxxxxx.bin
local: xxxxxxxx.bin remote: xxxxxxxx.bin
200 PORT is set to IP ADDR = 192.168.1.50 PORT = 45801
150 Data connection open, checked file transfer in process...
#####
226 STOR completed, 7185536 bytes processed, data connection is closed.
7185536 bytes sent in 2.99 secs (2348.7 kB/s)
ftp>

```

- (7) Once the transfer has completed, execute the recording `quote site savebuffer` command.

```

ftp> quote site savebuffer
200 SAVEBUFFER completed O.K.
ftp>

```

- (8) Transfer and store the required firmware (files with “bfw” extension) one by one through the `put <firmware.bfw>` and `quote site savebuffer` commands. In order to determine the necessary firmware, please see [Information required for updating](#) on page 8.

```

ftp> put fw000010.bfw
local: fw000010.bfw remote: fw000010.bfw
200 PORT is set to IP ADDR = 192.168.1.50 PORT = 58248
150 Data connection open, checked file transfer in process...
#####
226 STOR completed, 249472 bytes processed, data connection is closed.
249472 bytes sent in 0.10 secs (2543.7 kB/s)
ftp> quote site savebuffer
200 SAVEBUFFER completed O.K.
ftp>

```

- (9) Finally, and optionally, there is a command that allows you to check if the device has all the required files and if the element versions are consistent.

```

ftp> quote site coherence
211-COHERENCE results
CIT          v11.0.1 ID 0x00000019 HDW LVL 13
BIOS         v5.1 HDW LVL 7
fw000010.bfw v1.1.0 HDW LVL 12
211 COHERENCE results end
ftp>

```

You can also check the integrity of a file by calculating its MD5 signature and contrasting it with the one included in the distribution .md5 file.

```

ftp> quote xmd5 fw000010.bfw
250 c103da2bb21508c797088eb4b5ca5a7c
ftp>

```

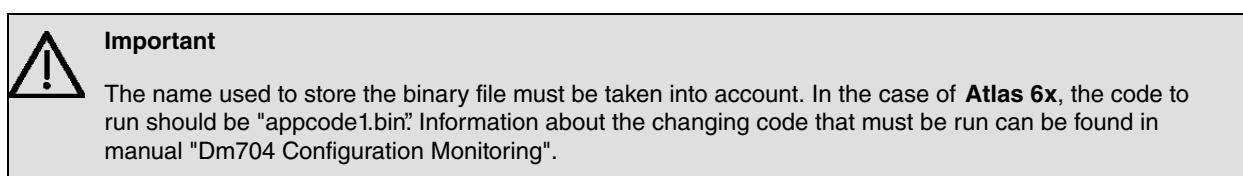
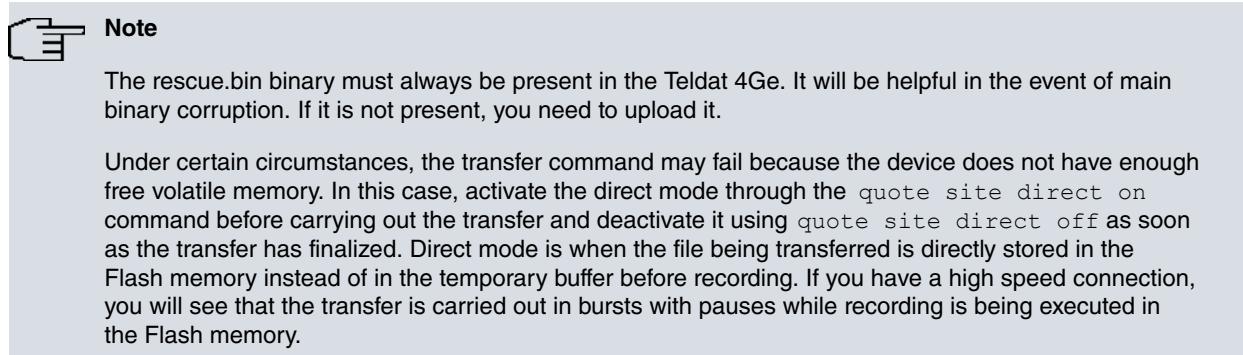
- (10) Restart the device through the `quote site reload on` command; if you are exiting from FTP as usual, the device restarts after some 30 seconds. If you are exiting FTP using **CTRL+C**, the device restarts immediately. You can also restart the device using the `load immediate` console command.

```

ftp> quote site reload on
200 RELOAD mode is set to ON.
ftp> quit
221 Goodbye.
>

load immediate
Are you sure to reload the device(Yes/No)? yes

```



1.2.2 Distributing with the C.I.T Image file (IMG)

The steps to follow to execute updating are as follows:

- (1) Decompress the distribution content to a directory; if it works properly, the content will remain unaltered.
- (2) Connect to the device's FTP server (you need a user and password: default is user "root" without password).

```
ftp 192.168.1.25
Connected to 192.168.1.25.
220 FTP server ready, 1 active clients of 4 simultaneous clients allowed.
Name (192.168.1.25:admin): root
331 User name accepted, need password.
Password: 230
User login complete.
Remote system type is UNIX.
ftp>
```

- (3) Configure the binary mode through the "`bin`" command and, optionally, HASH marking through the "`hash`" command.

```
ftp> bin
200 TYPE is set to IMAGE.
ftp> hash Hash mark printing on (1024 bytes/hash mark).
ftp>
```

- (4) Transfer the image using `put <cit-model-profile-version.img>`.

```
ftp> put cit-xxxx-11.01.02.img
local: cit-xxxx-11.01.02.img remote: cit-xxxx-11.01.02.img
200 PORT is set to IP ADDR = 192.168.1.50 PORT = 55878
150 Data connection open, checked file transfer in process...
#####
226 STOR completed, 8500566 bytes processed, data connection is closed.
8500566 bytes sent in 3.67 secs (2261.1 kB/s)
ftp>
```

- (5) Once the transfer is finished, execute the `quote site savebuffer recording` command.

```
ftp> quote site savebuffer
200 SAVEBUFFER completed O.K.
ftp>
```

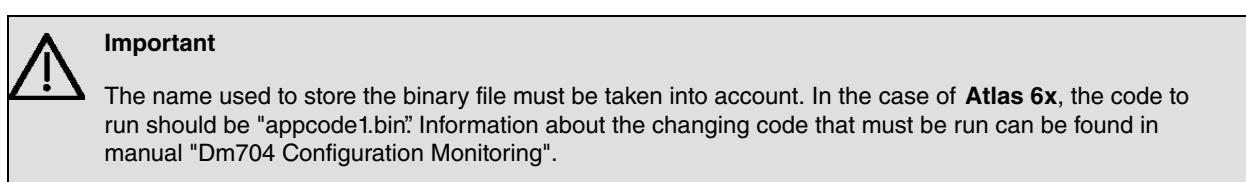
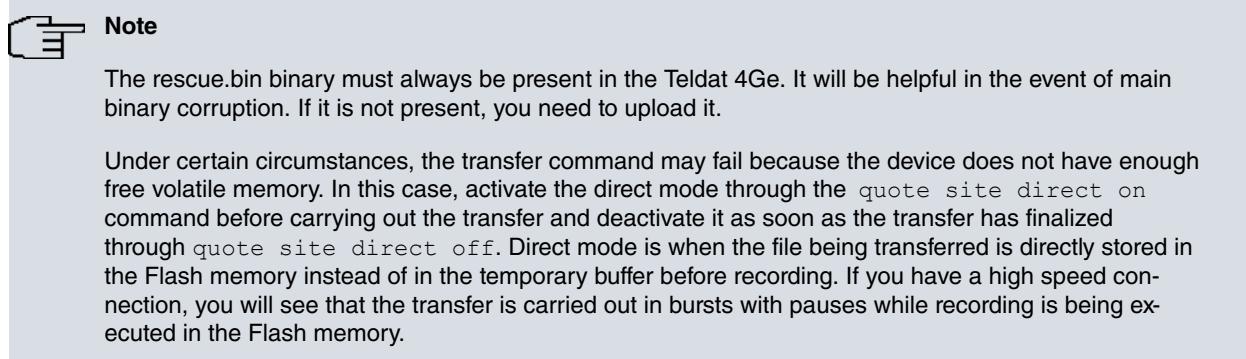
- (6) Finally, and optionally, there is a command that lets you check whether the device has all the necessary files and the element versions are consistent.

```
ftp> quote site coherence
211-COHERENCE results
CIT      v10.8.34.5.3 ID 0x00000000 HDW LVL 13
BOOT     v07 HDW LVL 4
211 COHERENCE results end
ftp>
```

- (7) Restart the device through the `quote site reload on` command; if you are exiting from FTP as usual, the device restarts after some 30 seconds. If you are exiting FTP using **CTRL+C**, the device restarts immediately. You can also restart the device using the `load immediate` console command.

```
ftp> quote site reload on
200 RELOAD mode is set to ON.
ftp> quit
221 Goodbye.
>

load immediate
Are you sure to reload the device(Yes/No)? yes
```



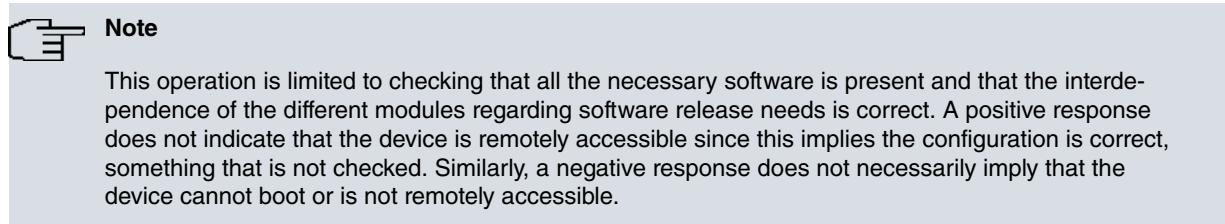
1.3 FTP Features

1.3.1 INTEGRITY Test

There is a device system that allows you to verify that the main file system contents remain consistent. The command used to check whether the device is capable of booting with the available software is as follows:

- **SITE COHERENCE**

This command returns the complete software check as a response. The response begins with a numerical figure (see the RFC). If the figure begins with a "2" this means that the checking is correct. If not, the device can indicate the problem, in order to correct it, in the response.



- **SITE GETAPPNAME**

This returns the application file name used to boot the device. This tells you which file is used in cases where there are various files with a BIN extension.

- **SITE GETBIOSVER**

Returns the device BIOS version number.

- **SITE GETCFGNAME**

Returns the configuration file name used to boot the device. This tells you which file is used in cases where there are various files with a CFG extension.

- **SITE GETFILEVER**

This requires a parameter that is a file name. This returns the file version number in cases where it has the Teldat application format. This allows the clients that support this to know what the application release is.

- **SITE GETHDWLVL**

Returns the device hardware version number. This consists of two numbers, one corresponding to the BIOS and the other to the applications.

- **SITE LISTFIRMWARES**

Returns the firmware file list the device needs for certain devices to operate. Allows clients who support this to know the necessary firmware modules for proper device operation.

- **SITE SYSTID**

Returns the system identifier. This identifier indicates the type of device you are dealing with. Allows clients who can support this to know what software has to be sent.

1.3.2 CHECK Mode

Through this command, the device can execute a series of automatic checks and actions aimed at managing the received files and enabling them to be detected more easily as known files. Files detected as known have either a .BIN, .BFW or .IMG extension. There are various actions that can be controlled through this command. The checks on the files detected as known are only executed when the TEST mode is deactivated.

- **SITE CHECK ALL OFF | ON**

Activates or deactivates all checks and actions.

- **SITE CHECK BIOS OFF | ON**

Activates or deactivates the rejection of applications that need a minimum BIOS version beyond the one currently in the system.

- **SITE CHECK CRC OFF | ON**

Activates or deactivates software integrity checking (CRC). WARNING: in DIRECT ON mode (please see notes under subsections *Distributing with BIOS, C.I.T and FWs files* on page 1 and *Distributing with the C.I.T Image file (IMG)* on page 3) if the CRC file is erroneous, the wrong version will have already replaced the old version and deleted it.

- **SITE CHECK DELETE OFF | ON**

Activates or deactivates the automatic deletion of the temporary buffer content once the SITE SAVEBUFFER has finished executing correctly (when this is configured to accept connections from only one client simultaneously). This operation affects every file, not only the ones detected as known.

- **SITE CHECK FIRMWARE OFF | ON**

Activates or deactivates the verification of the firmware received (in terms of necessity and compatibility) for applications and the current operating environment.

- **SITE CHECK HARDWARE OFF | ON**

Activates or deactivates the rejection of applications whose imprinted hardware version or “hardware level” is prior to the one marked in the device. When this is activated, it ensures that the software received is capable of supporting or correcting known hardware problems in the device. ATTENTION: if this is deactivated, the device can malfunction after restart and start up.

- **SITE CHECK LENGTH OFF | ON**

Activates or deactivates the software integrity check (Length). ATTENTION: in DIRECT ON mode (please see notes of the subsections *Distributing with BIOS, C.I.T and FWs files* on page 1 and *Distributing with the C.I.T Image file (IMG)* on page 3), if the file is erroneous (different from a multiple of 128), the wrong version will have already replaced the old version and deleted it.

- **SITE CHECK PATH OFF | ON**

Activates or deactivates the automatic sending of all acknowledged files received, such as BIOS to the “BIO” system when the system is in DIRECT OFF mode (please see notes of the subsections *Distributing with BIOS, C.I.T and FWs files* on page 1 and *Distributing with the C.I.T Image file (IMG)* on page 3) and the SITE SAVEBUFFER command is executed (instead of sending them to the active system).

- **SITE CHECK PROFILE OFF | ON**

Activates or deactivates the dropping of files when their profile extension is different from the file currently active in the device.

- **SITE CHECK RENAME OFF | ON**

Activates or deactivates the automatic renaming of the file received. When this is active, it uses the name imprinted on the inside of the file instead of using the name received in the STOR command.

- **SITE CHECK SYSTEM OFF | ON**

Activates or deactivates the automatic selection of the files system that is active by default. This command has no real effect, since the operation executes once the connection with the client is established and cannot be modified during the session. This is implemented as a mirror of the command belonging to the effective configuration. In cases where the file system is not configured despite being active by default, when the connection with the client is established, the first system activates depending on device availability. The level of priority, from higher to lower, is as follows:

DSK FDA SMC FCO BIO MEM TST TS1 NUL

- **SITE CHECK UNKNOWN OFF | ON**

Activates or deactivates the rejection of files detected as unknown. These files have a .BIN, .BFW or .IMG extension but do not have the software format recognized by the device. When this rejection is active, these files are not accepted and an error is given when they are received.

- **SITE CHECK VERSION OFF | ON**

Activates or deactivates the rejection of files whose version is prior to the one that is currently active in the device.

The STAT command allows you to view the checking status. Each active check appears with the initial letter and each inactive one is represented with a hyphen. In cases where all or none of them are active, ALL or NONE appears respectively.

1.4 Known Problems

1.4.1 Error writing file (550)

This error message is normally sent by the server to the client when the latter sends a file and the file system does not have enough space to store it or an internal error has occurred.

- If this happens in DIRECT ON mode (please see notes under subsections *Distributing with BIOS, C.I.T and FWs files* on page 1 and *Distributing with the C.I.T Image file (IMG)* on page 3), the file system does not have enough space to store the file. You need to delete files from the file system in order to send the new file.
- If this happens in DIRECT OFF mode (please see notes under subsections *Distributing with BIOS, C.I.T and FWs files* on page 1 and *Distributing with the C.I.T Image file (IMG)* on page 3), the temporary memory buffer is full and is not capable of fully storing the file. In order to find out what is happening, you need to execute the following command.

SITE STATBUFFER

The information received is interpreted in the following way:

- MAX

If the figure is less than the total file length, this indicates that the temporary buffer is not capable of storing the file and you will need to configure the temporary buffer size in order to store it using the "TEMP-BUFF" console command. You could also try downloading again in DIRECT ON mode (please see notes under subsections *Distributing with BIOS, C.I.T and FWs files* on page 1 and *Distributing with the C.I.T Image file (IMG)* on page 3).

- REQ

If the figure is less than the total file length, this indicates that the temporary buffer cannot get more memory from the system and in turn this implies that the device does not have sufficient memory to execute secure downloads. In this case, you need to deactivate the DIRECT ON mode (please see notes under subsections *Distributing with BIOS, C.I.T and FWs files* on page 1 and *Distributing with the C.I.T Image file (IMG)* on page 3) and try to resend the file.

1.4.2 Connection closed by remote host

This error is produced by the Windows FTP client. This indicates that the connection has been closed by the server; however this is not the case. The real reason is the connection has been closed by the client himself. This error usually occurs under the following circumstances.

- The Server is executing a SITE SAVEBUFFER command. In this case, the device continues executing the operation normally even though the connection has been cut off. This occurs because the command's execution time can be quite long and the client assumes that the server has lost the connection as the latter takes so long in replying.

```
226 STOR completed, 9414766 bytes processed, data connection is closed.
ftp: 9414766 bytes sent in 5.85Seconds 1609.64Kbytes/sec.
ftp> quote site savebuffer
Connection closed by remote host.
ftp>
```

In [FTP clients](#) on page 10, we have provided details on some FTP clients that can be used to transfer files to or from the router as an alternative. We have also explained how to update the software by using each of them.

- The problem occurs in the middle of transmitting a file. In this case, the problem could involve traffic control systems that hinder transmission if one of the TCP ports involved in the transfer is not port 20. In this case, the client needs to send the PORT command to the server (since the device tries to ensure one of the ports is port 20).

1.4.3 File transfer has stopped

Occasionally, with some files a problem occurs that stops the file from being sent. This does not happen with all files. However, when it does happen with one, it always happens. This problem occurs when the Windows FTP client sends TCP packets with an erroneous checksum. We don't know why this behavior occurs with some specific files, but the issue can be simply solved by using a different FTP client.

1.4.4 Unable to open file (550)

This is an error response normally sent by the server to the client when a file is sent indicating the file cannot be opened in the server. There are clients that only send the file name to the remote server and others who send both the name and the local path. This message appears when the server is in DIRECT ON mode (please see notes under subsections 2.1 and 2.2) and the client includes the local path in the file name being sent.

Example with a Linux client:

```
ftp> put ../../_85xx/cit.bin
local: ../../_85xx/cit.bin remote: ../../_85xx/cit.bin
200 PORT is set to IP ADDR = 172.24.75.193 PORT 50021
150 Data connection open, checked file transfer in process...
#####
netout: Connection reset by remote peer
550 Unable to open file.
```

In this case, the storage system where the server is operating in DIRECT ON mode is "/DSK". When sending the file name as "../../_85xx/cit.bin", the device tries to open the file in "/_85xx/cit.bin". As the "/_85xx" system doesn't exist, the file cannot be opened. The storage systems available request the address from the root system.

To solve this issue, you can use specific client commands to manage the file name in remote systems (each client has their own management options), or you can specify the name the remote system must use as shown below (example with Linux client):

```
ftp> put ../../_85xx/cit.bin cit.bin
local: ../../_85xx/cit.bin remote: cit.bin
200 PORT is set to IP ADDR = 172.24.75.193 PORT 50021
150 Data connection open, checked file transfer in process...
#####
226 STOR completed, 7214720 bytes processed, data connection is closed.
7214720 bytes sent in 41.73 secs (169.1 kB/s)
```

1.4.5 Unix Clients (ASCII mode)

Warning: FTP clients from the World of Unix, Linux and similar operating systems use the ASCII mode by default to send files. Binary files that the devices need must be sent in BINARY mode, therefore this must be activated in the client with the corresponding command (usually binary). Even though this is not necessary in Window environments; it's a good idea to always activate it.

In cases where the binary mode is not activated to transfer files to the device, the following problems may arise:

- DIRECT ON Mode (please see notes under subsections [Distributing with BIOS, C.I.T and FWs files](#) on page 1 and [Distributing with the C.I.T Image file \(IMG\)](#) on page 3):
 - CHECK LENGTH | CRC ON (COMPATIBLE ON) mode: If this is a binary file acknowledged as application or firmware, this is considered incorrect and a length error or a CRC error occurs. At this point, the file that has been sent and saved is incorrect and it's possible the device WON'T START UP.

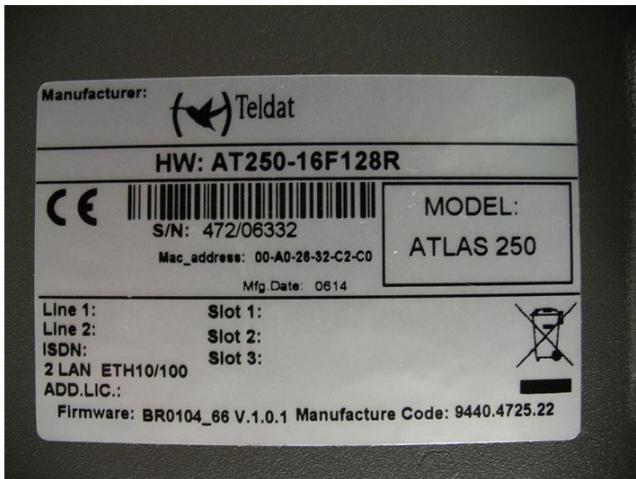
- CHECK LENGTH | CRC OFF (COMPATIBLE OFF) mode: In this case, an error does not occur, meaning the problem is underlying. At this point, the file that has been sent and saved is incorrect and it's possible the device WON'T START UP.
- DIRECT OFF Mode (please see notes under subsections *Distributing with BIOS, C.I.T and FWs files* on page 1 and *Distributing with the C.I.T Image file (IMG)* on page 3):
 - CHECK LENGTH | CRC ON (COMPATIBLE ON) Mode: If this is a binary file acknowledged as application or firmware, this is considered incorrect and a length error or a CRC error occurs. The file is located in the system/ MEM and nothing happens until the "SITE SAVEBUFFER" command has been sent. At this point, a corrupt file is saved and it's possible the device WON'T START UP.
 - CHECK LENGTH | CRC OFF (COMPATIBLE OFF) Mode: If this is a binary file acknowledged as application or firmware, this is considered incorrect and a length error or a CRC error occurs. The file is located in the system/ MEM and nothing happens until the "SITE SAVEBUFFER" command has been sent. At this point, a corrupt file is saved and it is possible the device WON'T START UP.

1.5 Information required for updating

1.5.1 How to determine the appropriate distribution and the appropriate binary

To update a device, you need to know its identifier and current license. This information can be obtained by:

- Checking the label found on the underside of the device (this is only valid to determine the device identifier, not the current license).



- In console (local or Telnet) through the monitoring command `configuration` (in this case TC-4F32R-W2AI L1.87).

```
*monitor
+configuration Teldat's Router, C6 SNA IPSec CR 1 87 S/N: 427/00127
P.C.B.=48 Mask=0502 Microcode=0000 CLK=49152 KHz BUSCLK=49152 KHz
ID: TC-4F32R-W2AI L1.87

Boot ROM release:
BIOS CODE VERSION: 01.09.01    Feb 1 2005 13:25:25
gzip Feb 1 2005 12:42:37
io1 Feb 1 2005 13:24:56
io2 Feb 1 2005 12:41:45
io3 Feb 1 2005 13:24:56
START FROM FLASH L1
Watchdog timer Enabled

Software release: 10.5.4-Alfa TM Feb 11 2005 13:12:12
Compiled by sfont on SFONT
Hostname:          Active user:
Date: Friday, 02/11/05   Time: 16:33:20
Router uptime: 4s
Num     Name      Protocol
0       IP        DOD-IP
3       ARP       Address Resolution Protocol
```

```

6      DHCP      Dynamic Host Configuration Protocol
11 SNMP SNMP 13 RIP Route Information Protocol

10 interfaces:
Conn   Interface   MAC/Data-Link       Hardware          Status
LAN1   ethernet0/0 Ethernet/IEEE 802.3 Quicc Ethernet    Up
WAN1   serial0/0   ASTM system        Async Line       Testing
DSL1   atm0/0      ATM               ATM SAR Device  Down
ISDN1  bri0/0     BRI               Net ISDN Basic Rate Int Up
      x25-node     internal          Router->Node    Up

SNMP OperStatus:
Interface      OperStatus
ethernet0/0     Up
serial0/0      Down
atm0/0         Down
bri0/0         Up
x25-node       Up
+

```

- Via FTP, using the `quote site systid` command.

```

ftp> quote site systid
211 TC-4F32R-WAI L1.2
ftp>

```

To identify the distribution corresponding to the device, simply check the initial part of the identifier:

- TC: Teldat M distribution (the Teldat C software is contained in the Teldat Modular).
- TM: Teldat M distribution
- AT: ATLAS distribution
- AT2G: ATLAS 2G distribution
- ...

To determine how much available Flash there is, check the number preceding the letter F (for Flash). To determine how much SDRAM is available, check the number preceding the letter R (for RAM). Both quantities are expressed in Megabytes.

To identify what application binary should be downloaded in your device, check the “version_map.txt” file included in the distribution and find the first condition it fulfills.

For example, if there are several devices where the corresponding distribution is Teldat M, the “version_map.txt” file included is as follows:

```

L1.5, 4F, 16R, *, teldatc_corp_mr.bin, TELDAT C4 (MR)
L1.6, 4F, 16R, *, teldatc_corp_mr.bin, TELDAT C4 SNA (MR)
L1.10, 4F, 16R, *, teldatc_corp_mr.bin, TELDAT C4 IPSEC (MR)
L1.11, 4F, 16R, *, teldatc_corp_mr.bin, TELDAT C4 SNA IPSEC (MR)
L1.13, 4F, 16R, *, teldatc_corp_mr.bin, TELDAT C4i (MR)
L1.14, 4F, 16R, *, teldatc_corp_mr.bin, TELDAT C4i SNA (MR)
L1.16, 4F, 16R, *, teldatc_corp_mr.bin, TELDAT C4i IPSEC (MR)
L1.17, 4F, 16R, *, teldatc_corp_mr.bin, TELDAT C4i SNA IPSEC (MR)
L1.21, 4F, 16R, *, teldatc_corp_mr.bin, TELDAT C4B (MR)
L1.22, 4F, 16R, *, teldatc_corp_mr.bin, TELDAT C4B SNA (MR)
L1.26, 4F, 16R, *, teldatc_corp_mr.bin, TELDAT C4B IPSEC (MR)
L1.27, 4F, 16R, *, teldatc_corp_mr.bin, TELDAT C4B SNA IPSEC (MR)
L1.12, 4F, 16R, *, teldatc_pai_mr.bin, TELDAT C2i (MR)
L1.15, 4F, 16R, *, teldatc_pai_mr.bin, TELDAT C2i IPSEC (MR)
L1.33, 4F, 16R, *, teldatc_pai_mr.bin, TELDAT C3i IPSEC (MR)
L1.1, 2F, 16R, *, teldatc_pa_mr.bin, TELDAT C2 (MR)
L1.2, 2F, 16R, *, teldatc_pa_mr.bin, TELDAT CSW (MR)
L1.7, 2F, 16R, *, teldatc_pa_mr.bin, TELDAT C2 IPSEC (MR)
L1.8, 2F, 16R, *, teldatc_pa_mr.bin, TELDAT C3 IPSEC (MR)
L1.29, 2F, 16R, *, teldatc_pa_mr.bin, TELDAT C3G IPSEC (MR)
L1.30, 2F, 16R, *, teldatc_pa_mr.bin, TELDAT C2 (no TMS) (MR)
L1.42, 2F, 16R, *, teldatc_pa_mr.bin, TELDAT C2UP (MR)
L1.43, 2F, 16R, *, teldatc_pa_mr.bin, TELDAT C2UP IPSEC (MR)

```

```
L1.18, 2F, 16R, *, teldatc_pi_mr.bin, TELDAT C2B (MR)
L1.19, 2F, 16R, *, teldatc_pi_mr.bin, TELDAT C2BM (MR)
L1.23, 2F, 16R, *, teldatc_pi_mr.bin, TELDAT C2B IPSEC (MR)
L1.24, 2F, 16R, *, teldatc_pi_mr.bin, TELDAT C2BM IPSEC (MR)
L1.35, 2F, 16R, *, teldatc_pi_mr.bin, TELDAT C3B IPSEC (MR)
L1.37, 2F, 16R, *, teldatc_pi_mr.bin, TELDAT MASTER ROUTER (MR)
L1.*,*F,*R,*, teldatm_standard.bin, TELDAT C
L4.*,*F,*R,*, teldatm_standard.bin, TELDAT S
L5.*,*F,*R,*, teldatm_standard.bin, TELDAT G
L8.*,*F,*R,*, teldatm_standard.bin, TELDAT A
```

- If the device identifier is TC-4F32R-W2AI L1.87, the first (and in this case only) condition that must be met is: “L1.*,*F,*R,**” (L1.87, 4F, 32R, W2AI). Consequently, the binary to be loaded is teldatm_standard.bin.
- If the device identifier is TC-4F16R-WAI L1.27, the first condition that must be met is: “L1.27, 4F, 16R, **” (L1.27, 4F, 16R, WAI). Consequently, the binary to be loaded is teldatc_corp_mr.bin.
- If the device identifier is TC-4F32R-WAI L1.27, the first condition that must be met is: “L1.*,*F,*R,**” (L1.27, 4F, 32R, WAI). Consequently, the binary to be loaded is teldatm_standard.bin.

1.5.2 How to determine the necessary firmware

To determine the firmware a device needs, you have two options:

- The FTP server `quote site listfirmwares` command returns a list with the firmware file names included in the distribution that must be sent.

```
ftp> quote site listfirmwares
211 fw000013.bfw
ftp>
```

- The system `firmwares-required` command.

```
*monitor
Console Operator
+system firmwares-required

List of required firmwares for detected hardware
-----
Filename          Description          Version/Subv
-----
fw000013.bfw    Broadcom 63268-TSS VDSL2/ADSL2+ POTS      Not present
```

1.6 FTP clients

As mentioned in previous chapters, there are several commands in FTP that, due to their nature, take quite a long time to execute. Due to this, some FTP clients decide to cut off the connection when they don't receive a response in the established time, believing that there is a problem with the server. The Windows FTP client is among these clients. In the following paragraphs, we have explained how to use and configure specific FTP clients to avoid this problem in processes as critical as software updating. Here the process is explained using the `site savebuffer` command; however, the same method can be applied if we activate the direct mode through the `site direct on` command (please see notes under subsections *Distributing with BIOS, C.I.T and FWs files* on page 1 and *Distributing with the C.I.T Image file (IMG)* on page 3).

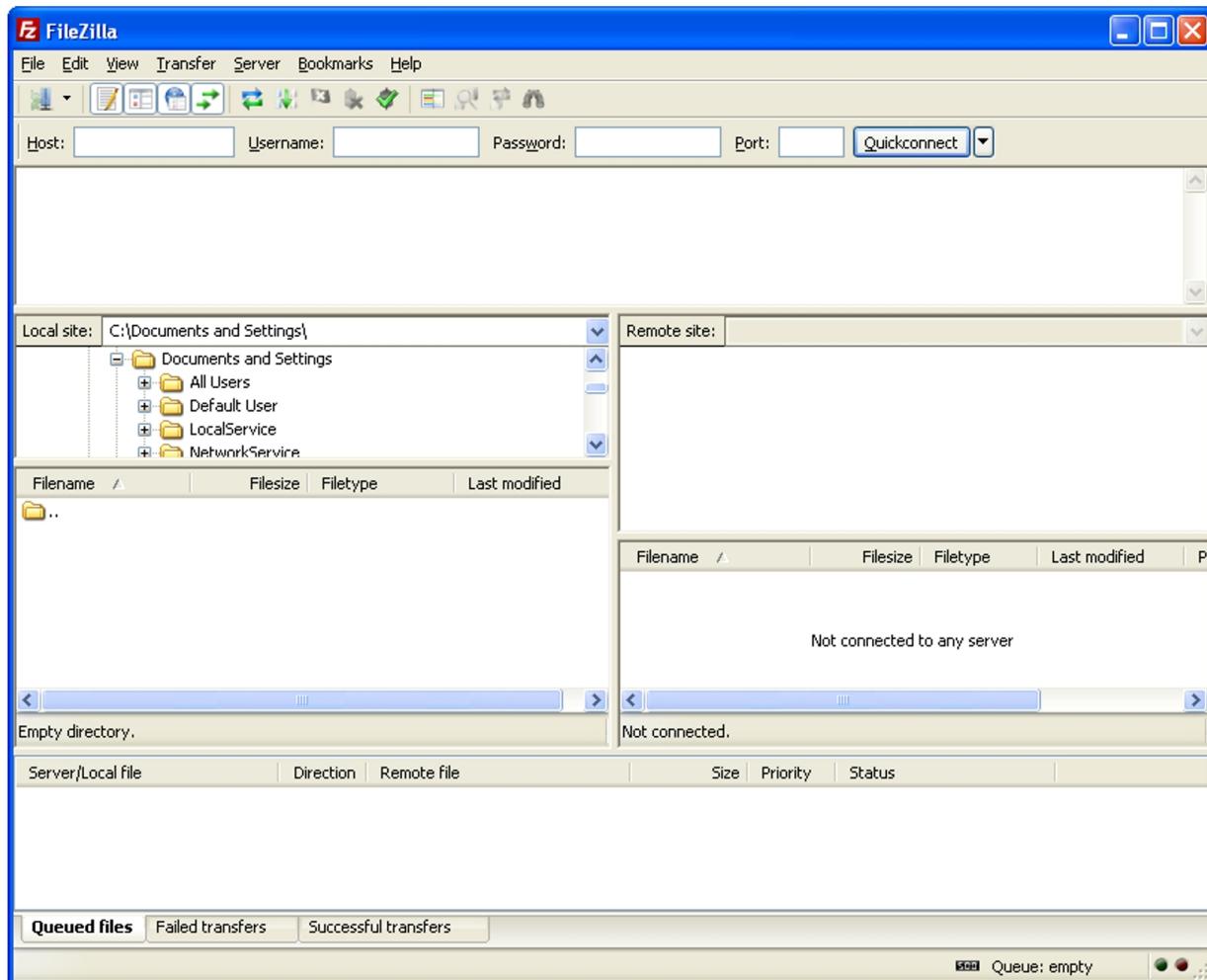
1.6.1 FileZilla Client

FileZilla is an open code multiplatform FTP client with free software, licensed under the GNU General Public License. It supports FTP, SFTP and FTP over SSL/TLS (FTPS) protocols. Its user friendly and intuitive interface shows both the local window and the remote window, thus allowing files to be passed on from one to the other through multiple techniques (including the “drag and drop” mechanism).



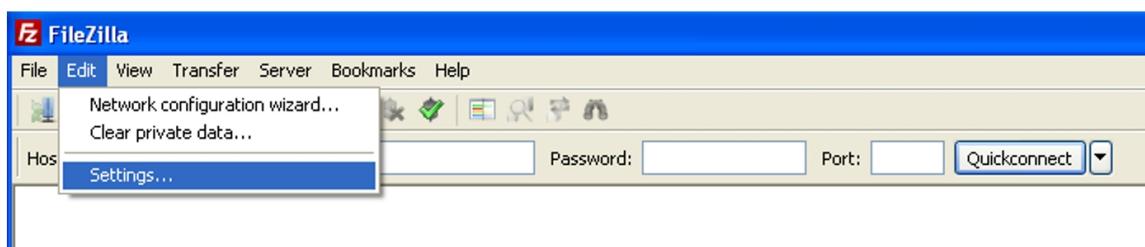
Note

The images shown here are for the Windows version. However, the operating mode is the same for both the Windows and Linux operating systems.

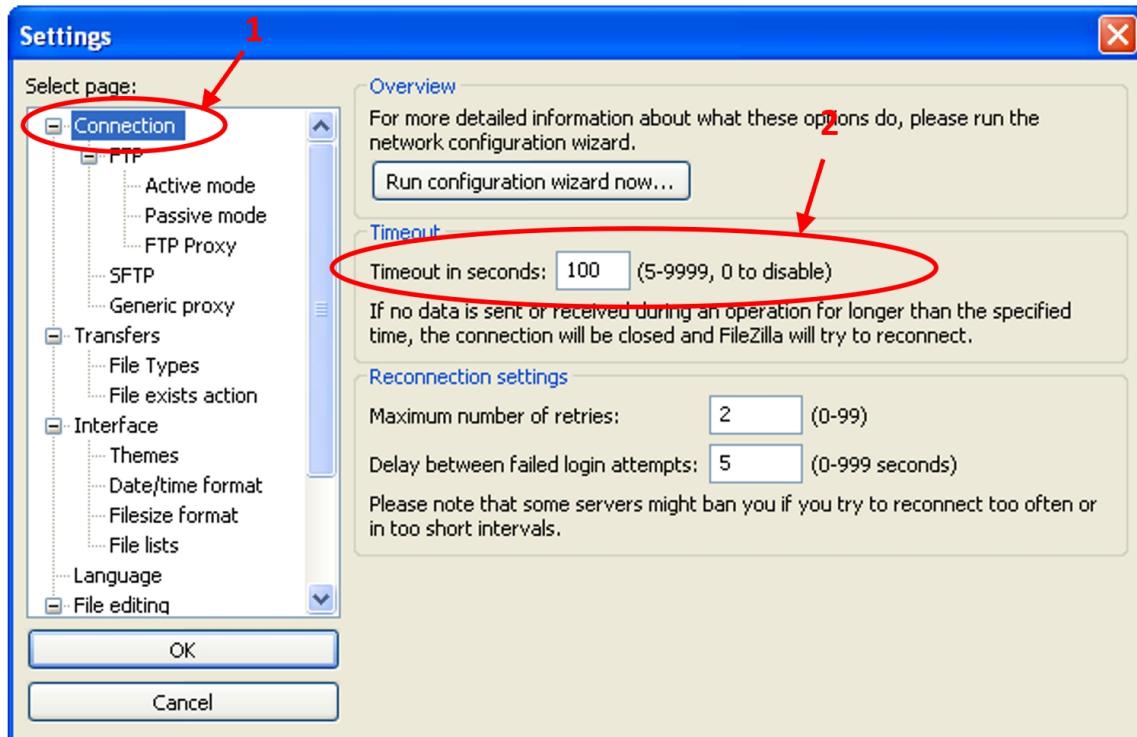


Before beginning the updating process, we need to increase the response wait time to prevent the connection being cut off while the `site savebuffer` command is being executed. To do this, you need to carry out the following:

- (1) In the **Edit** menu, select the **Settings...** option.



- (2) Using the mouse, click on the **Connection** option and modify the **Timeout in seconds** parameter, assigning it a value of at least *100 seconds*.



- (3) Click on the **OK** button.

Once this change has been made, you need to update the software by carrying out the steps given below:



Note

You should always use the FTP protocol.

- (1) Connecting to the router's FTP server

To do this, use the **Quickconnect** bar. Here, you must specify the router's IP address in the **Host** field, the user in the **Username** field (using user root when there are no users defined in the router) and the password, if necessary, in the **Password** field (user root does not have a password). The **Port** field can be left empty, unless a specific port, other than 21, has been configured in the router's FTP server.

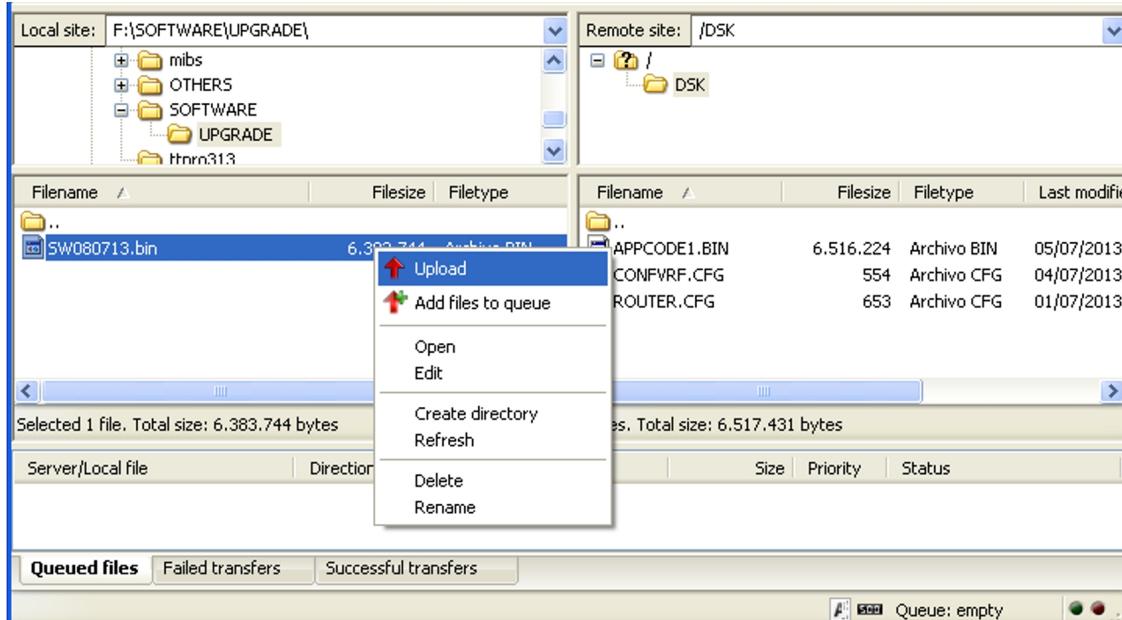
Subsequently, click on the **Quickconnect** button.

Host:	192.168.1.1	Username:	USER	Password:	*****	Port:		Quickconnect
-------	-------------	-----------	------	-----------	-------	-------	--	--------------

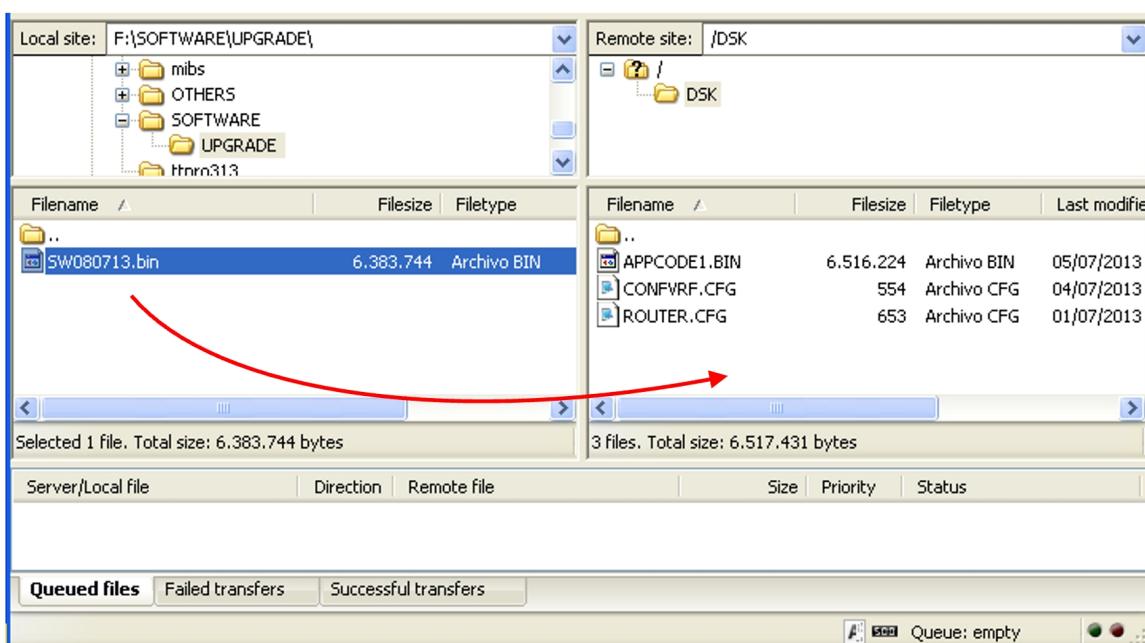
- (2) Transferring the file

There are various alternatives to do this:

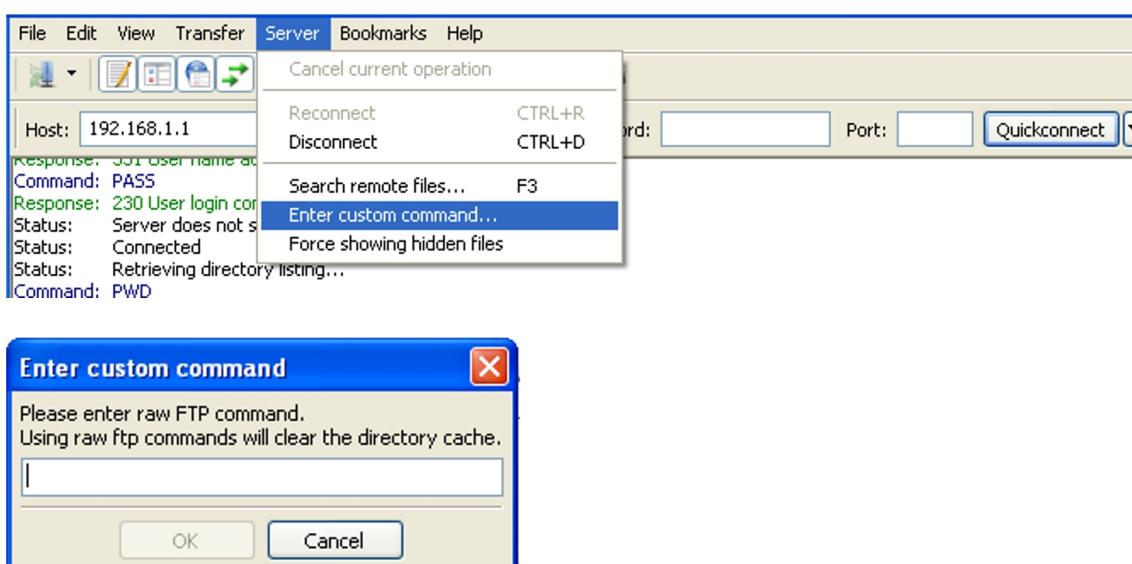
- Simply by clicking on the file with the right-hand mouse button and selecting the "Upload" option.



- By double clicking on the file.
- Or, through the “drag and drop” mechanism.



- (3) Execute the recording command of the file in the disk and close the FTP connection
 To do this, and for each FTP command going to be executed, select the **Enter custom command...** from the **Server** menu and enter the command to be executed in the new window. Once entered, click on the **OK** button or press the **Enter** key on the keyboard.



The following commands need to be executed in the indicated order:

- site savebuffer
- site reload on (optional command)
- quit



Note

While executing the `site savebuffer` command, you may receive a response indicating that you are disconnected from the server. In this case, do not perform any action since, after a while, you will receive an OK message associated with this command:

```
Command: LIST
Response: 150 Data connection open, list transfer in process...
Response: 226 List transfer completed, data connection is closed.
Status: Directory listing successful
Command: site savebuffer
Status: Disconnected from server
Response: 200 SAVEBUFFER completed O.K.
```

1.6.2 WinSCP Client

WinSCP is a Windows FTP client with free software that supports FTP, SFTP and SCP protocols. This application allows you to choose between two types of interfaces. In this section, we will be using the **Commander Interface**.

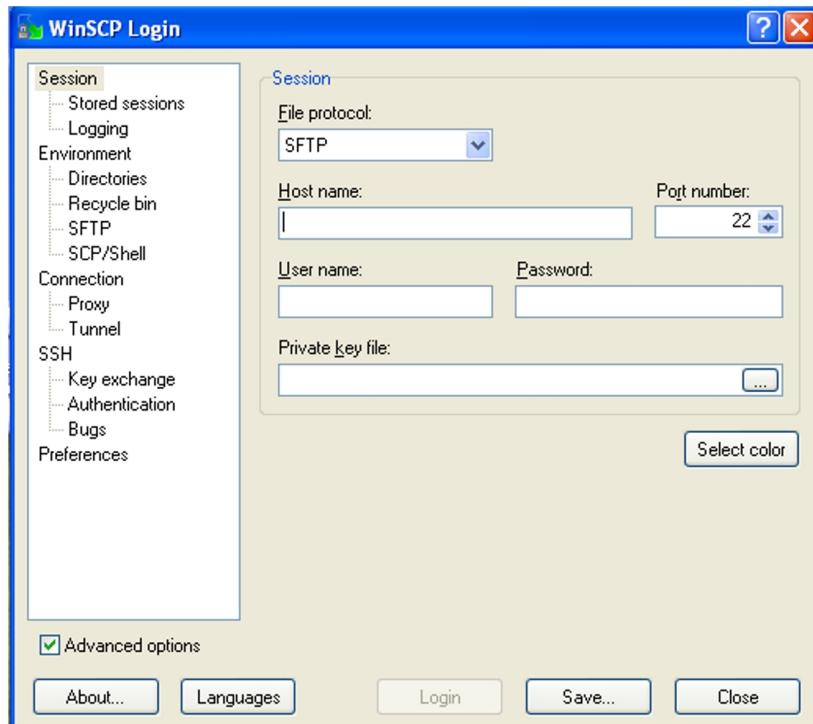


Fig. 2: WinSCP Login window

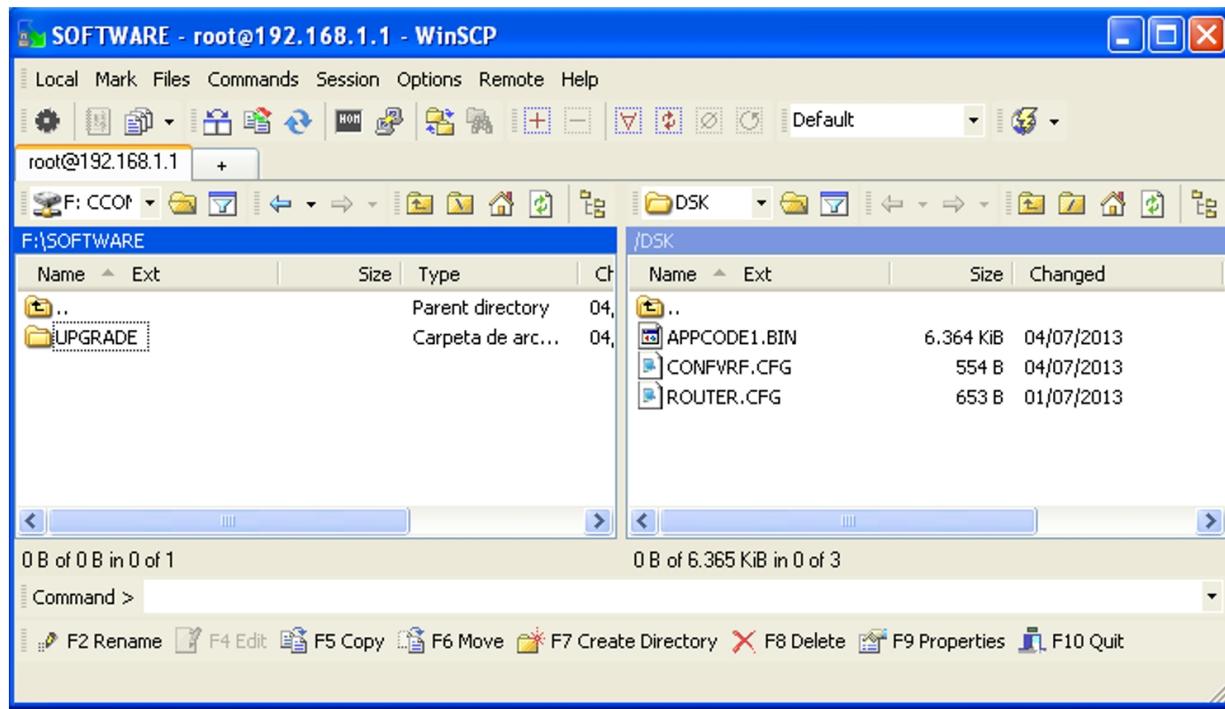


Fig. 3: The WinSCP Commander Interface

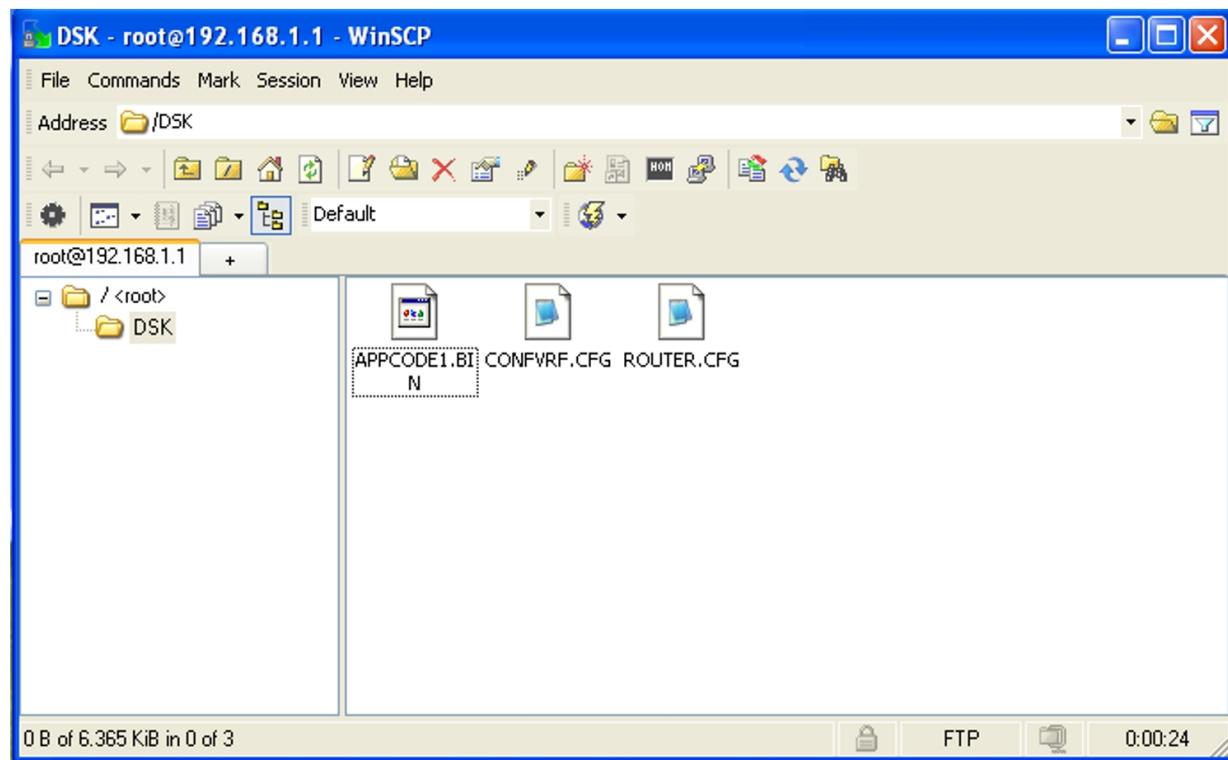
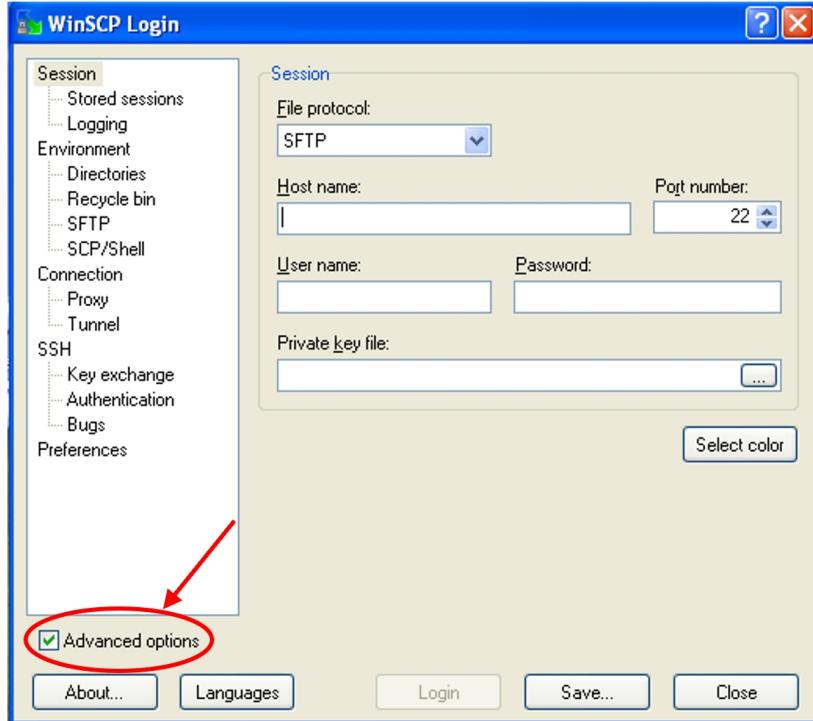


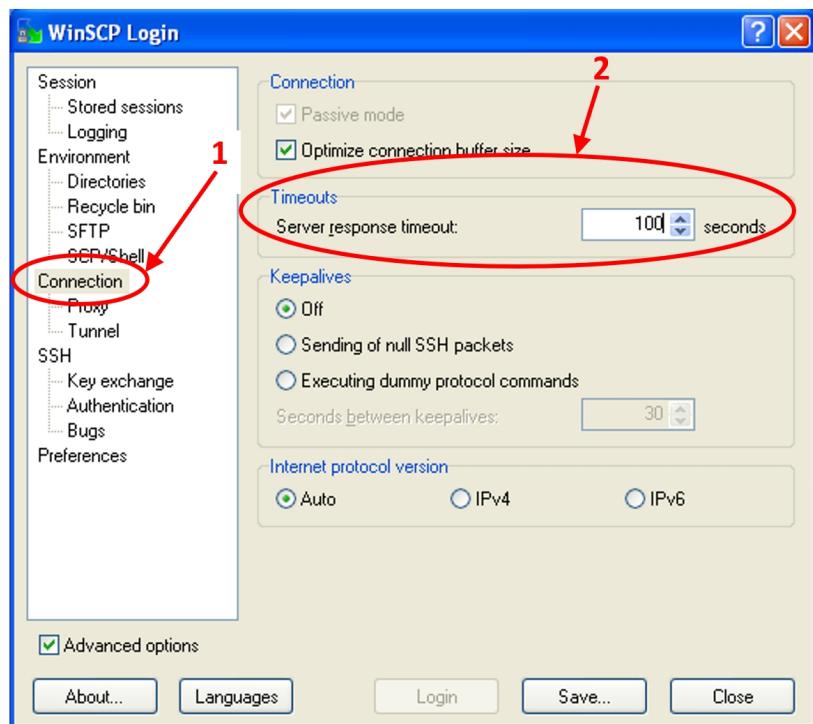
Fig. 4: The alternative Explorer Interface

Before the updating process begins, you need to increase the response wait time to prevent the connection being cut off while the `site savebuffer` command is being executed. To do this, you need to carry out the following:

- (1) Activate the **Advanced options** checkbox if it isn't already activated.



- (2) Using the mouse, click on the **Connection** option and modify the **Server response timeout** parameter, assigning it a value of at least 100 seconds.



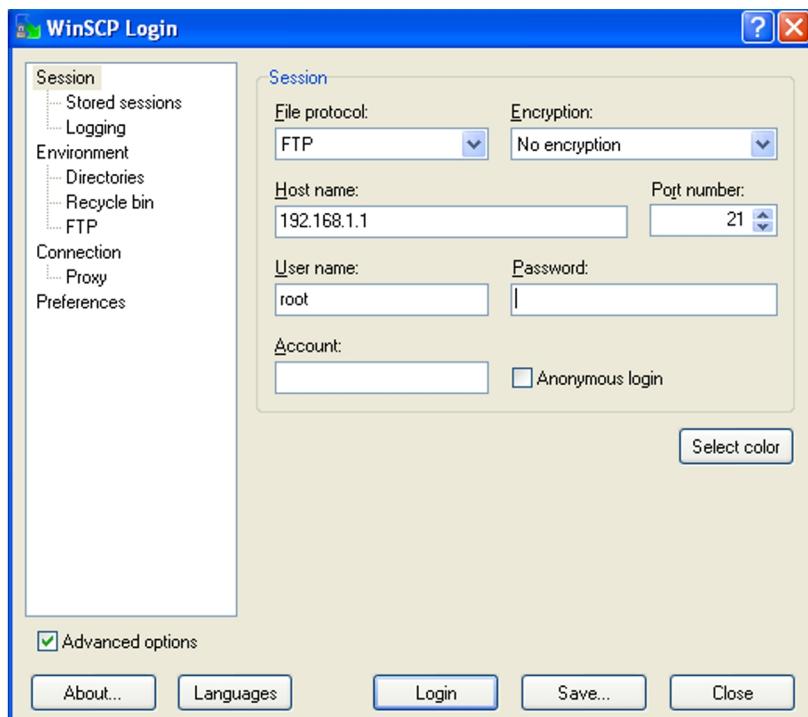
Once this change has been made, you can now update the software by carrying out the steps given below:

Note

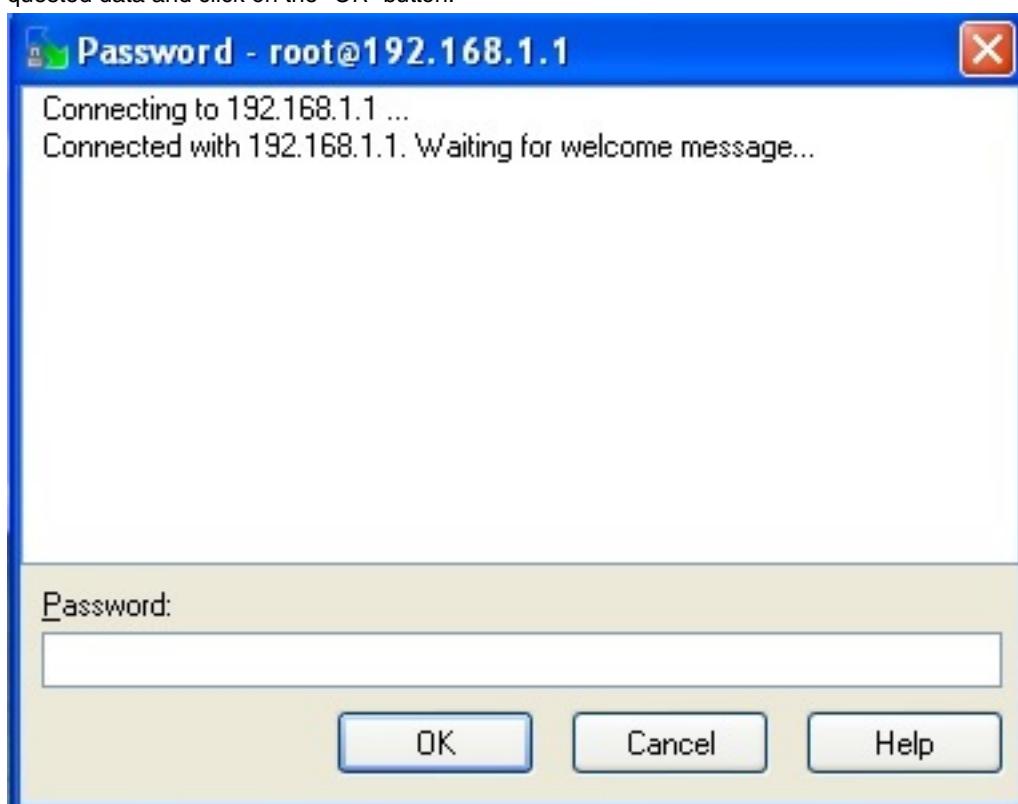
You should always use the **FTP** protocol.

- (1) Connecting to the router's **FTP** server

To do this, select **FTP** in the **File protocol** field and enter the router's IP address in the **Host name** field. The **User name** and **Password** fields need to be filled out with the username and the access password. In cases where the router does not have any defined users, specify `root` as the user without a password. The **Port** field should only be modified if a specific port, other than 21, has been configured in the router's **FTP** server.

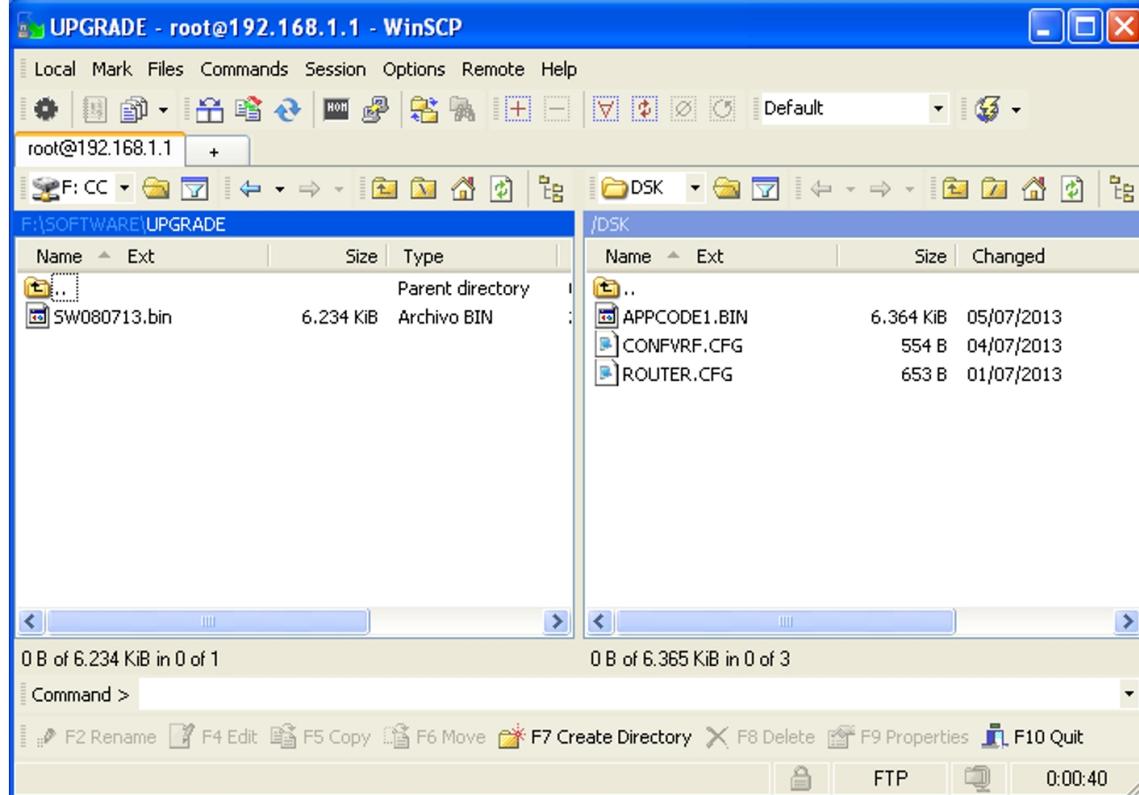


During the connection, you may be asked for the access credentials again. If this happens, reenter the requested data and click on the "OK" button.

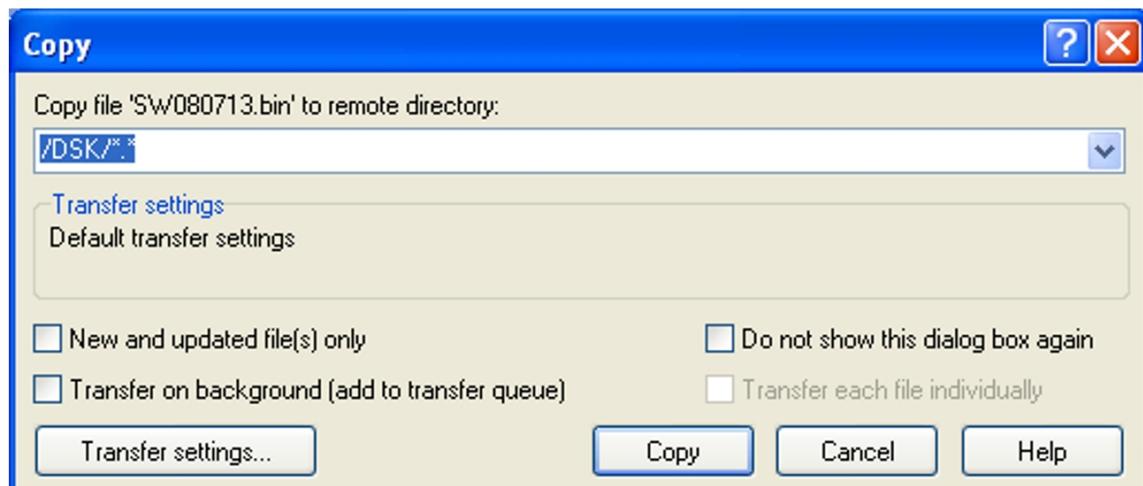


(2) Transferring the required file

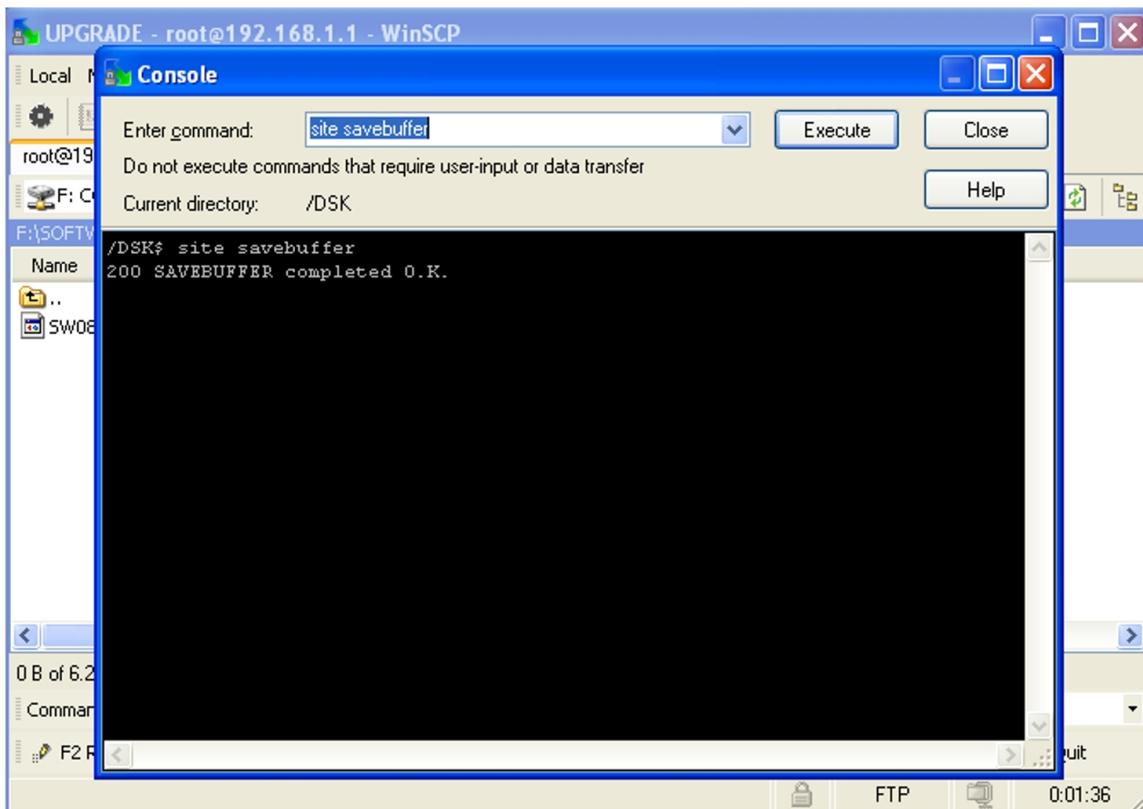
Once the connection has been established, the application will display the following window where two panels can be seen; the right panel shows your local device and the left one the router panel.



To transfer a file, use the drag and drop mechanism. On releasing the mouse, the following dialog box appears. Just click on the **Copy** button to complete the operation;



- (3) Execute the file recording command in the disk and close the FTP connection
To do this, select the **Open Terminal** from the **Commands** menu that then opens a new window:



Here, on the upper part of the window, enter and execute the necessary commands one by one. To execute a command, simply click on the **Execute** button or press the **Enter** key on your keyboard. At the bottom of the window, the application will display the results of each command. The following commands need to be executed in the indicated order:

- site savebuffer
- site reload on (optional command)
- quit

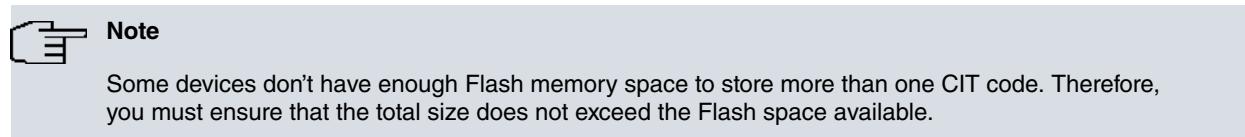
1.6.3 FTP client through Linux console

Another alternative to update the software is by using the FTP client through the Linux console. You simply need to follow the same steps as indicated in the corresponding subsection of *Updating Process* on page 1 based on the type of software you wish to update.

Chapter 2 Appendix A. Backup Systems

2.1 Distributing with BIOS, CIT and FWs files

These devices are equipped with two backup systems that allow the device to boot when it detects problems.



2.1.1 Two CIT codes loaded in the Flash disk

On start up, the BIOS searches for the application set as active. If it doesn't find it (searching by name) or the CRC is incorrect, it searches for the next application file (*.bin) available in the disk. If no problem is identified, the BIOS starts up this second application.

```
Current production date: 13 35
Current software license: 34 26
S/N: 819/02723
BIOS MAC Add: 00-a0-26-ae-3d-7a
>>

*****
TRYING APP DUMP
  (CONFIGURED) NEWCODE.BIN ver.: 0.10.9.12 0.0.0.0
  *** ERROR ***
CRC error.
  (BY SEARCHING APP FILES ON FLASH)
  TRYING: NEWCODE.BIN ver.: 0.10.9.12 0.0.0.0
  *** ERROR ***
CRC error.
  TRYING: APPCODE1.BIN ver.: 0.10.9.8 10.8.0.0
APP CODE DUMP.....
*****
*****
*****
APP DATA DUMP.....
Running application at: 0x00200140
Default configuration used
Parsing text mode configuration ...
Configuration parsed
Initializing

Press any key to get started
```

For this to happen, both files need to be stored with different names. By default, the device ignores the name of the file and uses a specific name to record it. As a result, the device always replaces the previous file with the same name.

The steps to execute are:

- (1) Connect to the device's FTP server.
- (2) Transfer and store the first CIT. code if you want to update or replace the existing file:
 - (1) Configure the binary mode through the `bin` command.
 - (2) Transfer the application through the `put <application.bin>` command.
 - (3) Once the transfer has completed, execute the `quote site savebuffer recording` command.

```

ftp> quote site savebuffer
200 SAVEBUFFER completed O.K.
ftp> ls
200 PORT is set to IP ADDR = 192.168.212.23  PORT = 39332
150 Data connection open, list transfer in process...
-rwxrwxrwx  1 ftp      ftp      7945344 Mar 27 2015 APPCODE1.BIN
226 List transfer completed, data connection is closed.
ftp> █

```

- (3) Transfer and store the second CIT code with a different name:

- (1) Execute the `quote site check rename off` command.

```

ftp> quote site check rename off
200 CHECK RENAME control is set to OFF.

```

- (2) Configure the binary mode through the `bin` command.

- (3) Transfer the application through the `put <application.bin> <remote_name>` command, where `<remote_name>` is the name that you want to assign to the file.

```

ftp> put teldatm1.bin newcode.bin

```

- (4) Once the transfer has completed, execute the `quote site savebuffer` recording command.

```

ftp> quote site savebuffer
200 SAVEBUFFER completed O.K.
ftp> ls
200 PORT is set to IP ADDR = 192.168.212.23  PORT = 58831
150 Data connection open, list transfer in process...
-rwxrwxrwx  1 ftp      ftp      8140160 Mar 27 2015 NEWCODE.BIN
-rwxrwxrwx  1 ftp      ftp      7945344 Mar 27 2015 APPCODE1.BIN
226 List transfer completed, data connection is closed.

```

- (4) Finally, indicate which of the two applications is established as active to boot the router. The non-selected application will be used as backup. Two commands are available for this:

- Console

```
Config>set application-active <code-file>
```

- FTP

```
ftp> rename <from-name> <to-name>
```

This command allows you to set the active application by renaming the files. For this to work, you must note that BIOS searches by name on start up. Therefore, you must name the new application that you want to establish as active exactly the same way as the application that is currently active in the device.

2.1.2 Flash Backup System

The Flash backup system allows the last successfully installed distribution to be automatically restored when the device detects problems in some of the software elements (BIOS FLASH, application and firmwares).

This system needs the Flash disk to be divided into two units, known as main and backup. This partitioning means the installation space available is low (half) and should only be activated when necessary. The installation to be carried out can be fitted into the main unit.

2.1.2.1 Flash Disk Formatting

Formatting the Flash disk is destructive. It can only be done from the local console to guarantee that the user has local access to the device and can load it properly..

- (1) Pause device start up in the BIOS by simultaneously pressing the CTRL-T keys when a series of periods appear after two ">" symbols.

```
*****
***** BIOS CODE DUMP.....*****
***** BIOS DATA DUMP....*****
***** End of BIOS dump*****



FLASH BIOS CODE VERSION: 02.07  Mar 12 2014 11:41:18   L0

System Info:
PCB:0x13A GPPORCR:0x00000000 PVR:0x80212151 SVR:0x80F90110
CLKs: CCB=396000 CPU0/1=792000/0 DDR(c1k)=330000 LBUS=99000 PCI0/1=0/0
Watchdog:Enabled
MMU Mode:Dynamic
ICache:ON DCache:ON Write-Back L2Cache:ON

Mem Info:
DRAM size: 128 Megabytes
  BANK 0: 128 Megabytes (detected)
FLASH: 32256 KB.
EEPROM: 16384 Bytes.

Devices:
SWITCH(4) 10/100/1000
GIGABIT ETHERNET 1
USB
NVRAM 128 KB
SECURITY ENGINE(0x0a140100)
PCI device: PowerPC processor, RC
(Bus: 0, Device: 0, Function: 0)
(Vendor: 0x1957, Device: 0x012A)
(Subs. Vendor: 0x0000, Subs. Device: 0x0000)
Slot 1 - PCI device: network controller
(Bus: 1, Device: 0, Function: 0)
(Vendor: 0x168C, Device: 0x0030)
(Subs. Vendor: 0x168C, Subs. Device: 0x3112)
PCI device: PowerPC processor, RC
(Bus: 10, Device: 0, Function: 0)
(Vendor: 0x1957, Device: 0x012A)
(Subs. Vendor: 0x0000, Subs. Device: 0x0000)

Current production date: 13 35
Current software license: 34 26
S/N: 819/02723
BIOS MAC Add: 00-a0-26-ae-3d-7a
>>

***
```

- (2) Access the Flash disk menu:

```

    === INITIAL MENU ===

a) Change Time
b) Change Date
c) Change Code to Run
d) Change Licence
f) Disk menu
g) Set default name for file loaded from console
h) Change BIOS licence
l) Load from lan
sc) show configuration file name
s) Set temporary licence
u) Unset temporary licence
v) Change version control for loading
w) Change default ethernet device
x) Load from console (xmodem)
r) Reset
0) Exit
    >>f

    === DISK MENU ===

a) Change active drive.
c) Copy file.
d) Show files.
e) Erase file.
f) Format disk.
r) Rename archive.
0) Exit
    A:>>f

```

- (3) Format the main partition through the **AH: (Main disc - Half size)** option. Move on to the backup through **B: (BK disc - Half size)**.

```

    === DISK MENU ===

a) Change active drive.
c) Copy file.
d) Show files.
e) Erase file.
f) Format disk.
r) Rename archive.
0) Exit
    A:>>f

This operation can provoke important damages to equipment. Continue?(y/n): y
A: (only one disc - Full size);
AH: (Main disc - Half size);
B: (BK disc - Half size);
S: (Smart Card);
Drive: AH

Are you sure to format drive AH: ?(y/n):y.....
*****Drive formated O.K.

    === DISK MENU ===

a) Change active drive.
c) Copy file.
d) Show files.
e) Erase file.
f) Format disk.
r) Rename archive.
0) Exit
    A:>>f

This operation can provoke important damages to equipment. Continue?(y/n): y
A: (only one disc - Full size);
AH: (Main disc - Half size);
B: (BK disc - Half size);
S: (Smart Card);
Drive: B

Are you sure to format drive B: ?(y/n):y.....
*****Drive formated O.K.

```

After formatting and exiting, the device starts up and a CIT code must be loaded.

2.1.2.2 Operating Flash Backup System

Once the Flash backup system has been enabled, the user must establish the restoration point (i.e., copy the information in the main partition to the backup partition). Two commands are available for this:

- Console

```
Config>backup-files
Backup in progress...
Backup successful.
Config>
```

- FTP

```
ftp> quote site backup
250 Backup successful.
ftp>
```

```
Config>file list
Config Media: Flash only
A: APPCODE1.BIN 7945344 10/12/00 00:00 Flash
Flash Available Space : 6867 Kbytes

B: APPCODE1.BIN 7945344 10/12/00 00:00 Flash Backup
Flash Backup Available Space : 6995 Kbytes

Config>■
```

Once the restoration point has been established, the system does it automatically:

- (1) On start up, the BIOS searches for the application established as active.
- (2) If it doesn't find it (searching by name) or the CRC is incorrect, it searches for the next application file (*.bn) available in the main partition.
- (3) If it doesn't find the next application file or the CRC is incorrect, it makes a copy from the backup partition to the main partition: i.e., it executes a backup restoring.

```
Current production date: 13 35
Current software license: 34 26
S/N: 819/02723
BIOS MAC Add: 00-a0-26-ae-3d-7a
>>

***** TRYING APP DUMP
  (CONFIGURED) APPCODE1.BIN ver.: 0.10.9.8 10.9.0.0
  *** ERROR ***
CRC error.
  (BY SEARCHING APP FILES ON FLASH)
    TRYING: APPCODE1.BIN ver.: 0.10.9.8 10.9.0.0
    *** ERROR ***
CRC error.
Restoring backup for application fault.....
Reading B:APPCODE1.BIN
Writing A:APPCODE1.BIN.....
..... OK.
Backup restored for application fault.
Restoring BIOS backup for application fault.....
BIOS Backup restored for application fault. Resetting...
```

- (4) Once the application has started up, when a particular firmware has been requested (*.bfw files), the application checks that the file is in the main partition and if it has a valid CRC; if the `firmware-checking` command is configured, and some of the requested firmwares fail (or do not exist or the CRC is invalid), the application requests a `backup restoring` and forces the router to reset.
- (5) Once the BIOS or the application has forced a `backup restoring`, the flag (which indicates the process has launched from backup and can only be deactivated when you successfully re-execute the `backup-files` or the `quote site backup` command) activates.

2.2 Distributing with the CIT image file (IMG)

2.2.1 Introduction

Devices with CIT. image file distribution do not implement the backup flash functionality, although it does allow you to save two CIT images. It's the BOOT that automatically maintains the last two loaded images, provided the total size of the images does not exceed the Flash space available.

2.2.2 Operating a system with double image in flash

- (1) On start up, the BOOT searches for the application established as active.
- (2) If it finds it, the device boots. If it doesn't or the CRC is wrong, it looks for the second image.
- (3) If it finds it, the device boots. If it doesn't or the CRC is wrong, this causes the router to restart.