Software Updating

April, 2015

ÍNDICE

Software Updating Via FTP

Introduction

The 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. Loss of this program is practically impossible and it also permits you to recoup a device in extreme cases. This element cannot be updated via software.

- **BIOS FLASH**

  Consists of the basic interface with the router hardware providing the C.I.T. with a more abstract view of this. 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 which 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 Teldat routers modular updating as well as reducing the size of the C.I.T., determined blocks are provided as isolated files. The need for these depends on the available hardware. E.g., the Teldat devices support various ADSL chipsets and depending on the type of chipset available in your device, will need one firmware (BFW) or another.

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

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

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

Updating Process

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

Distributing with BIOS, CIT 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 have been altered.

2) Connect to the device FTP server (you need a user and a password; default is user "root" without a 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 b8260.bin
local: b8260.bin remote: b8260.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 through "**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 teldath2gmr.bin
local: teldath2gmr.bin remote: teldath2gmr.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 command "**quote site savebuffer**".

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

8) One by one transfer and store the required firmware (files with "bfw" extension) through the "**put <*firmware.bfw*>**" and "**quote site savebuffer**" commands. In order to determine the necessary firmware, please see *Chapter 5 "Information required for updating"*.

```
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 permits you to check if the device has all the required files and if the elements versions are coherent with each other.

```
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 that included in the distribution .md5 file.

```
ftp> quote xmd5 fw000010.bfw
250 c103da2bb21508c797088eb4b5ca5a7c
ftp>
```

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

```
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
```

Note: The rescue.bin binary must be always present in the Teldat 4Ge. It will be helpful in case of main binary corruption. If it is not present it is needed to upload it.

> ***Note: Under certain circumstances, the transfer command may fail because the device does not have enough free volatile memory. In this case, activate the direct mode through the “****quote site direct on****” command before carrying out the transfer and deactivate it as soon as the said transfer has finalized through “****quote site direct off****”. Direct mode is when the file being transferred is directly stored in the Flash memory instead of in the temporary buffer before recording. If you have a high speed connection, you will see that the transfer is carried out in bursts with pauses when recording is being executed in the Flash memory.***

> ***WARNING: It must take into account the name used to store the binary file. In the case of “****Atlas 6x****” the code to run should be “****appcode1.bin****”. Information about changing code to run can be found in manual Dm704 Configuration Monitoring.***

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 the decompress has worked properly, then the content won’t have undergone any alteration.

2) Connect to the device FTP server (you need a user and password: default is user “root” without any 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 CIT image “**put <*cit-model-profile-version.img*>**”.

```
ftp> put cit-rp6xer-10.08.34.05.03.img
local: cit-rp6xer-10.08.34.05.03.img remote: cit-rp6xer-10.08.34.05.03.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 you have finished the transfer, execute the recording command through **“quote site savebuffer**”.

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

6) Finally and optionally, you have a command that lets you check to see if the device has all the necessary files and if the versions of the elements are compatible with each other.

```
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 normally from FTP, the device restarts after some 30 seconds. If you are exiting FTP through "CTRL.-C" the device restarts immediately. You can also restart the device using the console command "**load immediate.**

```
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
```

> ***Note: Under certain circumstances, it's possible that the transfer command fails because the device doesn't have enough free volatile memory; in this case, activate the direct mode through the "***quote site direct on***" command before executing the transfer and deactivate it as soon as transfer is finished using the "***quote site direct off* ***"command. The direct mode causes the file being transferred to save directly in the Flash memory instead of being stored in a temporary buffer before being recorded. If you have a high speed connection, you'll see that the transfer is executed in bursts with pauses when recording to the Flash memory.***

FTP Features

INTEGRITY Test

There is a system in the device which permits you to check the integrity or the coherency of the main file system contents. The command used to check if 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. Contrariwise, the device can indicate the problem, in order to correct it, in the response.

> ***Note: This operation is limited to checking that all the necessary software is present and that the interdependence of the different modules regarding the software release needs is correct. A positive response does not indicate that the device is remotely accessible as this implies the configuration is correct, something that is not checked. Also a negative response does not necessarily imply that the device cannot boot or is not remotely accessible.***

Other commands that permit you to obtain information:

- **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 permits clients supporting 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 for the applications.

- **SITE LISTFIRMWARES**
  Returns the firmware file list needed by the device so certain devices can operate. Allows clients who support this to know the necessary firmware modules so the device operates correctly.

- **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.

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 the checks and actions.

- **SITE CHECK BIOS OFF | ON**
  Activates or deactivates the rejection of applications whose minimum BIOS version needed is later than that of the BIOS currently in the system.

- **SITE CHECK CRC OFF | ON**
  Activates or deactivates the software integrity checking (CRC). **WARNING**: in DIRECT ON mode (please see notes of the subsections 2.1 and 2.2), in cases where the file CRC is erroneous, the file will have already been recorded in the file system and the old one eliminated.

- **SITE CHECK DELETE OFF | ON**
  Activates or deactivates the automatic deleting 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 all the files, not only those detected as known.

- **SITE CHECK FIRMWARE OFF | ON**
  Activates or deactivates the checking on the necessity and compatibility of the firmware received with the 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 that marked in the device. When this is activated, it ensures that the software received is capable of supporting or rectifying the known hardware problems in the device. **ATTENTION**: if this is deactivated, the device can mal function after the 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 2.1 and 2.2), in cases where the file length is erroneous (different from a multiple of 128), file will have already been recorded in the file system and the old one eliminated.

- **SITE CHECK PATH OFF | ON**
  Activates or deactivates the automatic sending of acknowledged files received such as BIOS to the “BIO” system when the system is in DIRECT OFF mode (please see notes of the subsections 2.1 and 2.2) when executing the SITE SAVEBUFFER command 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 received file. 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 which is active by default. In fact this command has no effect as the operation executes on establishing the connection with the client and cannot be modified during the session. This is implemented as a mirror of the command that is in the configuration which is effective. When activated, in cases where the files system, active by default, is not configured, when establishing the connection with the client, the first system activates depending on availability in the device and the 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 previous to that currently active in the device.

The STAT command permits you to view the state of the checks. 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.

Known Problems

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 been produced.

- In cases when this happens in DIRECT ON mode (please see notes of the subsections 2.1 and 2.2), this means that the file system does not have enough space to store the file. You need to see if it's necessary to delete files from the file system in order to send the new file.

- In cases when this happens in DIRECT OFF mode ((please see notes of the subsections 2.1 and 2.2), this means that 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:

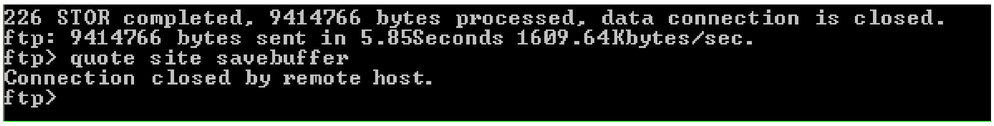
  - MAX
    If the figure is less than the total file length, this indicates that the temporary buffer is not capable of storing the file and you will need to configure the temporary buffer size in order to store it using the console command "*TEMP-BUFF*". You could also try downloading again in DIRECT ON mode (please see notes of the subsections 2.1 and 2.2).

  - 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 of the subsections 2.1 and 2.2) and try to resend the file.

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 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 *Chapter 6*, 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 this could be a problem with the traffic control systems which do not allow 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, as the device tries to make sure that one of the ports is port 20.

File transfer has stopped

Occasionally, with some files a problem occurs that stops the file being sent. This does not happen with all files however when it does happen with one, it always happens. It has been discovered that this problem occurs when the Windows FTP client sends TCP packets with an erroneous checksum and consequently cannot send the file. We don't know why this behavior occurs with some specific files but the problem can be resolved by using a different FTP client.

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 effect appears when the server is in DIRECT ON mode (please see notes of the subsections 2.1 and 2.2) and the client includes the local path in the file name it's sending.

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 and in DIRECT ON 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 available storage systems request the address from the root system.

In order to resolve this problem you can use specific client commands to manage the file name in remote systems (each client has their management), 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)
```

Unix Clients (ASCII mode)

Warning: ftp clients from the World of Unix, Linux and other similar operating systems, by default use the ASCII mode 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:

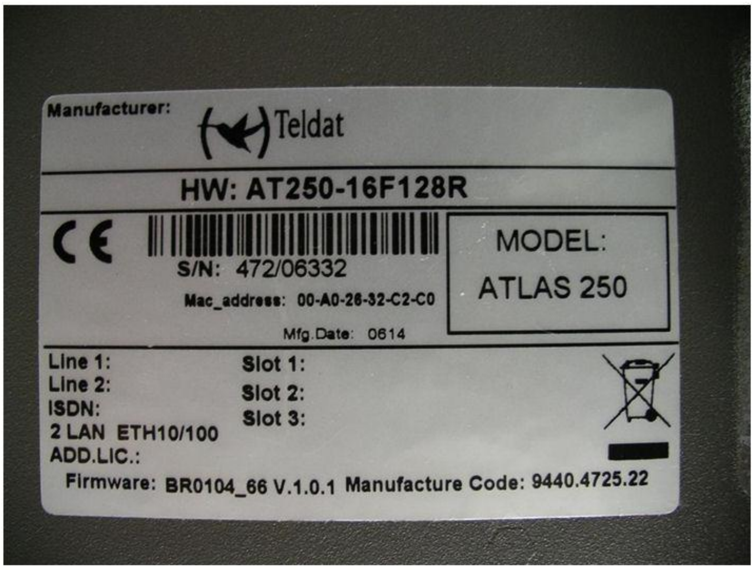
- DIRECT ON Mode (please see notes of the subsections 2.1 and 2.2):
  - CHECK LENGTH | CRC ON (COMPATIBLE ON) mode: If this is a binary file acknowledged as application or firmware, this is considered incorrect and a length error or a CRC error is produced. At this point, the file that has been sent 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 is not produced so 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 of the subsections 2.1 and 2.2):
  - 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 is produced. 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 is produced. 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.

Information required for updating

How to determine the appropriate distribution and the appropriate binary

To update a device, you need to know its identifier and the 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).



Manufacturer: Teldat

HW: AT250-16F128R

S/N: 472/06332

Mac_address: 00-A0-26-32-C2-C0

Mfg.Date: 0614

MODEL:
ATLAS 250

Line 1:
Line 2:
ISDN:
2 LAN ETH10/100
ADD.LIC.:

Slot 1:
Slot 2:
Slot 3:

Firmware: BR0104_66 V.1.0.1 Manufacture Code: 9440.4725.22

- 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) and 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 this fulfills.

For example, if we have various devices where the corresponding distribution is Teldat M, the "version_map.txt" file contained there 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 this must fulfill 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 this must fulfill 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 this must fulfill is: "L1.*, *F, *R, *" (L1.27, 4F, 32R, WAI), consequently, the binary to be loaded is teldatm_standard.bin.

How to determine the necessary firmware

To determine what firmwares a device needs, you have two options:

1) The FTP server command "**quote site listfirmwares**" which returns a list with the firmware file names included in the distribution which must be sent.

```
ftp> quote site listfirmwares
211 fw000000.bfw;fw000002.bfw
ftp>
```

2) The "**system firmwares-required**" command.

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

List of required firmwares for detected hardware
------------------------------------------------
   Filename                       Description
-------------- --------------------------------------------------
 fw000000.bfw   Alcatel-SGS Thomson DynaMiTe ADSL over POTS
 fw000002.bfw   Analog Devices Eagle ADSL over POTS
```

FTP Clients

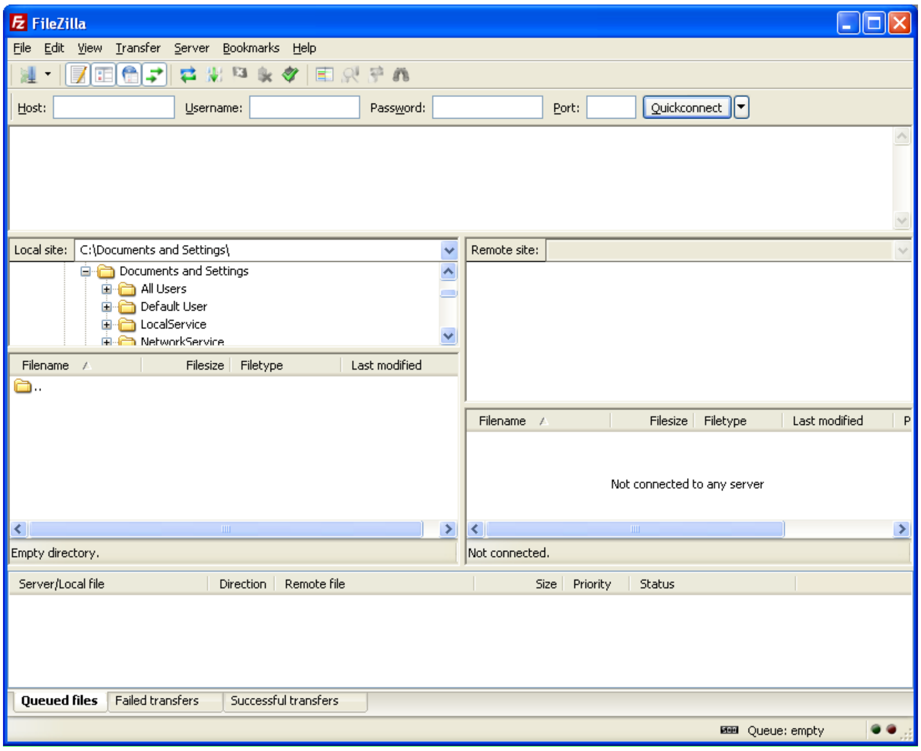
As already mentioned in previous chapters, there are several commands in FTP that due to their nature, take quite a long time to execute. Due to this, some FTP clients decide to cut off the connection when they don't receive a response in the established time, believing that there is a problem with the server. The Windows FTP client is among these clients. In the following paragraphs, we have explained how to use and configure determined 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 of the subsections 2.1 and 2.2).

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 as well as the remote window, thus permitting files to passed from one to another through multiple techniques including the "drag and drop" mechanism.

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


FileZilla
File Edit View Transfer Server Bookmarks Help
Host: Username: Password: Port: Quickconnect
Remote site:
Documents and Settings
All Users
Default User
LocalService
NetworkService
Filename Filesize Filetype Last modified
Filename Filesize Filetype Last modified P
Server/Local file Direction Remote file Size Priority Status
Queued files Failed transfers Successful transfers

Local site: C:\Documents and Settings\

Not connected to any server

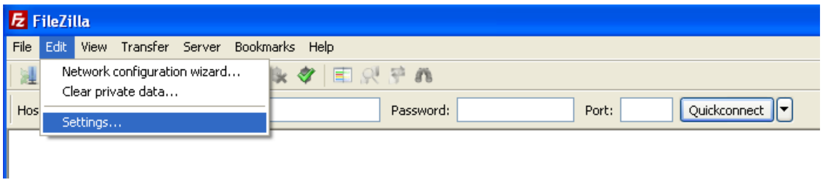
Empty directory.

Not connected.

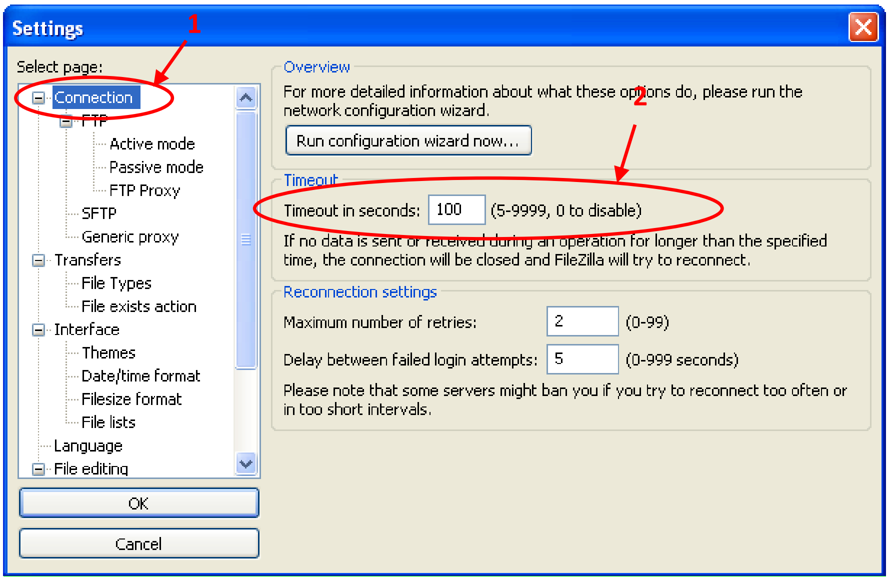
Queue: empty

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.


FileZilla
File Edit View Transfer Server Bookmarks Help
Network configuration wizard…
Clear private data…
Settings…
Hos
Password:
Port:
Quickconnect

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.



Overview

For more detailed information about what these options do, please run the network configuration wizard.

Timeout

Timeout in seconds: 100 (5-9999, 0 to disable)

If no data is sent or received during an operation for longer than the specified time, the connection will be closed and FileZilla will try to reconnect.

Reconnection settings

Maximum number of retries: 2 (0-99)

Delay between failed login attempts: 5 (0-999 seconds)

Please note that some servers might ban you if you try to reconnect too often or in too short intervals.

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:

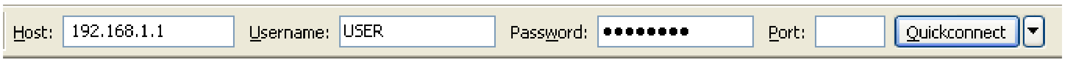
You should always use the FTP protocol.

1) Connecting to the router’s FTP server

To do this, use the *“Quickconnect”* bar. Here 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.

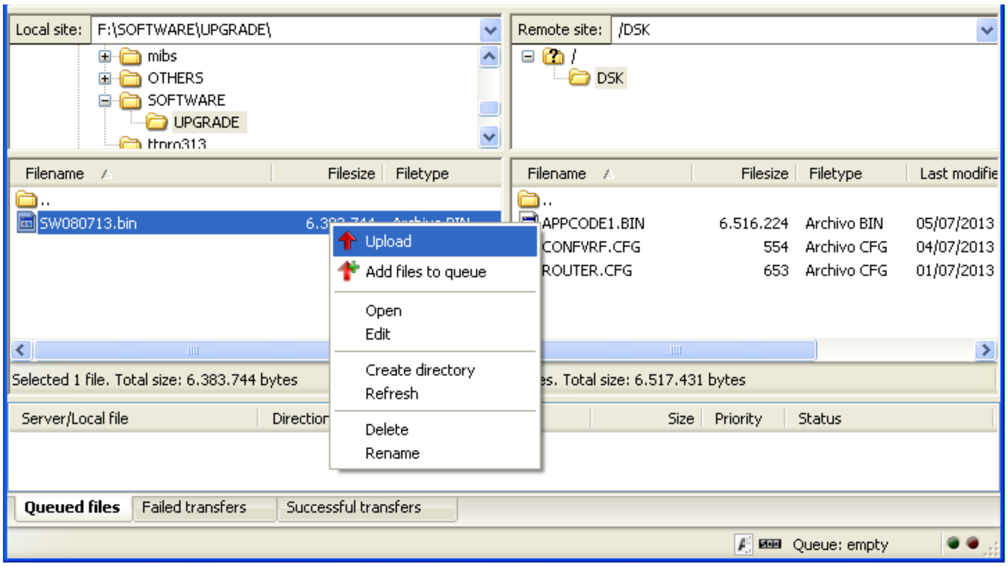


Host: 192.168.1.1 Username: USER Password: •••••••• Port:

2) Transferring the file

There are various alternatives to do this:

- By simply clicking on the file with the right-hand mouse button and selecting the "*Upload*" option.



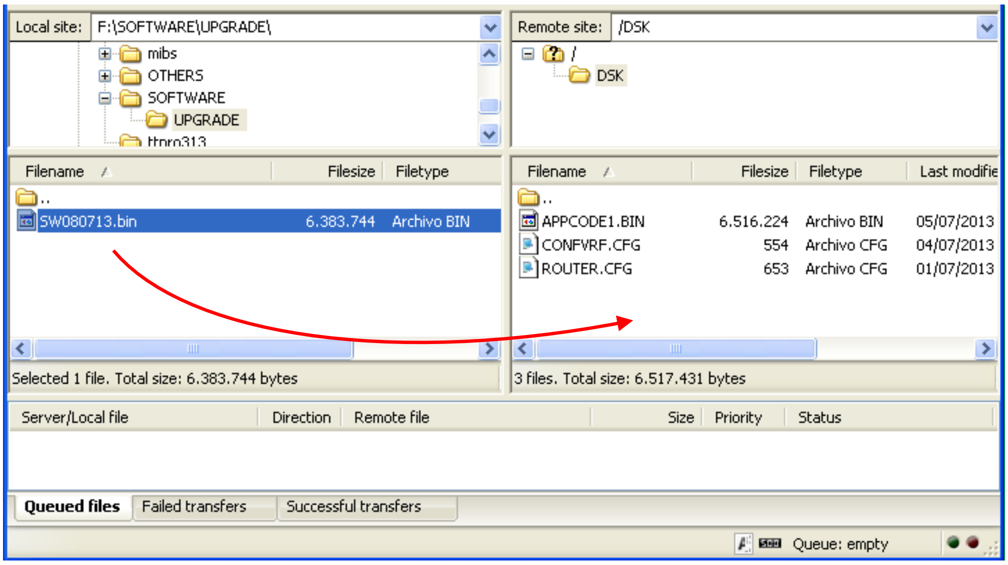
Filename	Filesize	Filetype
..		
SW080713.bin	6.383.744	Archivo BIN

Filename	Filesize	Filetype	Last modifie
..			
APPCODE1.BIN	6.516.224	Archivo BIN	05/07/2013
CONFVRF.CFG	554	Archivo CFG	04/07/2013
ROUTER.CFG	653	Archivo CFG	01/07/2013

Selected 1 file. Total size: 6.383.744 bytes

es. Total size: 6.517.431 bytes

- By double clicking on the file.
- Or, through the "*drag and drop*" mechanism.



Filename	Filesize	Filetype
..		
SW080713.bin	6.383.744	Archivo BIN

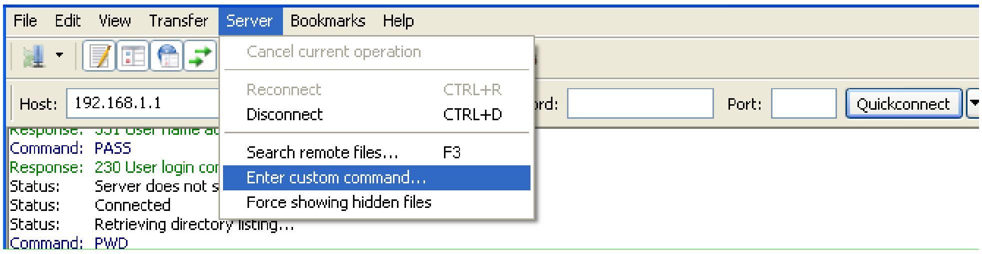
Filename	Filesize	Filetype	Last modifie
..			
APPCODE1.BIN	6.516.224	Archivo BIN	05/07/2013
CONFVRF.CFG	554	Archivo CFG	04/07/2013
ROUTER.CFG	653	Archivo CFG	01/07/2013

Selected 1 file. Total size: 6.383.744 bytes

3 files. Total size: 6.517.431 bytes

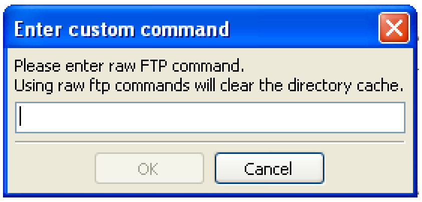
3) <u>Execute the recording command of the file in the disk and close the FTP connection</u>

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 *"Enter"* key on the keyboard.



Host: 192.168.1.1

```
Response:  331 User name ac
Command:   PASS
Response:  230 User login co
Status:    Server does not s
Status:    Connected
Status:    Retrieving directory listing…
Command:   PWD
```



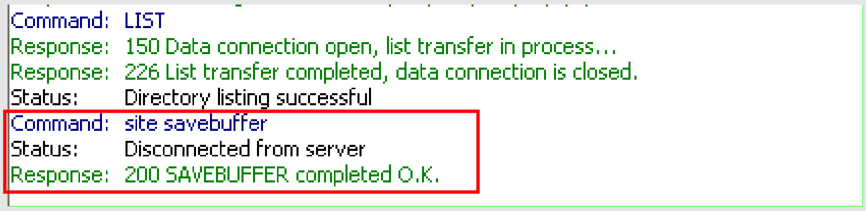
Enter custom command

Please enter raw FTP command.
Using raw ftp commands will clear the directory cache.

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

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

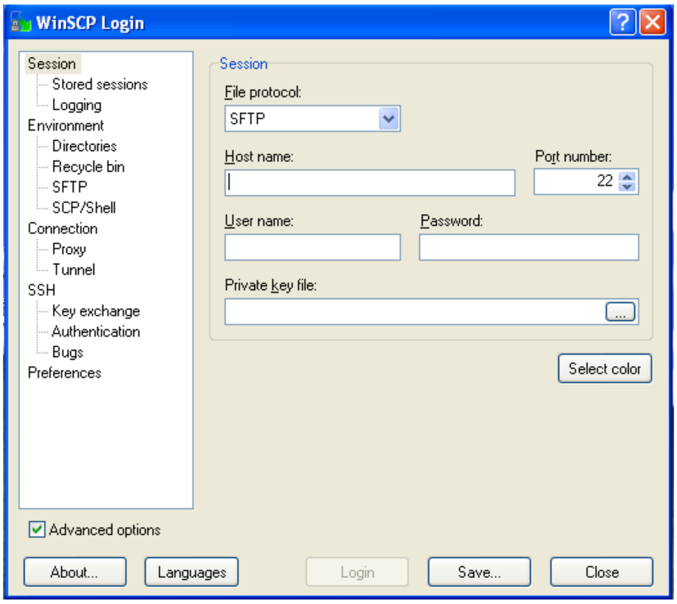
While executing the "site savebuffer" command, you may receive a response indicating that you are disconnected from the server. In this case, do not execute any action as after a certain amount of time you will receive an OK message associated to this command.



```
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.
```

WinSCP Client

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



WinSCP Login

Session

File protocol: SFTP

Host name:

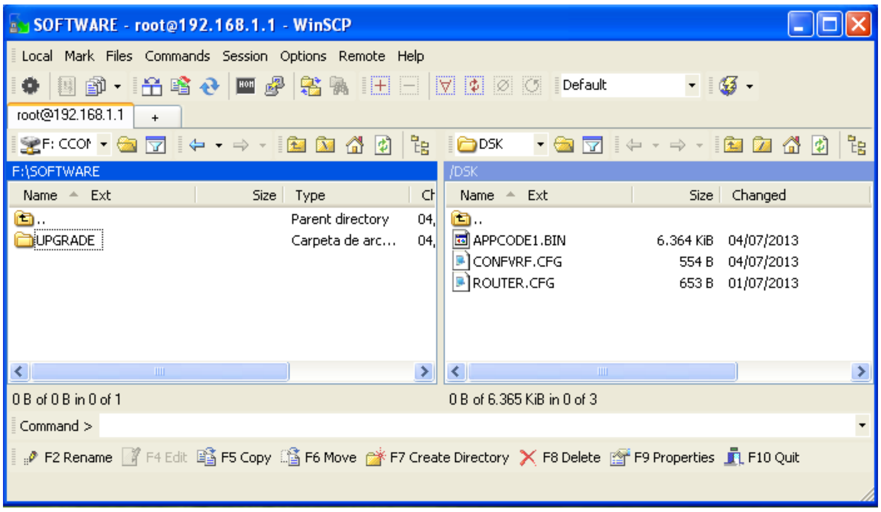
Port number: 22

User name:

Password:

Private key file:

☑ Advanced options



SOFTWARE - root@192.168.1.1 - WinSCP

root@192.168.1.1

F:\SOFTWARE

Name	Ext	Size	Type	Ch
..			Parent directory	04,
UPGRADE			Carpeta de arc...	04,

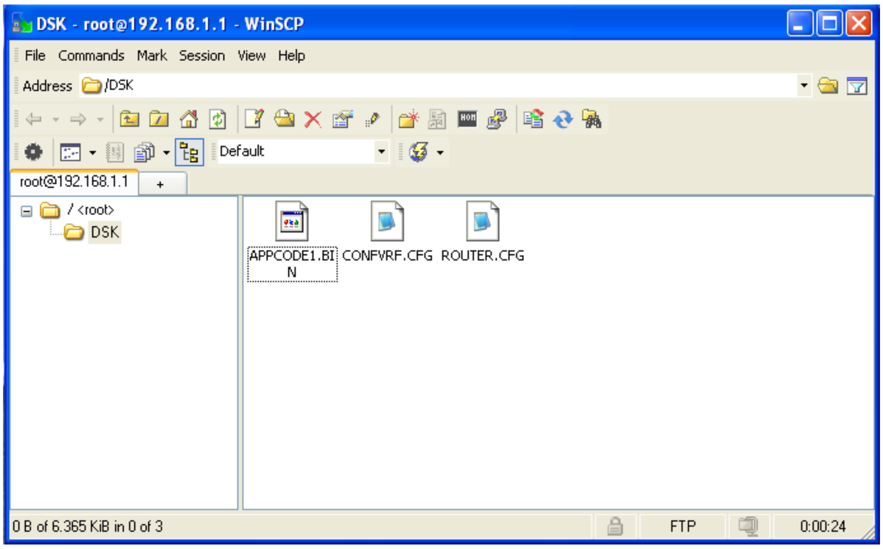
/DSK

Name	Ext	Size	Changed
..			
APPCODE1.BIN		6.364 KiB	04/07/2013
CONFVRF.CFG		554 B	04/07/2013
ROUTER.CFG		653 B	01/07/2013

0 B of 0 B in 0 of 1

0 B of 6.365 KiB in 0 of 3

"*Commander Interface*" Interface



Address /DSK

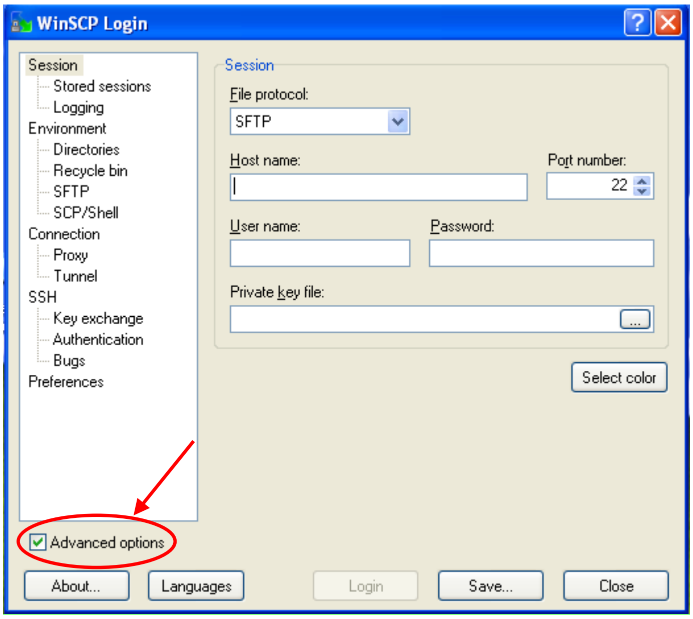
0 B of 6.365 KiB in 0 of 3

0:00:24

“*Explorer Interface*” Interface

Before beginning the updating process, 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.

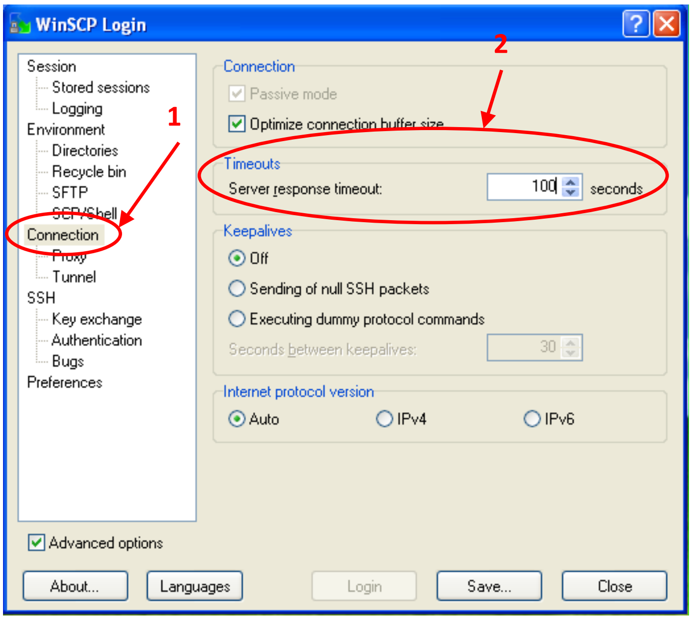


File protocol: SFTP

Port number: 22

☑ Advanced options

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



Connection

☑ Passive mode

☑ Optimize connection buffer size

Timeouts

Server response timeout: 100 seconds

Keepalives

● Off

○ Sending of null SSH packets

○ Executing dummy protocol commands

Seconds between keepalives: 30

Internet protocol version

● Auto ○ IPv4 ○ IPv6

☑ Advanced options

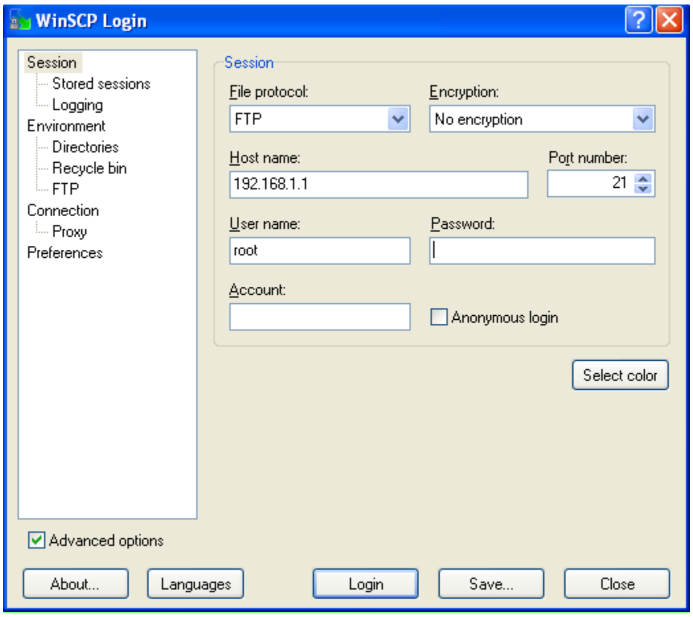
Once this change has been made, you can now update the software by carrying out the steps given below:

You should always use the FTP protocol.

1) <u>Connecting to the router's FTP server</u>

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 respectively. 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.



Session

File protocol: FTP

Encryption: No encryption

Host name: 192.168.1.1

Port number: 21

User name: root

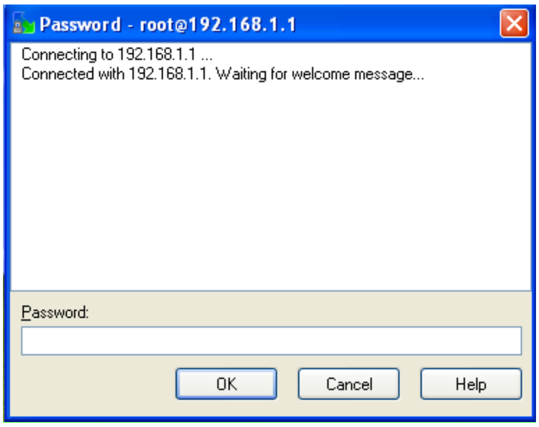
Password:

Account:

□ Anonymous login

☑ Advanced options

During the connection, it’s possible that you will be asked for the access credentials again. If this happens, reenter the requested data and click on the *“OK”* button.



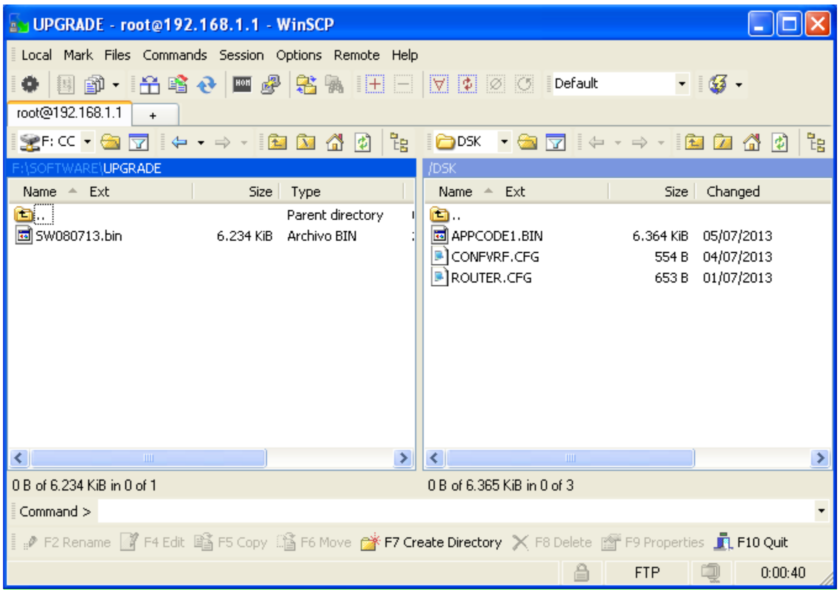
Password - root@192.168.1.1

```
Connecting to 192.168.1.1 ...
Connected with 192.168.1.1. Waiting for welcome message...
```

Password:

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 hand panel shows your local device and on the left is the router panel.



UPGRADE - root@192.168.1.1 - WinSCP

F:\SOFTWARE\UPGRADE

Name	Ext	Size	Type
..			Parent directory
SW080713.bin		6.234 KiB	Archivo BIN

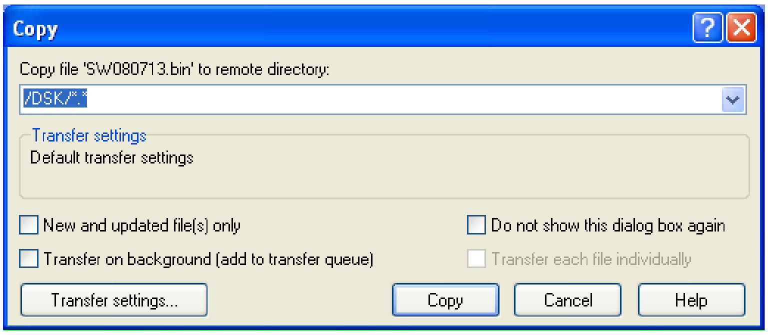
0 B of 6.234 KiB in 0 of 1

/DSK

Name	Ext	Size	Changed
..			
APPCODE1.BIN		6.364 KiB	05/07/2013
CONFVRF.CFG		554 B	04/07/2013
ROUTER.CFG		653 B	01/07/2013

0 B of 6.365 KiB in 0 of 3

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.



Copy file 'SW080713.bin' to remote directory:

/DSK/*.*

Transfer settings

Default transfer settings

□ New and updated file(s) only

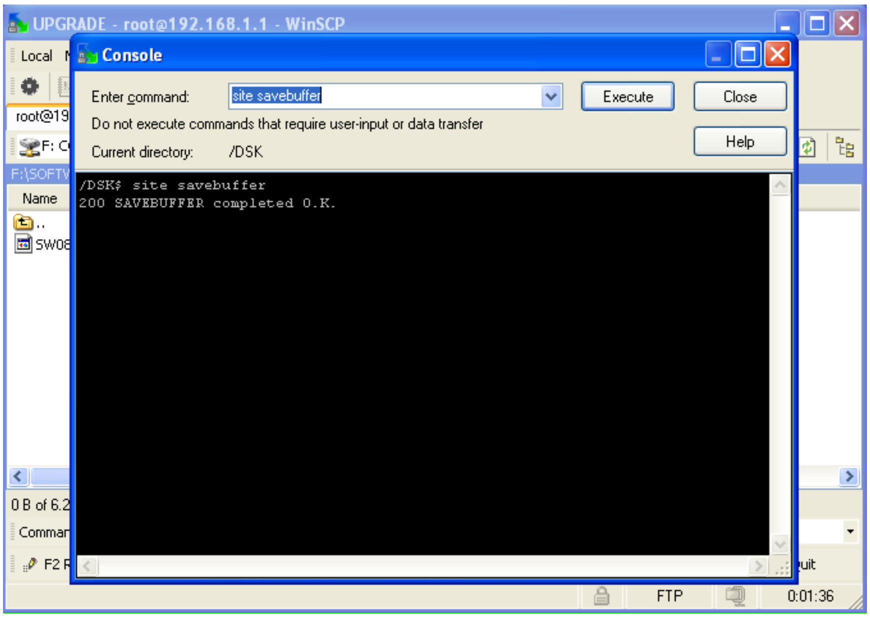
□ Do not show this dialog box again

□ Transfer on background (add to transfer queue)

□ Transfer each file individually

3) <u>Execute the recording command of the file in the disk and close the FTP connection</u>

To do this, select the *“Open Terminal”* from the *“Commands”* menu that then opens a new window.



Enter command: site savebuffer

Do not execute commands that require user-input or data transfer

Current directory: /DSK

```
/DSK$ site savebuffer
200 SAVEBUFFER completed O.K.
```

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. The lower part 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*”

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 the *Chapter 2 “Updating Process”* according to the type of software you wish to update.

Appendix A. Backup Systems

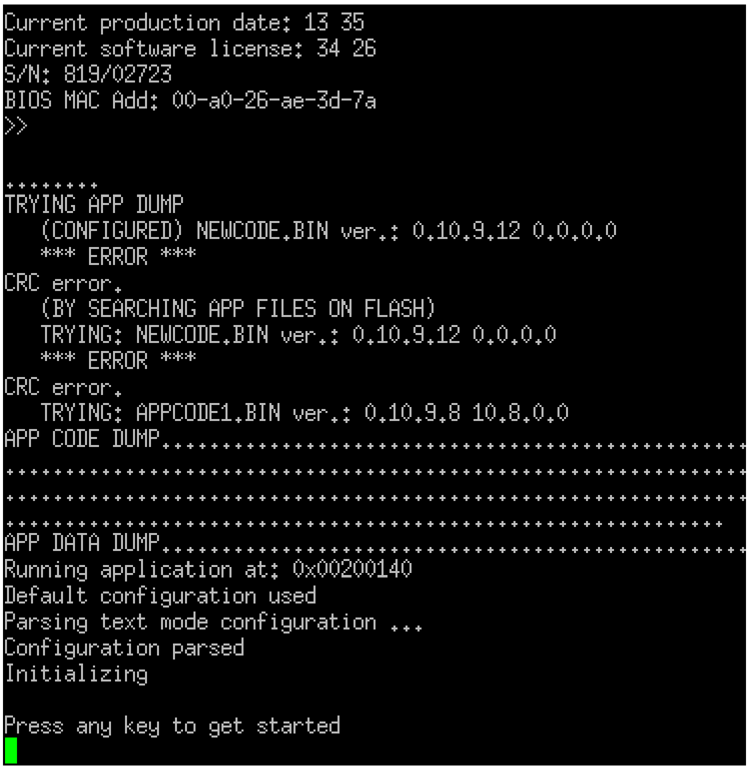
1. Distributing with BIOS, CIT and FWs files

These devices implement two backup systems that permit the boot when the device detects problems.

> ***Some devices don't have enough space in Flash to store more than one C.I.T code. Therefore, you must ensure that the total sum of the sizes does not exceed the available amount of Flash.***

a. Two C.I.T. codes loaded in the Flash disk.

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

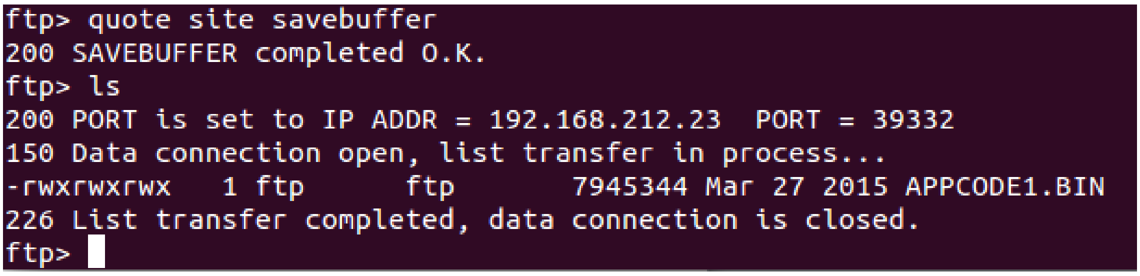


```
Current production date: 13 35
Current software license: 34 26
S/N: 819/02723
BIOS MAC Add: 00-a0-26-ae-3d-7a
>>

........
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, it is necessary to store both files with different names because by default the device ignores the name of the file and uses a specific name for recording it and as consequence the device always replaces the file if it exists.

The steps to execute are:

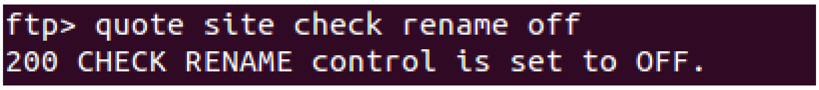
1. Connect to the device FTP server.
2. Transfer and store the first C.I.T. code if you want to update or replace the existing file:
   a. Configure the binary mode through the "`bin`" command.
   b. Transfer the application through the "`put <application.bin>`" command.
   c. Once the transfer has completed, execute the recording command "`quote site savebuffer`".



```
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 C.I.T. code with a different name:

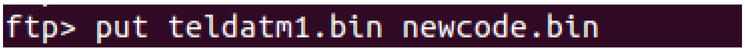
   a. Execute the "`quote site check rename off`" command.



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

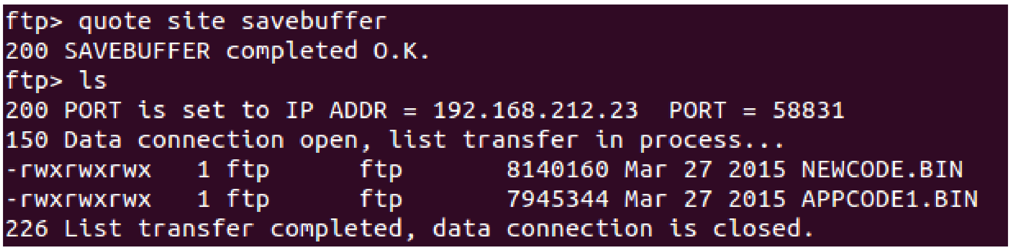
   b. Configure the binary mode through the "`bin`" command.

   c. 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
```

   d. Once the transfer has completed, execute the recording command "`quote site savebuffer`".



```
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 application no selected will be used as backup. There are two commands available for this:

   1) Console

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

   2) FTP

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

   This command permits you to establish the active application through renaming of the files. For this works you must take into account the BIOS searches by name on start up, therefore, you must assign to the new application that you want to establish as active the same name that the active application has currently in the device.

b. Flash Backup System

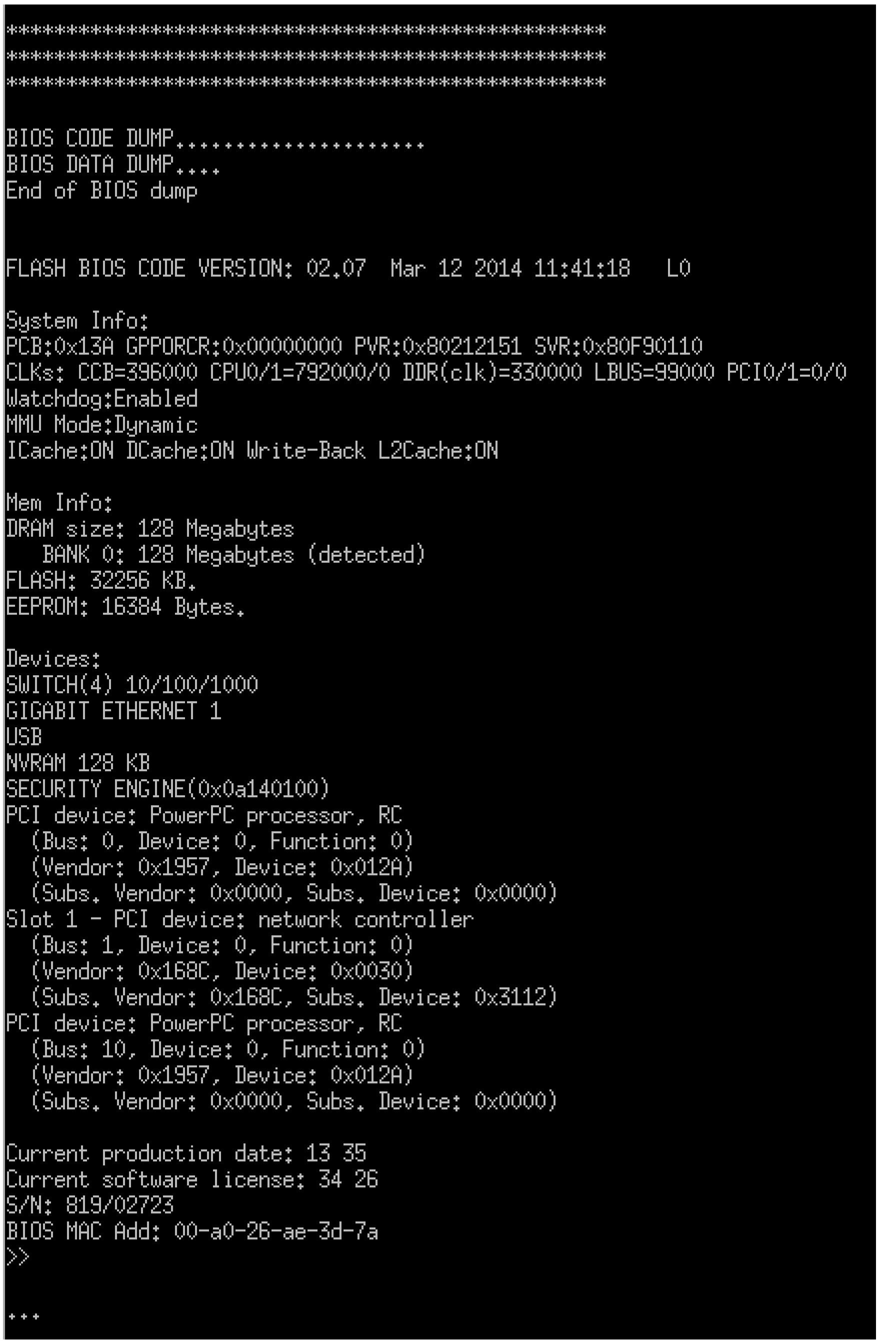
The Flash backup system permits automatic restoration of the last successfully installed distribution when the device detects problems in some of the software elements (BIOS FLASH, application and firmwares).

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

Flash Disk Formatting

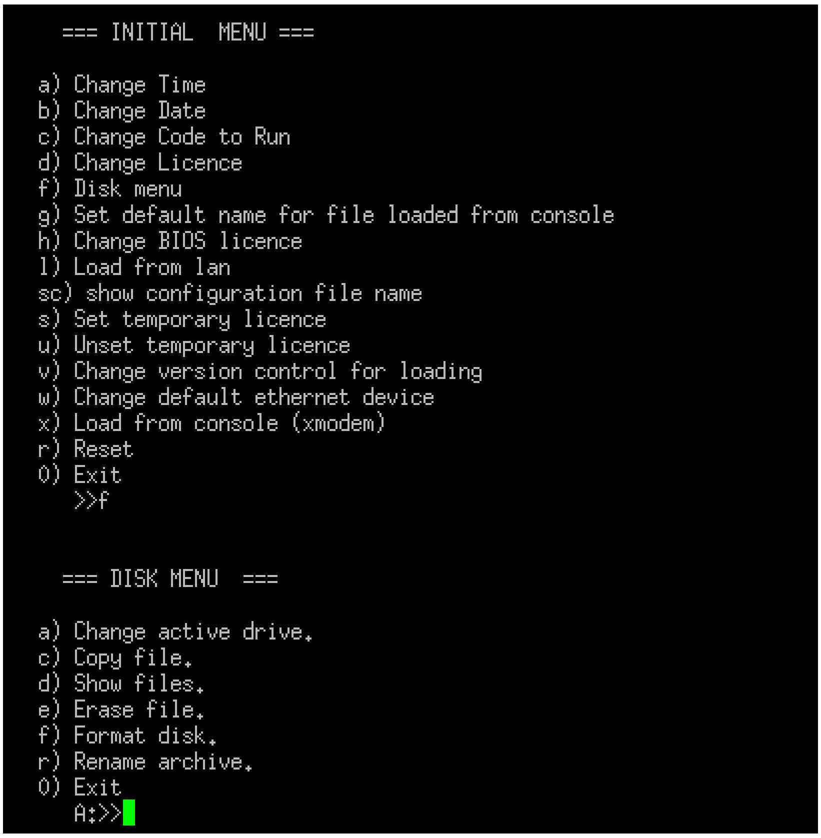
Formatting the Flash disk is destructive and only available in the local console in order to guarantee that the user has local access to the device to load it adequately.

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



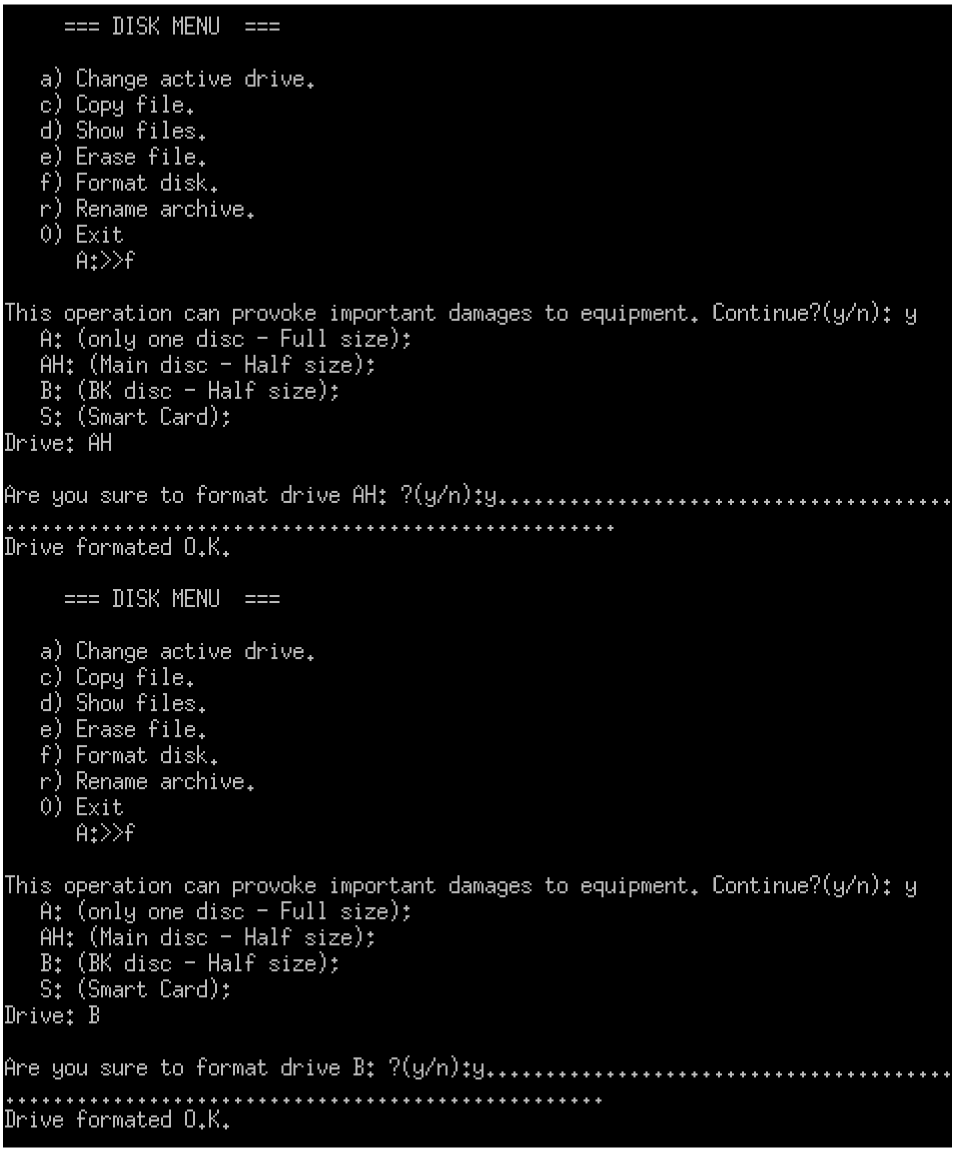
```
**************************************************
**************************************************
**************************************************


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(clk)=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:>>
```

3. Format the main partition through the "`AH: (Main disc - Half size)`" option and subsequently 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 menus, the device starts up and a C.I.T. code must be loaded.

Operating Flash Backup System

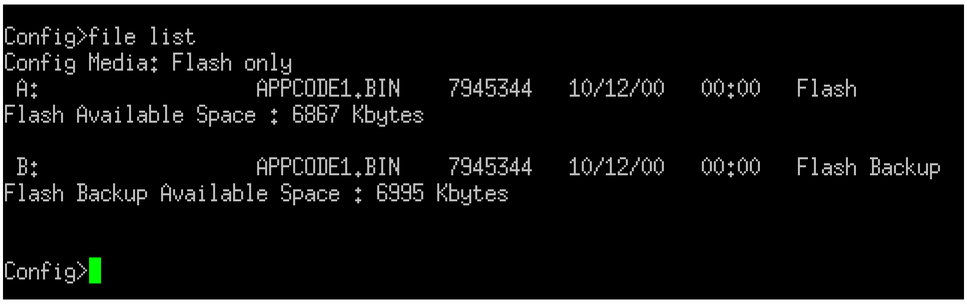
Once the Flash backup system has been enabled, the user must establish the restoration point, i.e. execute the copy of the main partition information to the backup partition. There are two commands available for this:

1) Console

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

2) FTP

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



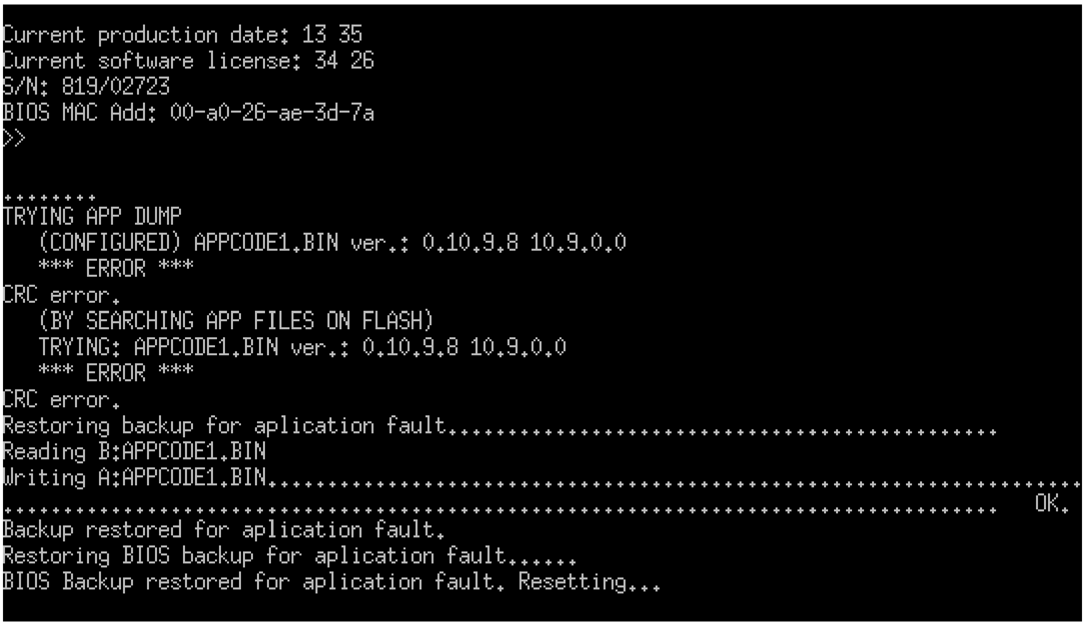
```
Config>file list
Config Media: Flash only
 A:                 APPCODE1.BIN    7945344   10/12/00   00:00   Flash
Flash Available Space : 6867 Kbytes

 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 is automatic:

1. On start up, the BIOS search 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 existing application file (*.bn) 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 aplication fault.............................................
Reading B:APPCODE1.BIN
Writing A:APPCODE1.BIN.....................................................................
....................................................................................   OK.
Backup restored for aplication fault.
Restoring BIOS backup for aplication fault......
BIOS Backup restored for aplication fault. Resetting...
```

4. Once the application has started up, when a determined 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 makes the router reset.

5. Once the BIOS or the application has provoked a "`backup restoring`", the flag, which indicates that this has started up from backup and which can only be deactivated when you successfully re-execute the "`backup-files`" or the "`quote site backup`" command, activates.

2. Distributing with the C.I.T. image file (IMG)

1. Introduction

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

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.