



Base Stations/Handset Firmware Update Via TFTP

Contents

Contents	1
Document History	1
Introduction: Firmware Upgrades/Downgrades	1
Terms & Abbreviations	2
References	2
Network Dimensioning	2
TFTP Configuration from "SolarWinds" TFTP Server	3
Create Firmware Directories	4
Login to Base SME Configuration Interface	5
Firmware Update Settings	7
Base Station(s) Firmware Upgrade	9
Handset (s) Firmware Upgrade	10
Verification of Firmware Upgrade	10
Reboot the Base station(s).....	11

i-Serv

I-SERV supports and provides to the vendor an interface that performs the following operations related to firmware on the device:

- 1) Verify whether the new firmware package is compatible with the device.
- 2) Upgrade the firmware on the device to the new firmware
- 3) Roll back the firmware on the device to the previous firmware version

Terms & Abbreviations

For the purpose of this document, the following abbreviations hold:

DHCP: Dynamic Host Configuration Protocol

DNS: Domain Name Server

HTTP: Hyper Text Transfer Protocol

IOS: Internetworking Operating System

NAT: Network Address Translator

PCMA: A-law Pulse Code Modulation

PCMU: mu-law Pulse Code Modulation

SME: Small and Medium scale Enterprise

STUN: Session Traversal Utilities for NAT

Network Dimensioning

In principle, a number of hardware and software components should be available or be satisfied before base station/handset update can be possible.

The minimum hardware and software components that are required to be able update via TFTP include the following (but not limited to):

Standard SIP Nodes (i.e. handsets)

Base stations

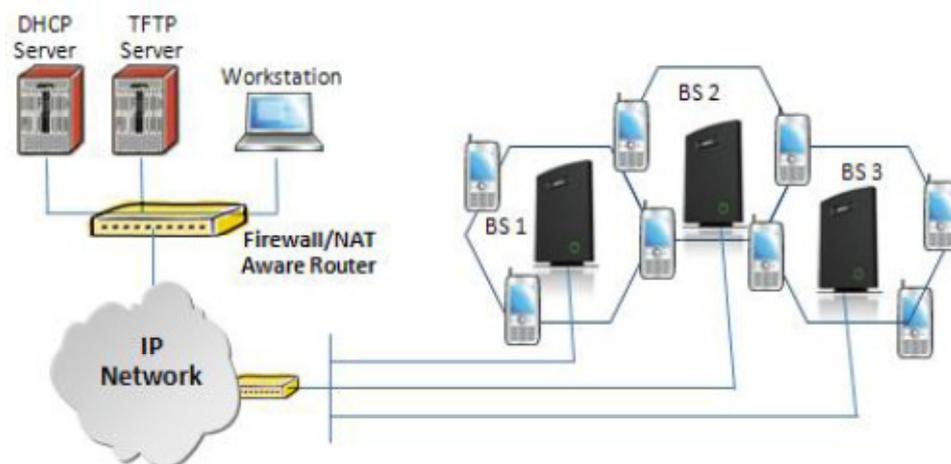
TFTP Server (Several Windows and Linux applications are available)

DHCP Server (Several Windows and Linux applications are available)

Workstation (for e.g. Normal terminal or PC)

Any standard browser (for e.g. firefox)

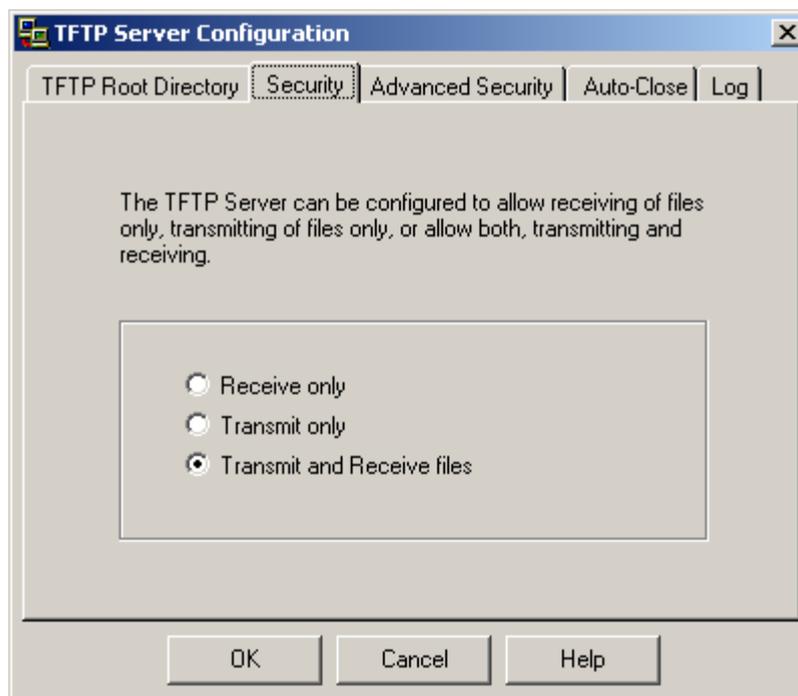
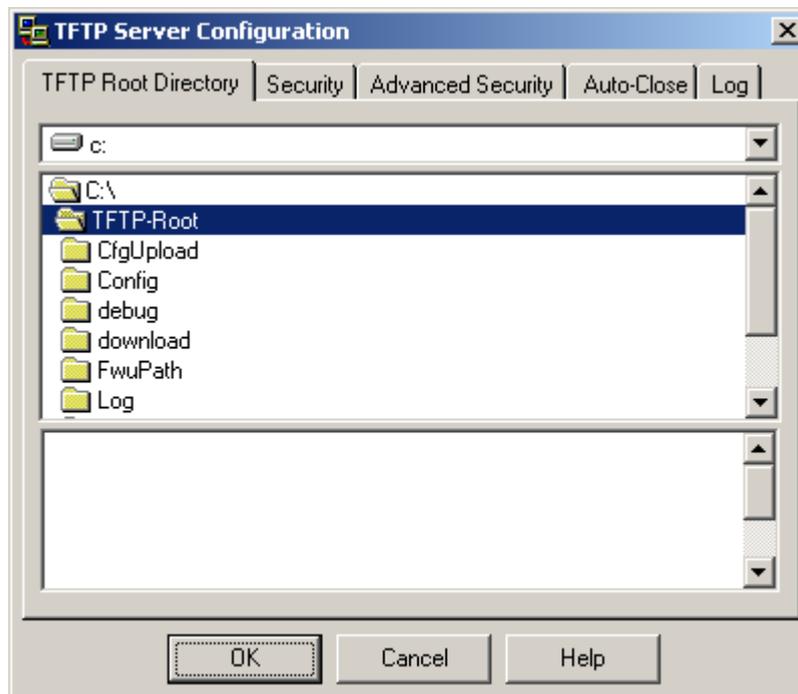
Public/Private Network



TFTP Configuration from “SolarWinds” TFTP Server

i-Serv

Create the following relevant folders as shown in the snap shots and choose defaults settings for the remaining options.



Create Firmware Directories

STEP 1 For Umber base firmware update make a folder named **“BeatUs”** in the TFTP-Root and place the fwu file/files (Firmware) in this folder. The base firmware must be renamed to **“BeatUsSw_v00xx.fwu”** or **“BeatUsSw_4181_v00xx.fwu”**.

The admin from the service provider’s side must create the relevant firmware directory in the server where both old and new firmware(s) can be placed in it. (See the STEP above)

i-Serv

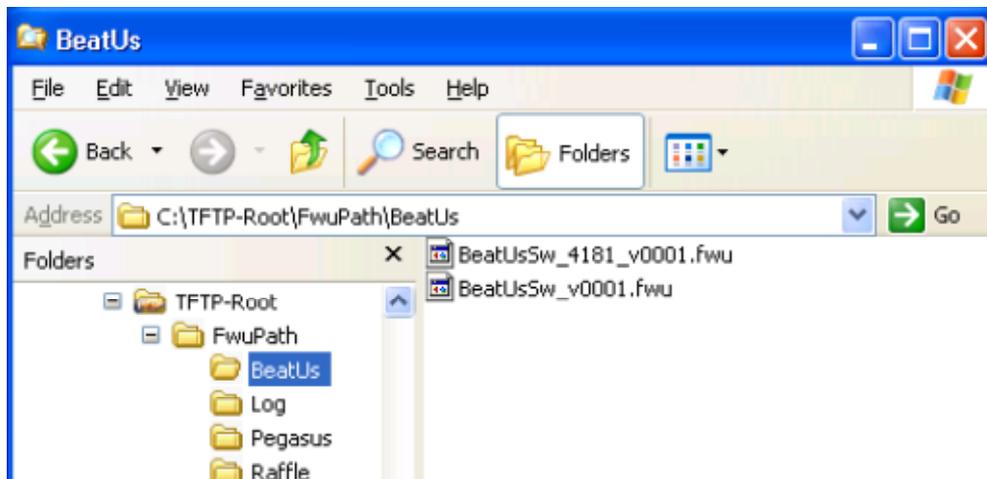
The firmware directory or path should be `\<Server>\<FwuPath>\BeatUs\`, where `<Server>` is usually the root directory of the server (for e.g. `C:\TFTP-Root`) and `<FwuPath>` is a folder within the `<Server>` that contains the **BeatUs** directory.

STEP 2 For UMBER handset firmware update, make a folder named “**Pegasus**” in the TFTP-Root and place the fwu file/files (Firmware) in this folder. The handset firmware must be renamed to “**PegasusSw_v00xx.fwu**” or “**PegasusSw_4181_v00xx.fwu**”.

For Raffle handset firmware update, make a folder named “**Raffle**” in the TFTP-Root and place the fwu file/files (Firmware) in this folder. The base firmware must be renamed to “**Raffle_v00xx.fwu**”. The firmware directory or path should be `\<Server>\<FwuPath>\Pegasus\ (or \Raffle\)`, where `<Server>` is usually the root directory of the server (for e.g. `C:\TFTP-Root`) and `<FwuPath>` is a folder within the `<Server>` that contains the **Pegasus (or Raffle)** directory.

IMPORTANT:

The **BeatUs**, **Pegasus**, **Raffle** directory names cannot be changed.



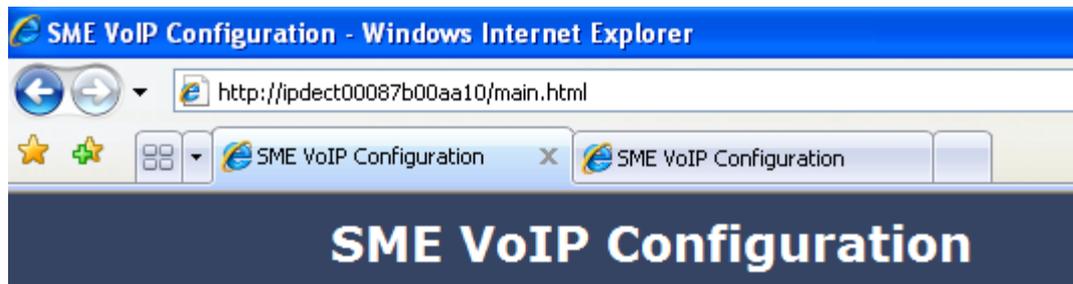
Login to Base SME Configuration Interface

STEP 3 Connect the Base station to a private network via standard Ethernet cable (CAT-5).

STEP 4 Open any standard browser and enter the address:

`http://ipdect<MAC-Address-Base-Station>`

for e.g. `http://ipdect00087B00AA10`. This will retrieve the HTTP Web Server page from the base station with hardware address **00087B00AA10**.



STEP 5 You can also use a sniffer like Wireshark (freeware program) to identify which IP the base has received.

i-Serv

Below is shown how to see which IP address the base has received from the DHCP server. In the example we start the trace and filter on **"bootp"**. Then we power up the base which is connected to the same network as the sniffer (wireshark). After a short while an offer is given by the DHCP server, and it is possible to see that the base received the IP address 192.168.50.76

The screenshot shows the Wireshark interface with the filter set to 'bootp'. The packet list table is as follows:

No.	Time	Source	Destination	Protocol	Info
148	19.088556	0.0.0.0	255.255.255.255	DHCP	DHCP Discover - Transaction ID 0x683d
149	19.088979	192.168.50.3	255.255.255.255	DHCP	DHCP Offer - Transaction ID 0x683d
150	19.108222	0.0.0.0	255.255.255.255	DHCP	DHCP Request - Transaction ID 0x683d
151	19.110455	192.168.50.3	255.255.255.255	DHCP	DHCP ACK - Transaction ID 0x683d
315	33.511515	0.0.0.0	255.255.255.255	DHCP	DHCP Discover - Transaction ID 0x401edbf1
331	36.511562	0.0.0.0	255.255.255.255	DHCP	DHCP Discover - Transaction ID 0x401edbf1

The details pane for frame 149 shows the following information:

- Message type: Boot Reply (2)
- Hardware type: Ethernet
- Hardware address length: 6
- Hops: 0
- Transaction ID: 0x0000683d
- Seconds elapsed: 0
- Bootp flags: 0x0000 (Unicast)
- Client IP address: 0.0.0.0 (0.0.0.0)
- Your (client) IP address: 192.168.50.76 (192.168.50.76)**
- Next server IP address: 192.168.50.3 (192.168.50.3)
- Relay agent IP address: 0.0.0.0 (0.0.0.0)

STEP 6 On the Login page, enter your authenticating credentials (i.e. username and password). Click OK button.

The dialog box titled "Connect to ipdetect00087b00aa10" contains the following text and controls:

The server ipdetect00087b00aa10 at requires a username and password.

Warning: This server is requesting that your username and password be sent in an insecure manner (basic authentication without a secure connection).

User name:

Password:

Remember my password

Buttons: OK, Cancel

STEP 7 Once you have authenticated, the browser will display front end of the SME Configuration Interface. The front end will show relevant information of the base station.

SME VoIP Configuration

Home/Status
Extensions
Servers
Network
Management
Firmware Update
Time
Country
Security
Contact List
Multi cell

Welcome

Please select a configuration page in the index pane on left.

System Information:

Phone Type:	IPDECT
System Type:	Generic SIP (RFC 3261)
Current local time:	20/Sep/2010 13:36:33
Operation time:	00:25:03 (H:M:S)
RFPI-Address:	116E604904; RPN:04
MAC-Address:	00087b077cf7
IP-Address:	192.168.50.114
Firmware-Version:	IPDECT/00.37//16-Sep-10 20:50
Firmware-URL:	tftp://10.10.104.41/FwuPath

SIP Identity Status on this Base Station:

Press button to reboot.

Reboot

Firmware Update Settings

STEP 8 Scroll down and Click on **Firmware Update** url link in the **SME VoIP Configuration Interface** to view the **Firmware Update Settings** page.

Firmware Update Settings

Firmware update server address:

Firmware path:

Handset Type	Required version
<input type="button" value="Save"/>	

Update Base Stations

Update this Base Station only
 Update all Base Stations

Required version

i-Serv

Parameters

Firmware Update Settings

Firmware update server address

Firmware path

Description

This is the IP address of server where the firmware is located. Currently, only 32-bit is supported (i.e. IPv4 – <aaa.bbb.ccc.ddd>)

The firmware is found at the <Server>\<FwuPath>\BeatUs\ directory found in the FTP or TFTP server.

The <Server> is usually the root directory of the server created by the administrator and should NOT be specified.

The <FwuPath> is a folder within the <Server> that contains the BeatUs directory. This MUST be specified.

By default the ...BeatUs is hard-coded into the firmware. Therefore it should not be specified in the firmware path.

Example of firmware path is \HQ_Office, \South_Office, or \FwuPath, etc. in that manner.

Update Base Stations/Handsets

Required Version

This is 8-bit value. Usually the firmware filename is BeatUsSw_v00XX.fwu. The administrator has to enter for e.g. numerical value XX, where XX is a positive integer.

STEP 9 On the **Firmware Update Settings** page enter the relevant parameters as described in the table above.

Next, Click on **Save** button to keep the modified parameters into the base station.

The parameters are successfully saved

You will be redirected after 3 seconds

Base Station(s) Firmware Upgrade

STEP 10 On the **Firmware Update Settings** page > scroll down to the **Update Base Stations** section > Enter the relevant firmware version (for e.g. **11**) of the base station to upgrade or to downgrade.

It is possible to upgrade a single base station and/or several base stations > the admin should choose right the radio button.

STEP 11 Still on the same **Update Base Stations** section > choose **Start update** button > select **OK** button from the dialog window to start the update/downgrade procedure.

The relevant base station(s) will automatically reboot and retrieve the firmware specified from the server and update itself accordingly.

Firmware Update Settings

Firmware update server address:

Firmware path:

Handset Type

Required version

Update Base Stations

Update this Base Station only
 Update all Base Stations

Required version

Message from webpage

Are you sure you want to upgrade this base station with version 100?

All on-going voice calls are dropped from the base station(s) immediately the firmware update procedure starts.

Handset (s) Firmware Upgrade

STEP 12 In the **Handset Type** section on the **Firmware Update Settings** page > Enter the relevant handset firmware (for e.g. 100) to upgrade or downgrade > press **Save** button, and after “**The parameters are successfully saved**” the process of updating all handsets in the private network are initialized.

Handset Type	Required Version
UXP1240H	<input type="text" value="100"/>
8630	<input type="text" value="100"/>
UXP1240H HW ver 00	<input type="text" value="100"/>

It will take up to 3 hours before the handset has downloaded the software. When the software is transferred to the handset the old software version will swap with the new version, when the

i-Serv

handset is placed in the handset charger cradle. During software swap the handset top LED will flash in red and green colors.

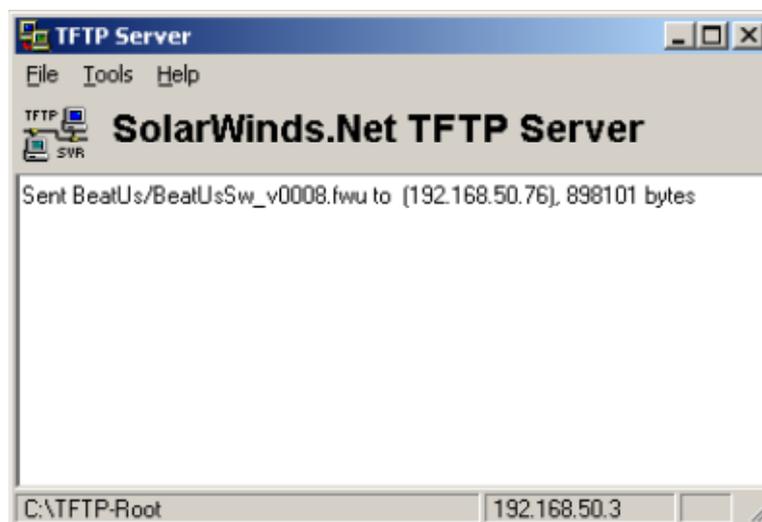
In case "Required version:" is set to "0" the handset FWU is disabled.

Verification of Firmware Upgrade

STEP 13 From the Handset **Menu** navigate to **Settings** > Scroll down to **Status** this will list some information including Base station and Handset firmware versions.



STEP 14 Now the download should be initiated and it should be stated in the log window of the TFTP server:



STEP 15 During the download, the Wireshark shows the download as shown below:

i-Serv

No.	Time	Source	Destination	Protocol	Info
203	26.639841	192.168.50.79	192.168.50.3	TFTP	Read Request, File: /Beatus/BeatUsSw_v0008.fwu
204	26.654789	192.168.50.3	192.168.50.79	TFTP	Data Packet, Block: 1
205	26.660174	192.168.50.79	192.168.50.3	TFTP	Acknowledgement, Block: 1
206	26.660610	192.168.50.3	192.168.50.79	TFTP	Data Packet, Block: 2
207	26.663632	192.168.50.79	192.168.50.3	TFTP	Acknowledgement, Block: 2
208	26.663965	192.168.50.3	192.168.50.79	TFTP	Data Packet, Block: 3
209	26.667229	192.168.50.79	192.168.50.3	TFTP	Acknowledgement, Block: 3
210	26.667546	192.168.50.3	192.168.50.79	TFTP	Data Packet, Block: 4
211	26.670955	192.168.50.79	192.168.50.3	TFTP	Acknowledgement, Block: 4
212	26.671270	192.168.50.3	192.168.50.79	TFTP	Data Packet, Block: 5
213	26.674694	192.168.50.79	192.168.50.3	TFTP	Acknowledgement, Block: 5
214	26.675007	192.168.50.3	192.168.50.79	TFTP	Data Packet, Block: 6
215	26.678754	192.168.50.79	192.168.50.3	TFTP	Acknowledgement, Block: 6
216	26.679280	192.168.50.3	192.168.50.79	TFTP	Data Packet, Block: 7
217	26.682781	192.168.50.79	192.168.50.3	TFTP	Acknowledgement, Block: 7
218	26.683110	192.168.50.3	192.168.50.79	TFTP	Data Packet, Block: 8
219	26.686694	192.168.50.79	192.168.50.3	TFTP	Acknowledgement, Block: 8
220	26.687023	192.168.50.3	192.168.50.79	TFTP	Data Packet, Block: 9
221	26.693048	192.168.50.79	192.168.50.3	TFTP	Acknowledgement, Block: 9
222	26.693400	192.168.50.3	192.168.50.79	TFTP	Data Packet, Block: 10
223	26.698878	192.168.50.79	192.168.50.3	TFTP	Acknowledgement, Block: 10
224	26.699199	192.168.50.3	192.168.50.79	TFTP	Data Packet, Block: 11
225	26.705615	192.168.50.79	192.168.50.3	TFTP	Acknowledgement, Block: 11
226	26.705931	192.168.50.3	192.168.50.79	TFTP	Data Packet, Block: 12
227	26.712233	192.168.50.79	192.168.50.3	TFTP	Acknowledgement, Block: 12
228	26.712549	192.168.50.3	192.168.50.79	TFTP	Data Packet, Block: 13

Frame 203 (81 bytes on wire, 81 bytes captured)
Ethernet II, Src: RtxTelc_07:7c:73 (00:08:7b:07:7c:73), Dst: Intel_b4:f7:83 (00:02:b3:b4:f7:83)
802.1Q Virtual LAN, PRI: 0, CFI: 0, ID: 21
Internet Protocol, Src: 192.168.50.79 (192.168.50.79), Dst: 192.168.50.3 (192.168.50.3)
User Datagram Protocol, Src Port: 60769 (60769), Dst Port: tftp (69)
Trivial File Transfer Protocol

Reboot the Base station(s)

These steps below should only be performed when certain conditions are met.

STEP 16 In principle the base station(s) should reboot automatically when the when the **Start update** button is selected > to begin the firmware update procedure.

If for some unknown reasons the base station does restart, then the admin must manually reboot the base station so the firmware update process can begin in the base station.

Make sure the URL is shown on the page before rebooting the base station.

System Information:

Phone Type: IPDECT HW Version 00
System Type: Generic SIP (RFC 3261)
RF Band: EU
Current local time: 07/Jun/2011 15:52:41
Operation time: 7 Days 23:25:14 (H:M:S)
RFPI-Address: 1000015E00; RPN:00
MAC-Address: 00087b077ce8
IP-Address: 192.168.11.104
Firmware-Version: IPDECT/01.41/26-May-2011 15:54
Firmware-URL: tftp://10.10.104.144/FwuPath

Multi cell Ready(Keep-alive) Primary

SIP Identity Str

2155@192.168.
2152@192.168.
2151@192.168.
2156@192.168.
2154@192.168.
2153@192.168.

Message from webpage

Are you sure you want to reboot base station? NOTE: Ongoing call will delay the reboot until all active calls on the base station is ended.

OK Cancel

Press button to reboot.

Reboot Forced Reboot



Click **OK** button from the dialog window. A successful restart of the base stations will lead to a display of the page: **Base Station has been reset**. The firmware update is now in progress.

Base Station has been reset

Please wait, base station rebooting

Home

STEP 17 Wait about 3-5 minutes, Reboot the base station.

The base station will now be updated (base LED will flash). The software version number on the start page should be changed to the new version number.

The message “**Base FWU ended with exit code -2101**” is shown in the debug log and the new firmware will be running after a restart of the base station.