HOW TO CONFIGURE GATEWAY

(PRACTICAL SETTINGS)

Contents

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

References

[1]: System Parameter Description Version 0.1

Introduction

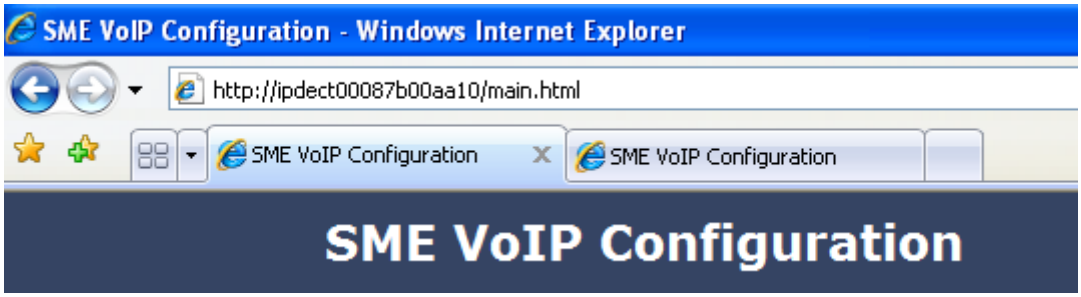
In this document we briefly describe how to configure the SME VoIP gateway (i.e. base stations).

NOTE This documentation is valid for Base station firmware version 00.41 and above.

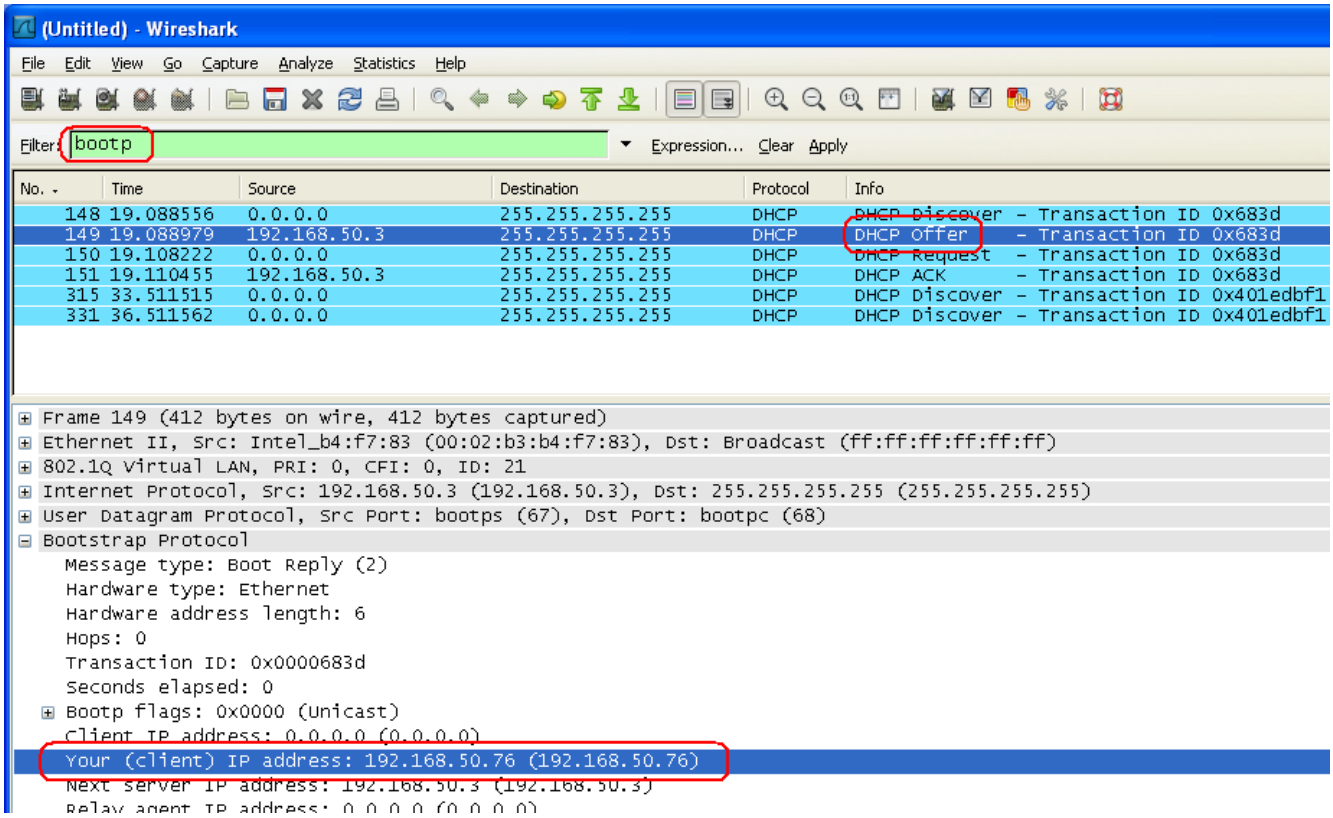
Gateway Firmware Upgrade

STEP 1 Connect the Base station (gateway) to a private network via standard Ethernet cable (CAT-5).

STEP 2 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**

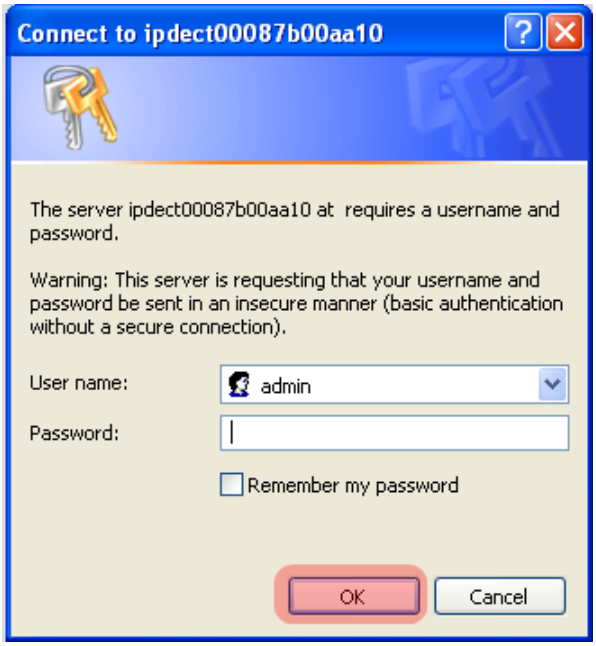


STEP 3 You can also use a sniffer like Wireshark (freeware program) to identify which IP the base has received.
Below is shown how to see which IP address the base has received from the DHCP server. In the example we start the trace and filter on "**bootp**". Then we power up the base which is connected 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

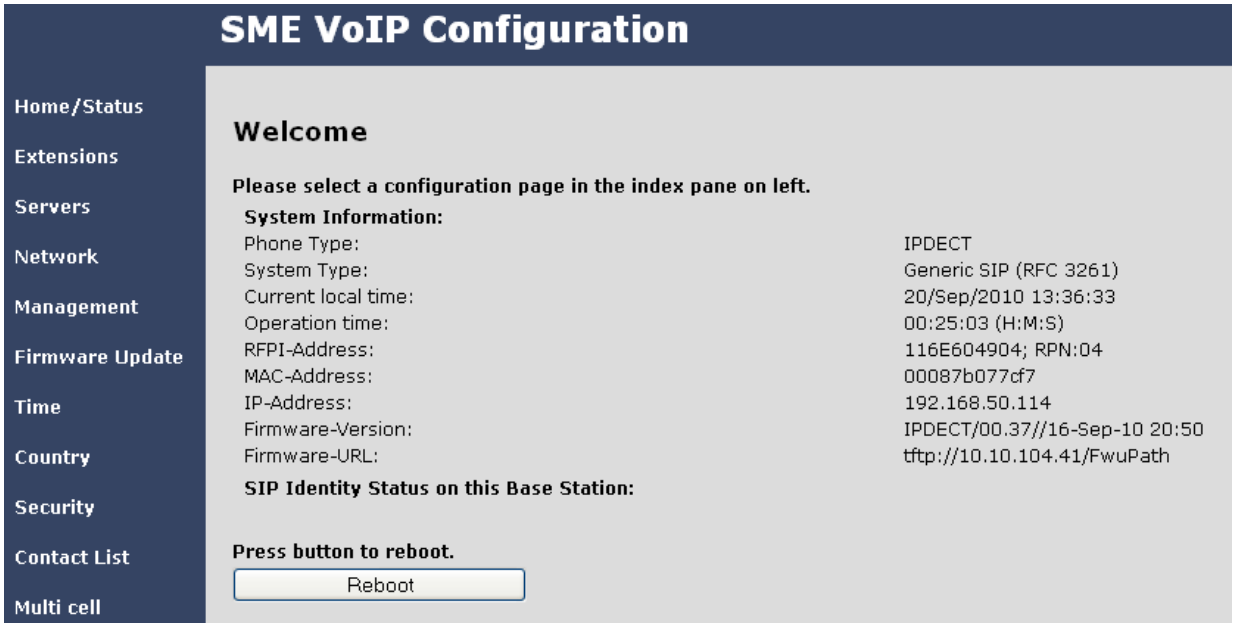


Source: JMG

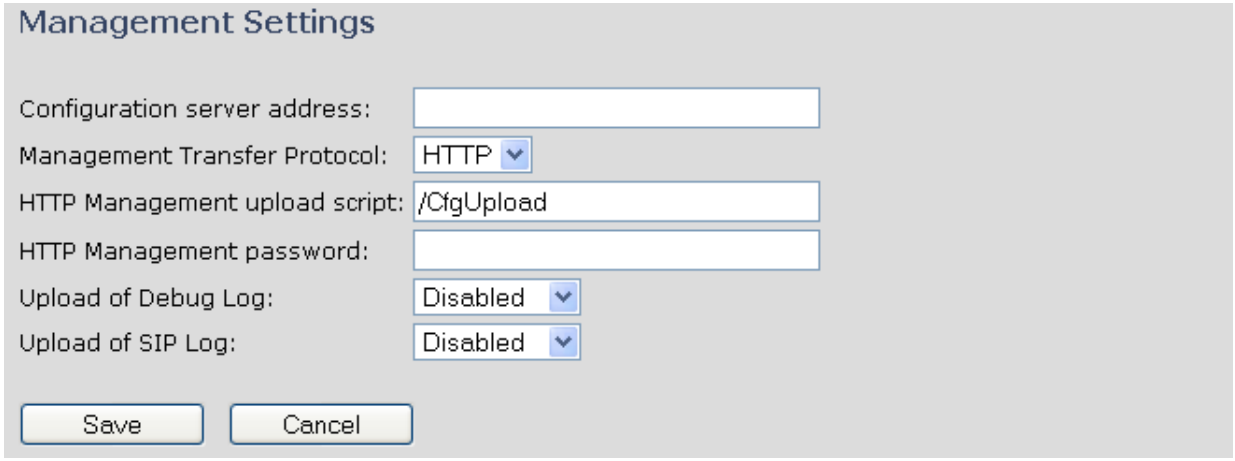
STEP 4 On the Login page, enter your authenticating credentials (i.e. username and password). Click **OK** button.



STEP 5 Once you have authenticated, the browser will display the front end of the SME Configuration Interface. The front end will show relevant information on the base station.



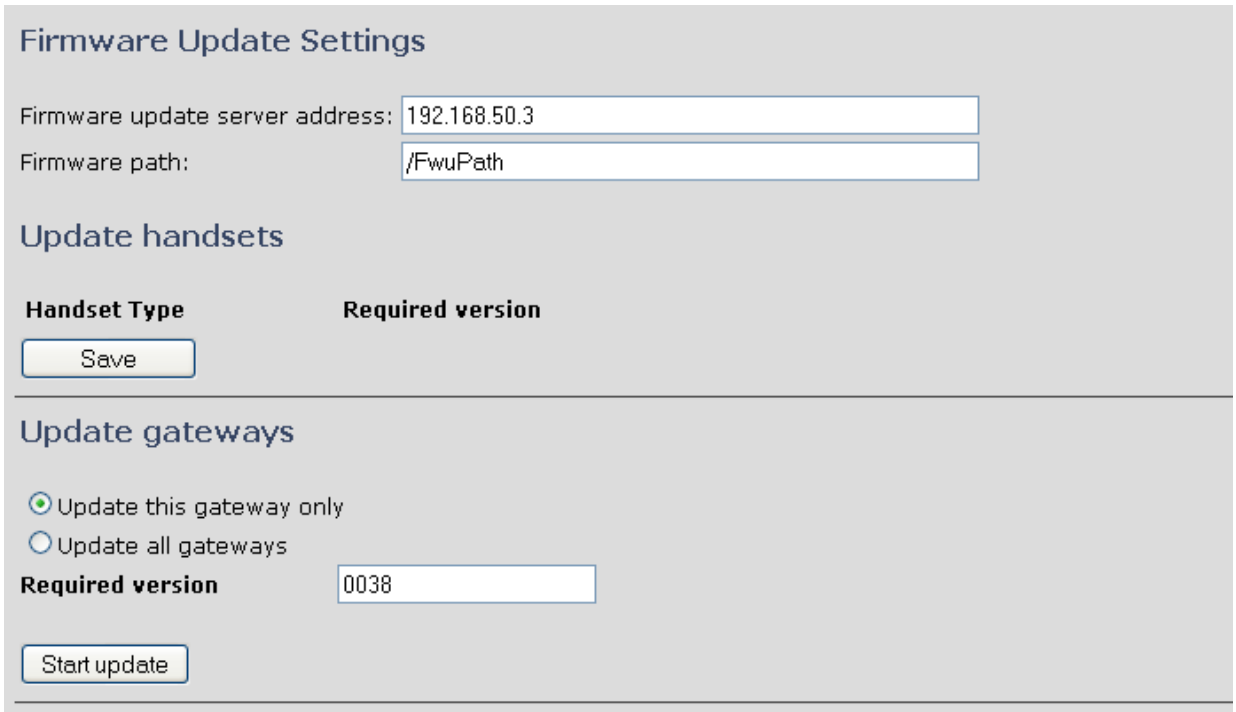
STEP 6 Enter the relevant Management server information in the system. Select the Management transfer protocol "**TFTP**" drop down menu.



.

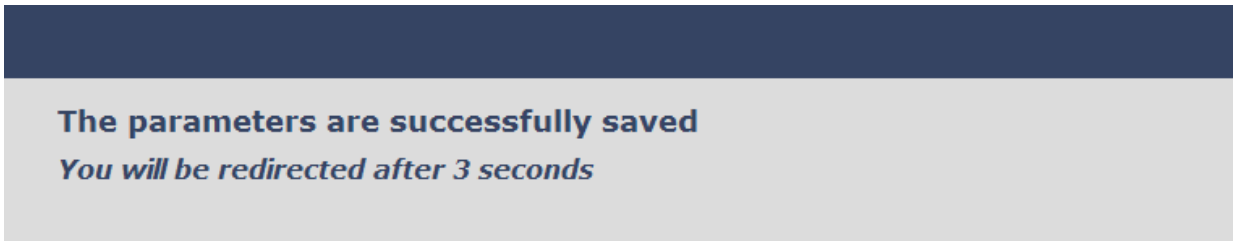
Firmware Update Settings

STEP 7 Scroll down and Click on **Firmware Update** url link in the **SME VoIP Configuration Interface** to view the **Firmware Update Settings** page.



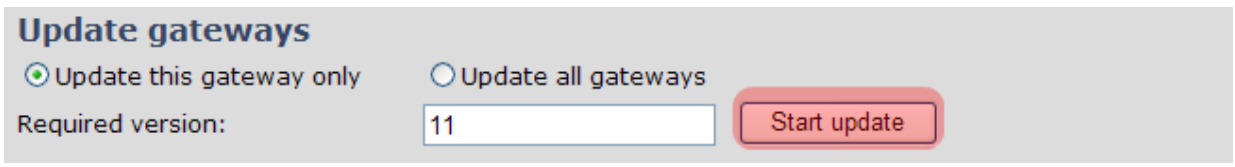
Parameters	Description
Firmware Update Settings	
Firmware update server address	This is the IP address of the server where the firmware is located. Currently, only 32 bit is supported (i.e. IPv4 – **<aaa.bbb.ccc.ddd>**)
Firmware path	The firmware is found at the **\<Server>\<FwuPath>\BeatUs** directory 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 Gateways/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 8 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.

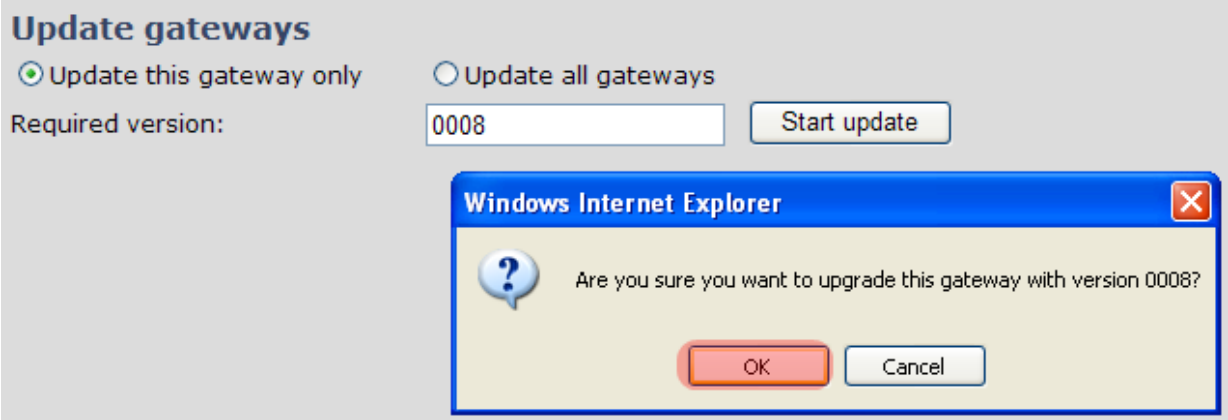


Gateway Firmware Version Setting

STEP 9 On the **Firmware Update Settings** page > scroll down to the **Update Gateways** 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 the right radio button.



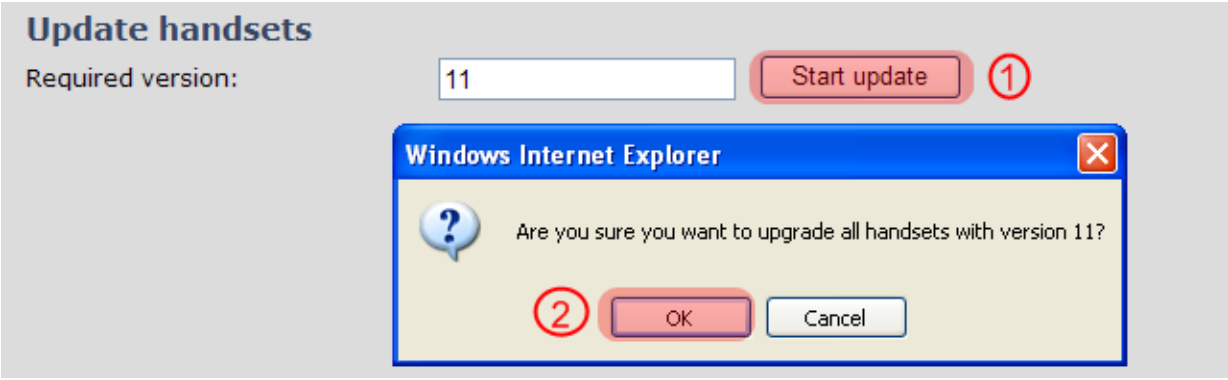
STEP 10 Still on the same **Update Gateway** section > choose **Start update** button > select **OK** button from the dialog window to start the update/downgrade procedure.
The relevant base station(s) will automatically reboot and retrieve the firmware specified from the server and update itself accordingly.



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

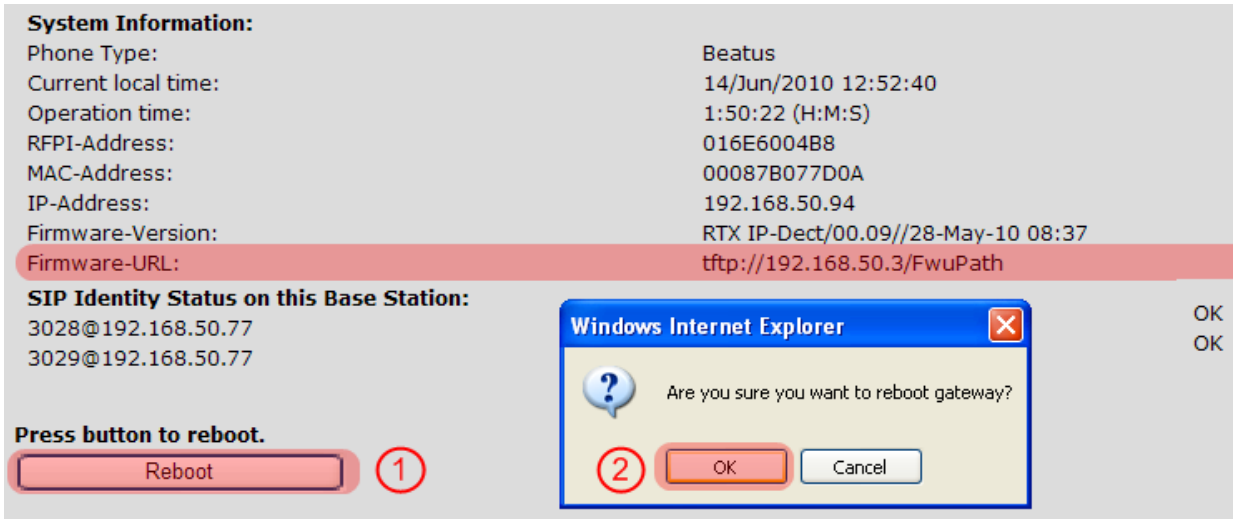
Handset (s) Firmware Version Setting

STEP 11 Scroll down to **Update handset** section on the **Firmware Update Settings** page > Enter the relevant handset firmware (for e.g. 11) to upgrade or downgrade > press **Start update** button > Click on **OK** button from the dialog window to initialise the process of updating all handsets in the private network.

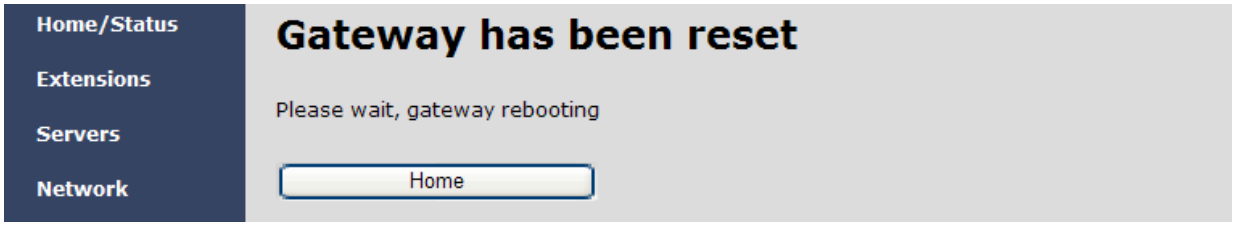


Reboot the Gateway

STEP 12 In principle the base station(s) should reboot automatically 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.



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



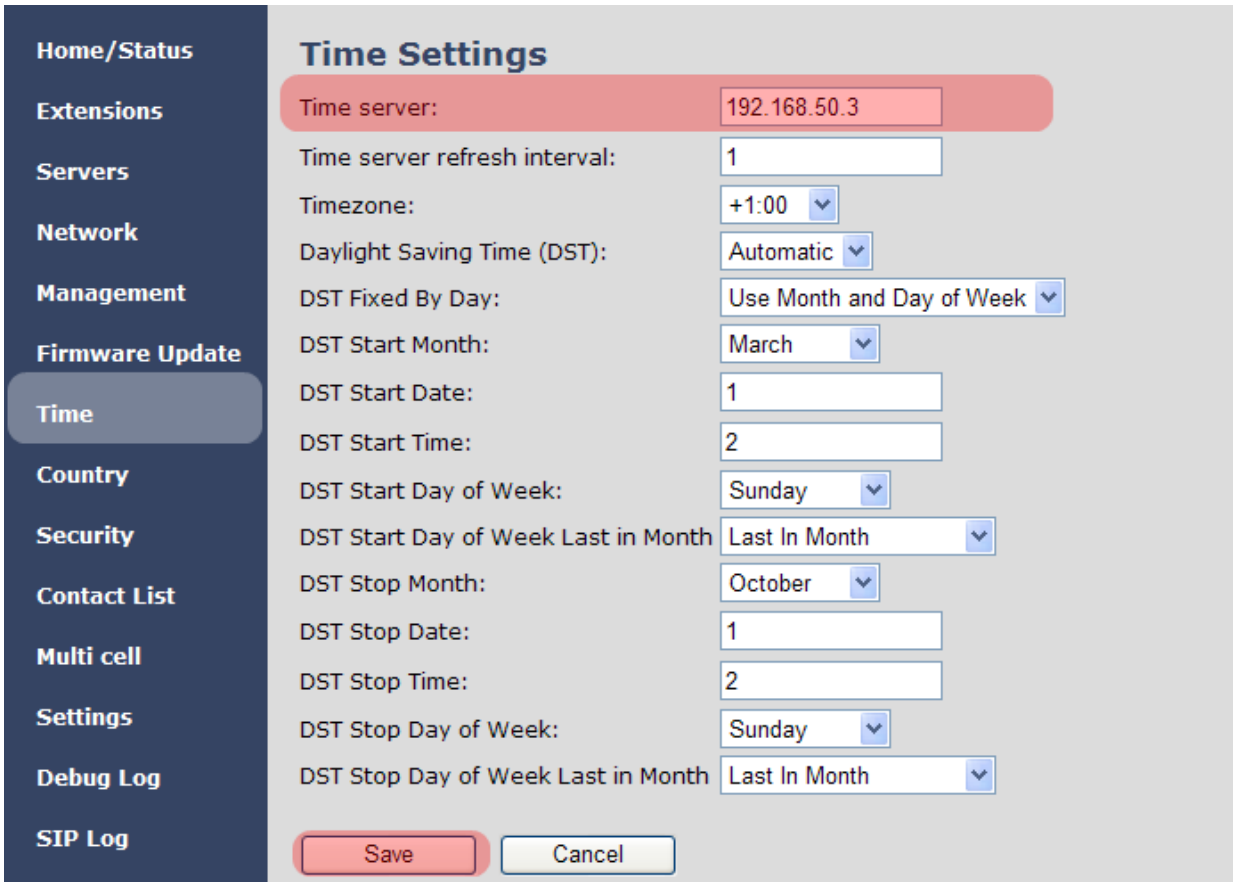
STEP 13 Wait about 3-5 minutes, Reboot the base/gateway.

The base/gateway 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/gateway.

Time Server Setup

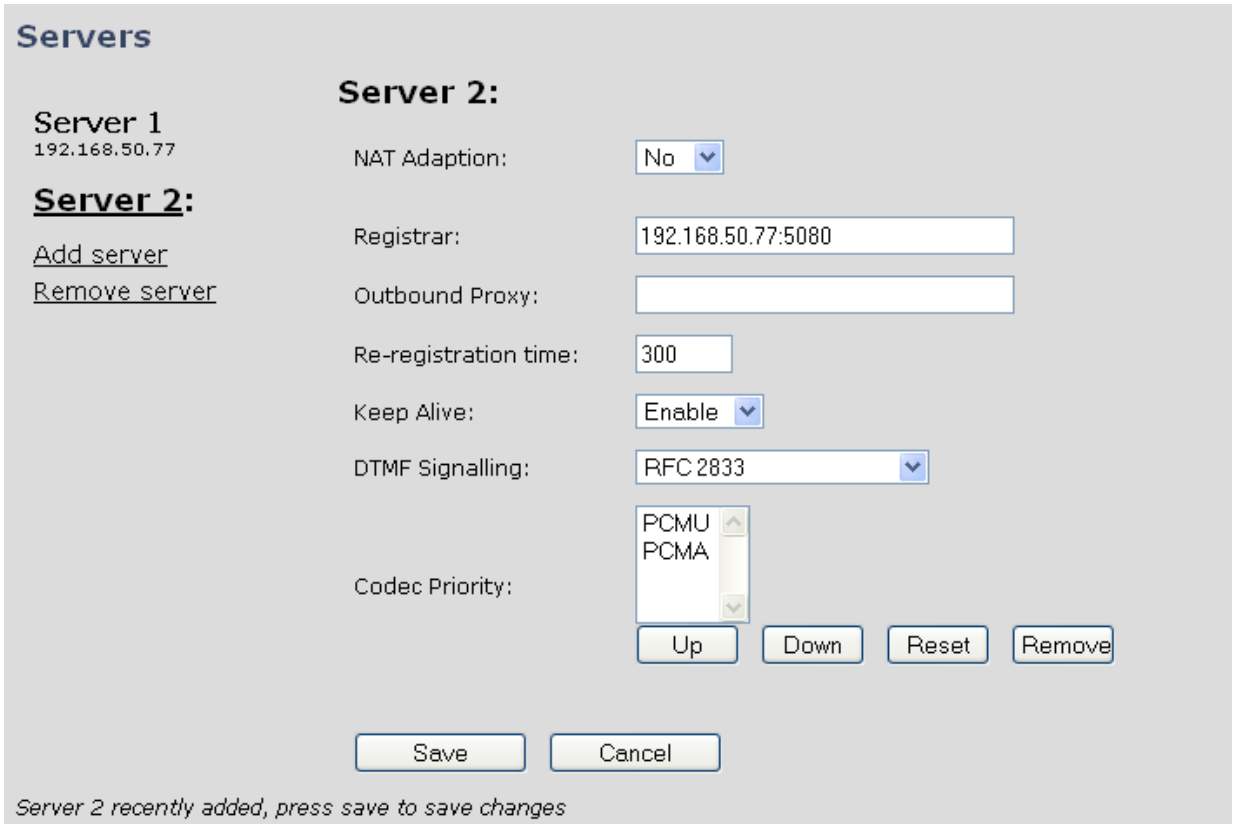
STEP 14 Navigate to the Time settings and configure it. Scroll on the left column and click on **Time** url link to Open the **Time Settings** Page. Enter the relevant parameters on this page and press the **Save** button.
Make sure there is contact to the “Time server” otherwise the Multi-cell feature will not work.



Add a SIP Server

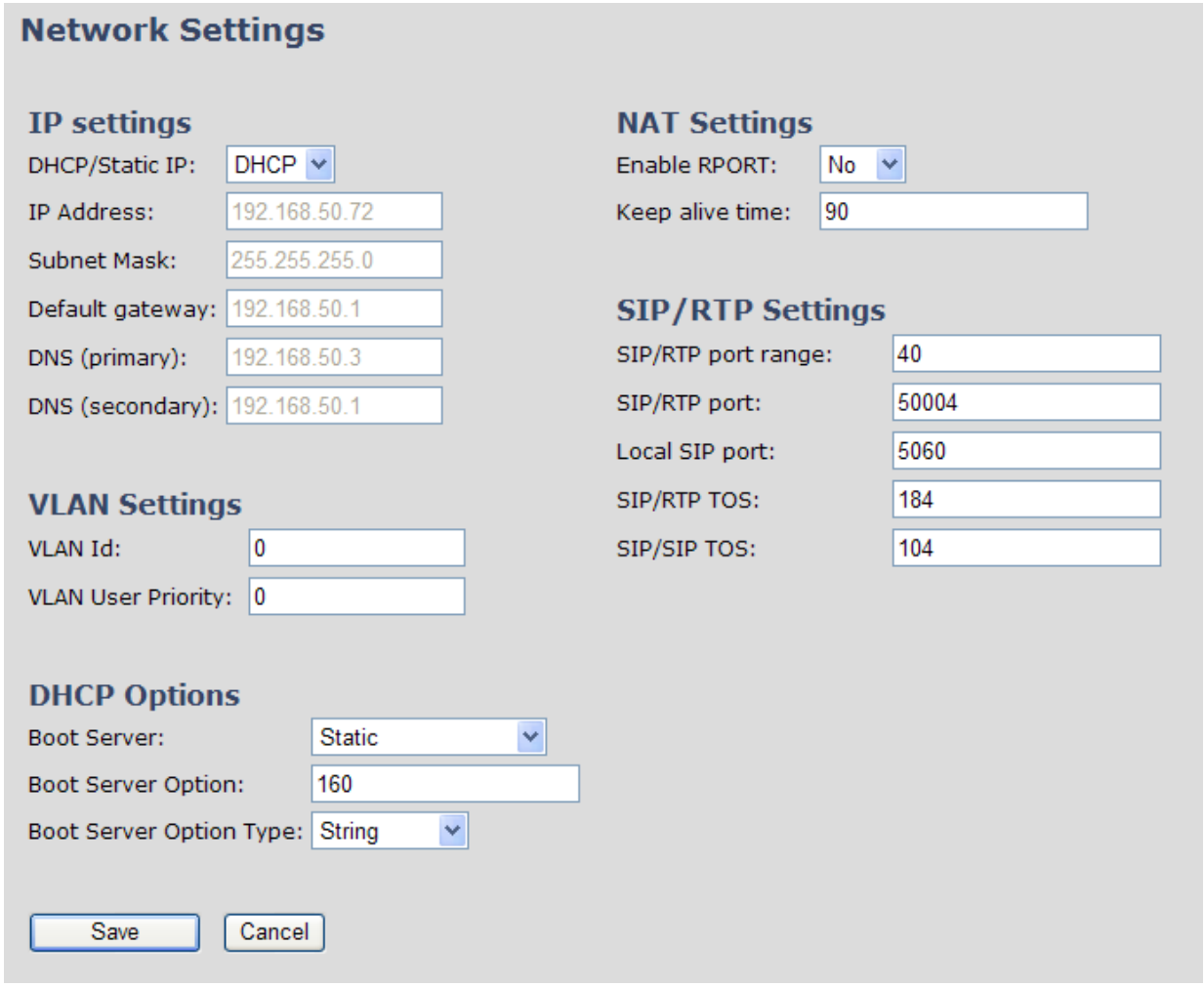
STEP 15 Navigate to the Servers page and Add a server with the following entries and Save:

NAT Adaptation:	No
Registrar:	<SIP-Server-IP-Address>:<Optional-Port##>
Outbound Proxy:	<Empty>
Re-registration time:	300
Other Parameters:	<Use-Default-values>



Configure Gateway Settings

STEP 16 From the "SME VoIP Configuration Interface", navigate to the network option and enter the relevant parameters.



Definition of Network Server Parameters

In this section, we describe the different parameters available in the network configurations menu.

IP Settings

Parameter	Description
DHCP/Static IP	If DHCP is enabled, the device automatically obtains TCP/IP parameters. **Possible value(s):** Static, DHCP. **DHCP:** IP addresses are allocated automatically from a pool of leased address. **Static IP:** IP addresses are manually assigned by the network administrator. If the user chooses DHCP option, the other IP settings or options are not available.
IP Address	32-bit IP address of device (for e.g. base station). 64-bit IP address will be

	supported in the future. **Permitted value(s): AAA.BBB.CCC.DDD**
Subnet Mask	Is device subnet mask. **Permitted value(s): AAA.BBB.CCC.DDD** This is a 32-bit combination used to describe which portion an IP address refers to the subnet and which part refers to the host. A network mask helps users know which portion of the address identifies the network and which portion of the address identifies the node. Class A, B, and C networks have default masks, as shown here: Class A: 255.0.0.0 Class B: 255.255.0.0 Class C: 255.255.255.0
Default Gateway	Device's default network router/switch (32-bit). **Permitted value(s): AAA.BBB.CCC.DDD** for e.g. **192.168.50.0** IP address of network router that acts as entrance to other network. This device usually provides a default route for TCP/IP hosts to use when communicating with other hosts on remote networks.
DNS (Primary)	Main server to which a device directs Domain Name System (DNS) queries. **Permitted value(s): AAA.BBB.CCC.DDD** for e.g. **192.168.50.1** This is the IP address of the server that contains mappings of DNS domain names to various data, for e.g. IP address, etc. The user needs to specify this option when the static IP address option is chosen.
DNS (Secondary)	This is an alternate DNS server.

VLAN Settings

Parameter	Description
VLAN id	Is usually a 12 bit identification of the 802.1Q VLAN. **Permitted value(s):** 0 to 4094 (or FFE in Hex) A VLAN ID of 0 is used to identify priority frames and ID of 4095 (FFF) is reserved. Null means no VLAN tagging or No VLAN discovery through DHCP.
VLAN User Priority	This is a 3 bit value that defines the user priority. **Permitted value(s):** 8 priority levels (i.e. 0 to 7)

DHCP Options

Parameter	Description
Boot Server	**Static:** The network device uses the IP settings configured manually in the boot server through the Network Menu. **Option 66:** This is the option code contained in the client's initial boot file. The network device searches for option 66 (string type) from the response received from the DHCP server.

	Custom: The network device searches for the option number specified by the **Boot Server Option** parameter, and the type specified by the **Boot Server Option Type** parameter (below) in the response received from the DHCP server. **Custom+Option 66:** The 1st choice option for the network device will be to use the custom option if present and the 2nd choice is Option 66 if the custom option is not present. If the DHCP server sends nothing, the following scenarios are possible: • If a boot server value is stored in flash memory and the value is not "0.0.0.0", then the value stored in flash is used. • Otherwise the network device sends out a DHCP INFORM query. - If a single alternate DHCP server responds, this is functionally equivalent to the scenario where the primary DHCP server responds with a valid boot server value. The network device prefers the custom option value over the Option 66 value, but if no custom option is given, the device will use the Option 66 value. - If no alternate DHCP server responds, the INFORM query process will retry and eventually time out. **Permitted value(s):** Static, Option 66, Custom, Custom+Option 66
Boot Server Option	This is a value (usually positive integer) used to explain a DHCP action. When the boot server parameter is set to Custom, this parameter specifies the DHCP option number in which the network device will look for its boot server. **Permitted value(s):** 128 through 254 (Cannot be the same as VLAN ID Option) This parameter should not matter when the Boot server parameter is set.
Boot Server Option Type	This makes it possible for a user to choose some customised Boot Server Option types. These options are customised by the user itself in the configuration file. When the Boot Server parameter is set to Custom, this parameter specifies the type of the DHCP option in which a device should retrieve from its boot server. **Permitted value(s):** IP address, String The IP Address, must specify the boot server. The String can be URL, FTP, TFTP, HTTPS, etc. The address can be followed by optional directory.

NAT Provisioning

These are some definitions of NAT settings:

Parameter	Description
STUN Servers	Name or IP address of router that implements STUN through NAT **Permitted values:** 32-bit IP address or URL
STUN bindtime guard	When STUN is enabled, it specifies a value in seconds of how often a system will guard the NAT bindings OR a STUN binding request from client is used to discover the presence of NAT router(s). Guarding for NAT bindings helps the system to react properly if for e.g. the NAT device has been reset. If this value is disabled (i.e. set to 0), no guarding will be made. **Permitted value(s):** Positive integer, units in seconds. Default is 80.
STUN bindtime determine	When STUN is enabled and **STUN bindtime guard** is defined, setting this parameter to 1 compels the system to automatically determine the duration of NAT bindings in the system. **STUN bindtime guard** usually defines the initial test duration. **Permitted value(s):** No=disabled, Yes=Enabled (default)
Enable RPORT	Specifies whether RPORT should be used in SIP messages. Generally RPORT allows SIP responses to request over UDP be returned to the

	source address and to a specific port when the Base station is behind the Network Address Translator. **Permitted value(s):** No=disabled, Yes=Enabled (default)
Enable STUN	Allows network devices and/or applications to discover the presence and types of firewalls between them and the public internet. **Permitted value(s):** No=disabled, Yes=Enabled (default).
Keep alive time	When enabled, it defines the time in seconds how frequent keep-alives are forwarded to keep NAT bindings. For e.g. if SIP_STUN_BINDTIME_DETERMINE is set to 1, SIP_STUN_KEEP_ALIVE_TIME will be overruled and keep alives will be sent with a frequency of half of determined bindtime. This numerical value is set to force endpoints to re-register after a specific window time. **Permitted values:** Positive integer, units in seconds, default is 90.

SIP/RTP Settings

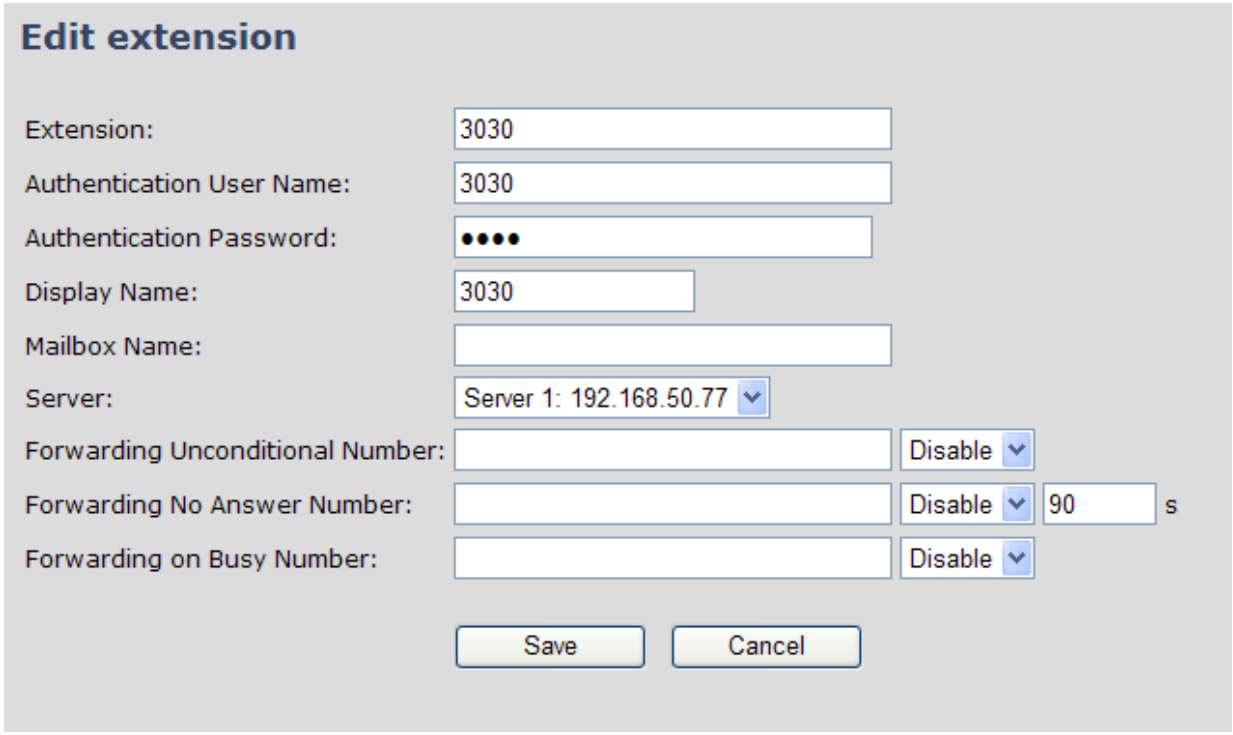
These are some definitions of SIP/RTP Server settings:

Parameter	Description
SIP/RTP port range	The number of ports that can be used for RTP audio streaming. **Permitted values:** Positive integers, default is 20.
SIP/RTP port	Usually the first RTP port to use for RTP audio streaming. **Permitted values:** Port number default 5004 or 50004 (depending on the setup).
Local SIP port	Port used for first user agent (UA) instance. Succeeding UA's will get succeeding ports. **Permitted values:** Port number default 5060.
SIP/RTP TOS	Priority of RTP traffic based on the IP layer ToS (Type of Service) byte. See RFC 1349 for details. “cost bit" is not supported. o Bit 7..5 defines precedence. o Bit 4..2 defines Type of Service. o Bit 1..0 are ignored. Setting all three of bit 4..2 will be ignored. **Permitted values:** Positive integer default is 0.
SIP/SIP TOS	Priority of SIP call control signalling traffic based on the IP layer Type of Service (ToS) byte. **Permitted values:** Positive integers

Register Handsets

STEP 17 Next, navigate to the Extensions page and add the relevant extension(s) to the SIP Server configured in the following manner:

Parameter	Description
Extension	Handset phone number or SIP username depending on the setup. **Possible value(s):** 8-bit string. **Example: 1024, etc.** **Note:** The Extension must also be configured in SIP server in order for this feature to function.
Authentication User Name/ Password	**Username:** SIP authentication username . **Password:** SIP authentication password. **Permitted value(s):** 8-bit string.
Display Name	Human readable name used for reference purposes on the HTTP web interface.(Usually does not display on handset). **Permitted value(s): 8-bit string.**
Mailbox Name/ Number	Name of centralised system used to store phone voice messages that can be retrieved by recipient at a later time. **Valid Input(s):** 8-bit string character (Latin characters for the **Name** and positive integer for the **Number**).
Server	DNS or IP address of SIP server or Server of SME VoIP Service provider. **Valid Input(s): AAA.BBB.CCC.DDD.**
Forwarding Unconditional Number	Number to which incoming calls must be re-routed to irrespective of the current state of the SIP node or handset. **Note:** Feature must be enabled in the SIP server before it can function in the Network.
Forwarding No Answer Number	Number to which incoming calls must be re-routed to when there is no response from the SIP end node. **Note:** Feature must be enabled in the SIP server before it can function in the Network.
Forwarding On Busy Number	Number to which incoming calls must be re-routed to when SIP node is busy. **Note:** Feature must be enabled in the SIP server before it can function in the Network.



STEP 18 Register the handset via navigating to the Extensions page > Click on the relevant <SIP Server > Check the relevant Extensions > Click on Register Handset(s) to initiate the process of location registration at SIP server.