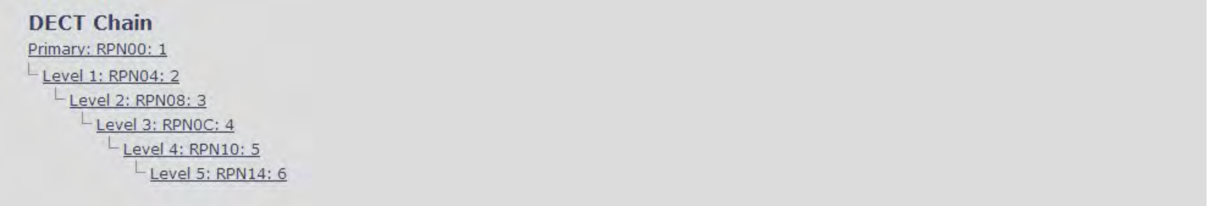
	Searching: Base unit in the process of locating to a Master/slave as specified in DECT sync source **Free Running:** A locked Base unit that suddenly lost synchronization to the Master. **Unknown:** No current connection information from specific Base unit **Assisted lock:** Base has lost DECT sync. source and Ethernet is used for synchronization **Sync. Lost:** Handset has an active DECT connection with the base. But the base has lost DECT sync. source connection. The base will stay working as long as the call is active and will go into searching mode when call is stopped.
BASE STATION NAME	Name from management settings.

5.12.5 DECT Chain

Below the “Base station Group” table is the DECT Chain tree. The DECT Chain tree is a graphical presentation of the Base Group table levels and connections. Repeaters are shown with green highlight.

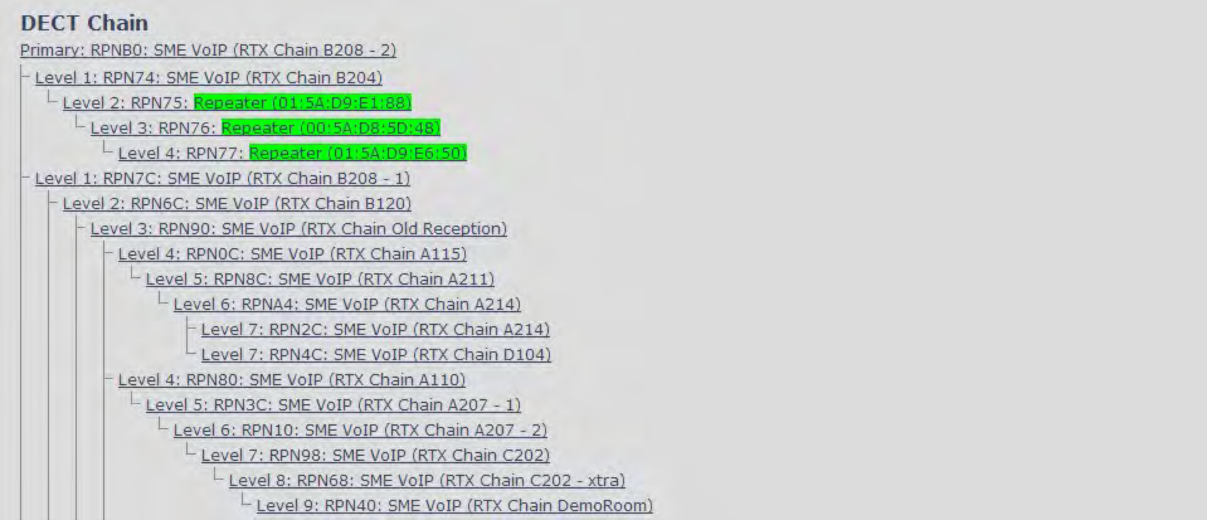
Screenshot: DECT Chain tree of above configuration



DECT Chain

```
Primary: RPN00: 1
└ Level 1: RPN04: 2
   └ Level 2: RPN08: 3
      └ Level 3: RPN0C: 4
         └ Level 4: RPN10: 5
            └ Level 5: RPN14: 6
```

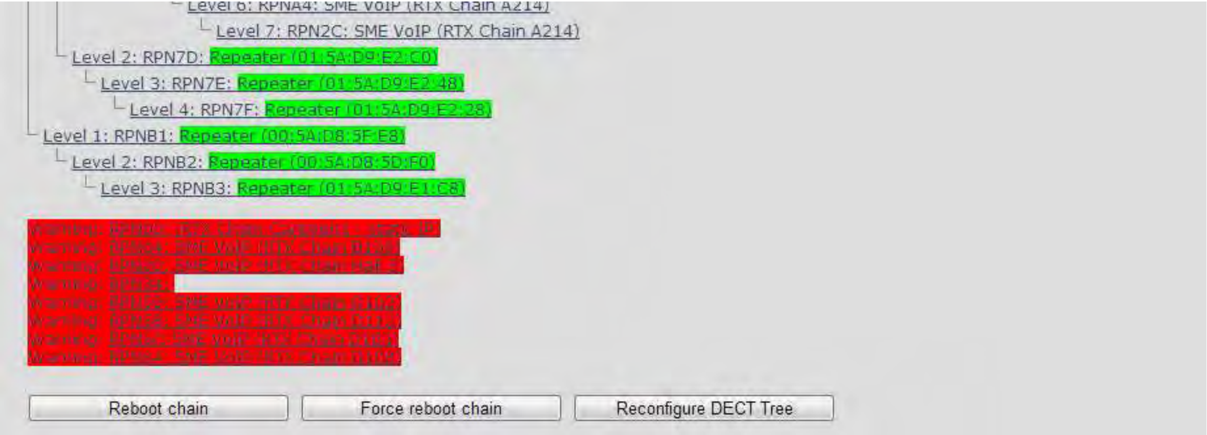
Screenshot: Example of part of DECT Chain tree with repeaters



DECT Chain

```
Primary: RPNB0: SME VoIP (RTX Chain B208 - 2)
├ Level 1: RPN74: SME VoIP (RTX Chain B204)
│  └ Level 2: RPN75: Repeater (01:5A:D9:E1:88)
│     └ Level 3: RPN76: Repeater (00:5A:D8:5D:48)
│        └ Level 4: RPN77: Repeater (01:5A:D9:E6:50)
├ Level 1: RPN7C: SME VoIP (RTX Chain B208 - 1)
│  ├ Level 2: RPN6C: SME VoIP (RTX Chain B120)
│  │  ├ Level 3: RPN90: SME VoIP (RTX Chain Old Reception)
│  │  │  ├ Level 4: RPN0C: SME VoIP (RTX Chain A115)
│  │  │  │  └ Level 5: RPN8C: SME VoIP (RTX Chain A211)
│  │  │  │     └ Level 6: RPNA4: SME VoIP (RTX Chain A214)
│  │  │  │        ├ Level 7: RPN2C: SME VoIP (RTX Chain A214)
│  │  │  │        └ Level 7: RPN4C: SME VoIP (RTX Chain D104)
│  │  │  ├ Level 4: RPN80: SME VoIP (RTX Chain A110)
│  │  │  │  └ Level 5: RPN3C: SME VoIP (RTX Chain A207 - 1)
│  │  │  │     └ Level 6: RPN10: SME VoIP (RTX Chain A207 - 2)
│  │  │  │        └ Level 7: RPN98: SME VoIP (RTX Chain C202)
│  │  │  │           └ Level 8: RPN68: SME VoIP (RTX Chain C202 - xtra)
│  │  │  │              └ Level 9: RPN40: SME VoIP (RTX Chain DemoRoom)
```

Screenshot: Example of part of DECT Chain tree with units in Base Group but not in tree by various reasons.



Level 6: RPNA4: SME VoIP (RTX Chain A214)
Level 7: RPN2C: SME VoIP (RTX Chain A214)
Level 2: RPN7D: Repeater (01:5A:D9:E2:C0)
Level 3: RPN7E: Repeater (01:5A:D9:E2:48)
Level 4: RPN7F: Repeater (01:5A:D9:E2:28)
Level 1: RPNB1: Repeater (00:5A:D8:5F:E8)
Level 2: RPNB2: Repeater (00:5A:D8:5D:F0)
Level 3: RPNB3: Repeater (01:5A:D9:E1:C8)

Warning: [illegible]
Warning: [illegible]
Warning: [illegible]
Warning: [illegible]
Warning: [illegible]
Warning: [illegible]
Warning: [illegible]
Warning: [illegible]

When a base or repeater has not joined the tree, it will be shown with read background below the tree.

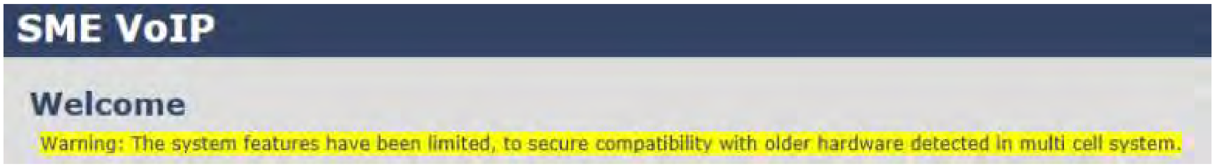
5.12.6 RTX8660 -Rove B4 Mixed mode

Rove B4 Base station can be added to existing systems using RTX8660 Base station. Even though the two base stations will be able to co-exist in the same Multi cell setup, the system will be set to some limitations. This means that the Multi cell will disable the features of Rove B4, that are not supported by RTX8660, and run on mixed mode but with limited to RTX8660 features.

NOTE: LAN SYNC will not work in mixed mode.
NOTE: RTX8660 cannot be added to an existing Rove B4 Multi-cell. Only Rove B4 can join an RTX8660 system.

The system will display a warning message on the Home/Status page.

Screenshot:



SME VoIP

Welcome

Warning: The system features have been limited, to secure compatibility with older hardware detected in multi cell system.

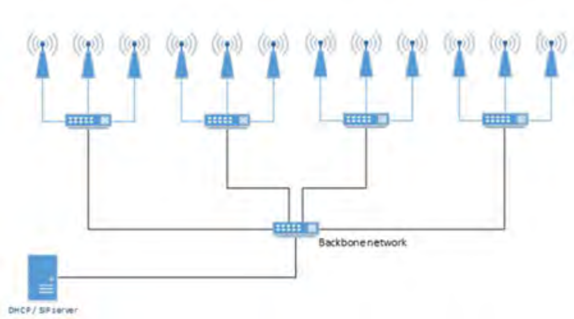
5.13 LAN SYNC

Apart from the DECT Over-the-air solution, the LAN SYNC provides an alternative option for base synchronization. The reason thereof is to allow a larger coverage of installations where the bases cannot see each other. This means that the LAN sync feature, specified by the IEEE1588 standard, will handle the synchronization over the network, instead of Over-the-Air.

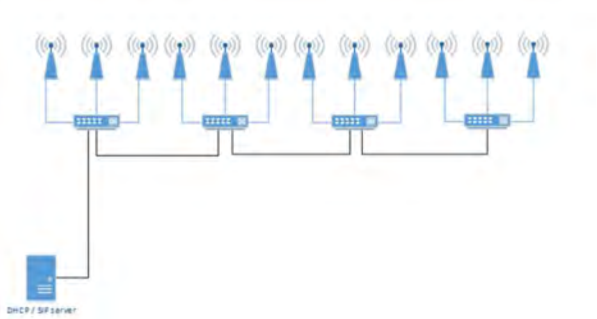
NOTE: To join 2 or more Base stations in a Multi Cell system you need to have one handset added to the system. For details and Step-by-Step guide to Multi Cell setup, please see Appendix.

In this section, we describe the other parameters available in the Multi-cell environment, namely the LAN SYNC menu. However, before stepping into the configuration details, the user must consider the following network requirements in order to minimize the impact from other devices on the network:

- A Maximum number of 3 cascaded Ethernet switches are supported between the Sync Master (SM) and a Sync Slave (SS) base stations.
- Only switches, which fulfill the requirements regarding Ethernet synchronization according to IEEE1588, are recommended and officially supported.
- All base stations must be connected to a dedicated DECT VLAN.
- The DECT VLAN must be configured to the highest priority in all switches that is connected to the DECT infrastructure.
- The backbone network load should not exceed 50 percent of the total link capacity.
- The Ethernet switch must be able to use DSCP as QoS parameter.
- The network must support multicast datagrams from IEEE1588.



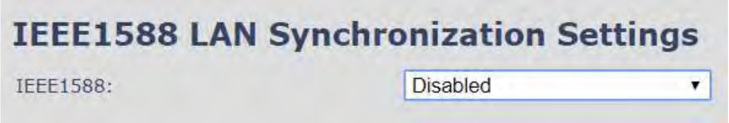
Good network topology



Bad network topology

5.13.1 LAN sync feature

The initial port of the page provides the option to enable / disable the feature for the device



IEEE1588 LAN Synchronization Settings

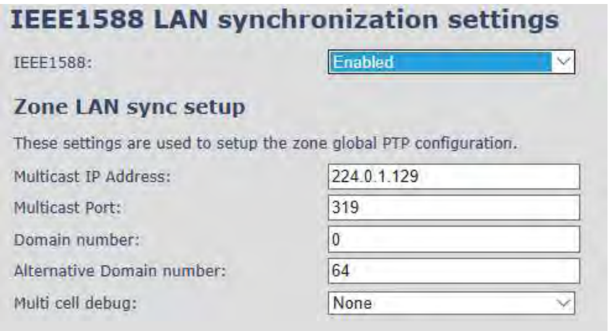
IEEE1588: Disabled ▾

PARAMETERS	DEFAULT VALUES	DESCRIPTION
IEEE1588	Disabled	The initial port of the page provides the option to enable / disable the feature for the device

5.13.2 Zone LAN sync setup

This part of the page covers the global configuration of the synchronization zone. Description of Settings for Specific Base units is as follows:

Screenshot:



IEEE1588 LAN synchronization settings

IEEE1588: Enabled

Zone LAN sync setup

These settings are used to setup the zone global PTP configuration.

Multicast IP Address: 224.0.1.129

Multicast Port: 319

Domain number: 0

Alternative Domain number: 64

Multi cell debug: None

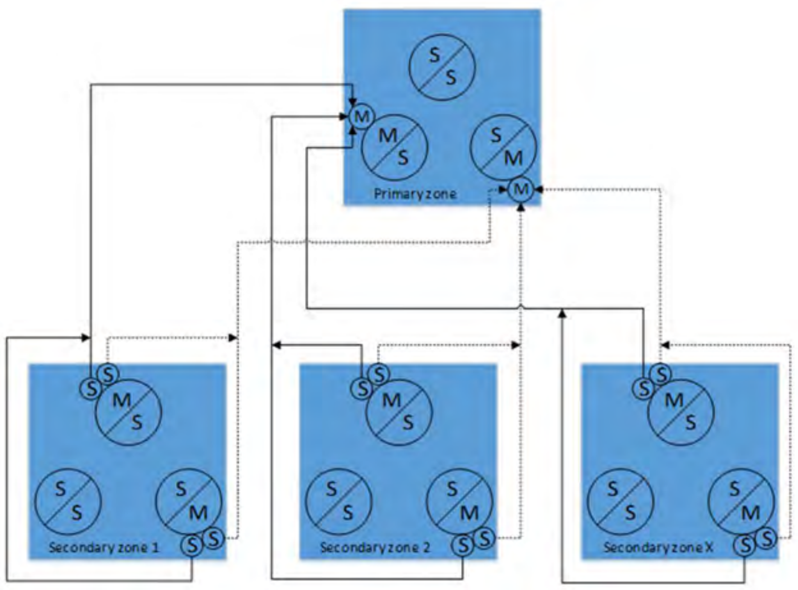
PARAMETERS	DEFAULT VALUES	DESCRIPTION
MULTICAST IP ADDRESS	224.0.1.129	This setting defines the IP address where to listen for IEEE1588 PTP packages IP address of the multicast group. The IP address must start with 224.0.xx.xx and this cannot be changed. To be compliant with IEEE1588, this port must be default value. Before setup, make sure no other devices are using the given IP. **NOTE:** This should only be changed in case other IEEE1588 equipment is on the network and using this specific IP address.
MULTICAST PORT	319	Define the port which the system will communicate on To be compliant with IEEE1588, this port must be default value. **NOTE:** This should only be changed in case other IEEE1588 equipment is on the network and using this specific port.
DOMAIN NUMBER	0	Domain number is used to set to which domain this specific Base station belongs to. Valid input: 0-127
ALTERNATIVE DOMAIN NUMBER	64	Alternative domain is only used in case the primary sync source from the main domain fails. If so, the Base station will sync with the alternative domain. It must NOT have the same value as the domain number. Valid input: 0-127
MULTI CELL DEBUG MODE	None	Enable this feature, if you want the system to catalogue low level multi-cell debug information or traces. Options: **Data Sync:** Writes header information for all packets received and sent to be used to debug any special issues. Generates LOTS of SysLog signaling and is only recommended to enable shortly when debugging. **Auto Tree:** Writes states and data related to the Auto Tree Configuration feature. **Both:** Both Data Sync and Auto Tree are enabled. **IEEE1588 Debug:** Writes IEEE1588 debug information to the syslog

		NOTE: Must only be used for debug purpose and not enabled on a normal running system

5.13.3 External LAN sync setup

The “External LAN sync setup” covers the configuration of an external synchronization. This means that, in order to support more than 250 Base stations in a system, it is necessary to use multi-level synchronization.

In multi-level synchronization, a primary zone is defined which is used by the other secondary zones in the system as synchronization source. Please see the figure below:



The primary and alternative sync source in each secondary zone, will be connected to the primary zone to ensure redundancy. When using this configuration, each secondary zone will cause a load to the primary zone as two base stations and this must be accounted for when configuring the primary zone. Therefore, it is recommended that the number of base stations in the primary zone is kept as low as possible, but it must as minimum contain 3 base stations to ensure redundancy.

To minimize synchronization jitter between each secondary zone, it is important that the network path between the primary zone and its secondary zones is as equal as possible. Therefore, the primary zone must be connected to the network switch which forms the top node in the switching tree. In a good network topology example, as the one mentioned in the beginning of the subchapter, this will be the switch where the DHCP server is connected.

The table below displays the available settings for configuring a Multi-Level synchronization.

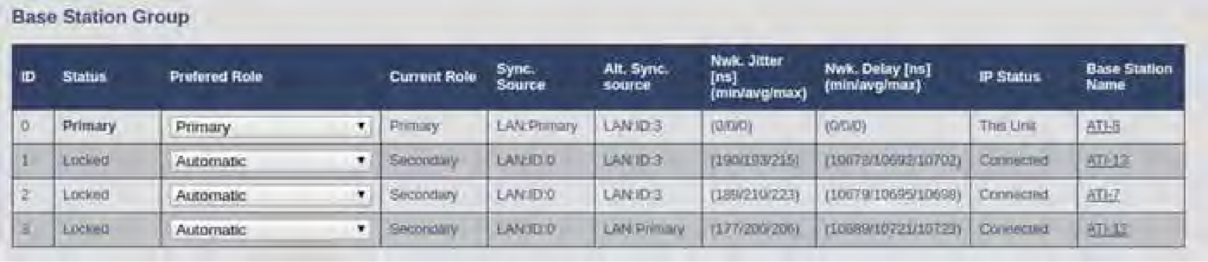
PARAMETERS	DEFAULT VALUES	DESCRIPTION
EXTERNAL SYNC	Disabled	To have external LAN synchronization, enable the feature by choosing one of the options below: **Primary zone configuration** **Secondary zone configuration**
MULTICAST IP ADDRESS	224.0.1.129	In order to listen for IEEE1588 PTP packages, the IP address should be defined The IP address must start with 224.0.xx.xx and this cannot be changed.

		To be compliant with IEEE1588, this port must be default value. Before setup, make sure no other devices are using the given IP. **NOTE:** This should only be changed in case other IEEE1588 equipment is on the network and using this specific IP address.
MULTICAST PORT	319	Define the port which the system will listen for IEEE1588 PTP messages To be compliant with IEEE1588, this port must be default value. **NOTE:** This should only be changed in case other IEEE1588 equipment is on the network and using this specific port.
DOMAIN NUMBER	1	The domain number is a preferred method to divide the IEEE1588 PTP messages into zones in IEEE 1588-2008. **Note:** The input must NOT be the same as the one used in the previous feature “Zone LAN sync setup”
ALTERNATIVE DOMAIN NUMBER	65	Alternative domain is only used in case the primary sync source from the main domain fails. If so, the base station will sync with the alternative domain. **Note:** The input must NOT have the same value as the “Domain number” from the previous parameter and must NOT be used in the “Zone LAN sync setup” feature.

5.13.4 Base station group

The Base station group lists various parameter settings for the Base stations and allows the user to check the status information for the whole system.

Screenshot:



Base Station Group

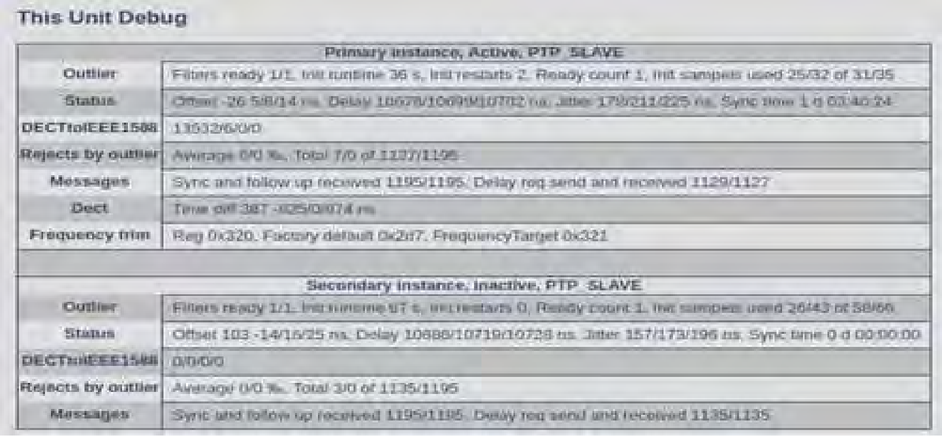
ID	Status	Prefered Role	Current Role	Sync. Source	Alt. Sync. source	Nwk. Jitter [ns] (min/avg/max)	Nwk. Delay [ns] (min/avg/max)	IP Status	Base Station Name
0	Primary	Primary	Primary	LAN:Primary	LAN:ID:3	(0/0/0)	(0/0/0)	This Unit	ATI-5
1	Locked	Automatic	Secondary	LAN:ID:0	LAN:ID:3	(190/193/215)	(10673/10692/10702)	Connected	ATI-12
2	Locked	Automatic	Secondary	LAN:ID:0	LAN:ID:3	(189/210/223)	(10679/10695/10698)	Connected	ATI-7
3	Locked	Automatic	Secondary	LAN:ID:0	LAN:Primary	(177/200/206)	(10689/10721/10723)	Connected	ATI-12

PARAMETERS	DESCRIPTION
ID	Base unit identity in the chained network. **Permitted Output:** Positive Integers
STATUS	Base station characteristics in connection to the current Multi cell network. Possible Output(s) **Primary:** Main Base station into which all other nodes in the chain synchronize to. **Locked:** The Base unit is currently synchronized and locked to the master Base unit. **Searching:** Base unit in the process of locating a Master/Slave as specified in DECT sync source **Free Running:** IEEE master is found, and is DECT synchronizing
PREFERED ROLE	**Disabled:** Disable the feature **Primary:** The Base station that is used for main sync; only one primary is allowed to the system **NOTE:** It is recommended to use Base stations that are closer to the backbone as primary **Secondary:** Base stations that will never be selected as primary. They become slaves **Automatic:** System finds primary sync source – it allows the system to decide the role of the base **Alt. Primary:** Backup for primary Base station in case it fails; only one redundant sync. master is allowed in the system

CURRENT ROLE	The current role of the Base station
SYNC SOURCE	Shows to which Base station this specific device is synchronized and indicates if it is via LAN or DECT
ALT. SYNC SOURCE	Alternative sync source in case main sync source fails
NWK JITTER [NS] (MIN/AVG/MAX)	Measures how the IEEE1588 packets are received, the lower the Jitter is the better **Max:** Displays the maximum jitter Average between primary and slave **Min:** Displays the minimum jitter Average between primary and slave **Average:** Displays the average jitter between primary and slave
MWK DELAY [NS] (MIN/AVG/MAX)	Measures the time it takes an IEEE packet to travel from Primary to Slave Base station in ns. **Max:** Displays the maximum delay Average between primary and slave **Min:** Displays the minimum delay Average between primary and slave **Average:** Displays the average delay between primary and slave
IP STATUS	Current Base station behavior in the SME network. Possible Outputs **Connected:** The relevant Base station(s) is online and connected to the network **Connection Loss:** Base station unexpectedly lost connection to network **This Unit:** Current Base station whose http Web Interface is currently being accessed
BASE STATION NAME	Name from management settings.

5.13.5 This unit debug

Screenshot:



This Unit Debug

Primary instance, Active, PTP_SLAVE	
Outlier	Filters ready 1/1, Init runtime 36 s, Init restarts 2, Ready count 1, Init samples used 25/32 of 31/35
Status	Offset -26 5/8/14 ns, Delay 10678/10691/10702 ns, Jitter 179/211/225 ns, Sync time 1 d 03:40:24
DECTtoIEEE1588	13532/6/0/0
Rejects by outlier	Average 0/0 %, Total 7/0 of 1127/1196
Messages	Sync and follow up received 1195/1195, Delay req send and received 1129/1127
Dect	Time diff 387 -825/0/874 ns
Frequency trim	Reg 0x320, Factory default 0x2d7, FrequencyTarget 0x321

Secondary instance, inactive, PTP_SLAVE	
Outlier	Filters ready 1/1, Init runtime 57 s, Init restarts 0, Ready count 1, Init samples used 26/43 of 58/66
Status	Offset 103 -14/16/25 ns, Delay 10688/10719/10728 ns, Jitter 157/173/196 ns, Sync time 0 d 00:00:00
DECTtoIEEE1588	0/0/0/0
Rejects by outlier	Average 0/0 %, Total 3/0 of 1135/1195
Messages	Sync and follow up received 1195/1195, Delay req send and received 1135/1135

Debug information is used only by RTX to debug IEEE1588 network issues.

In case debug is needed, send this information to RTX support team.

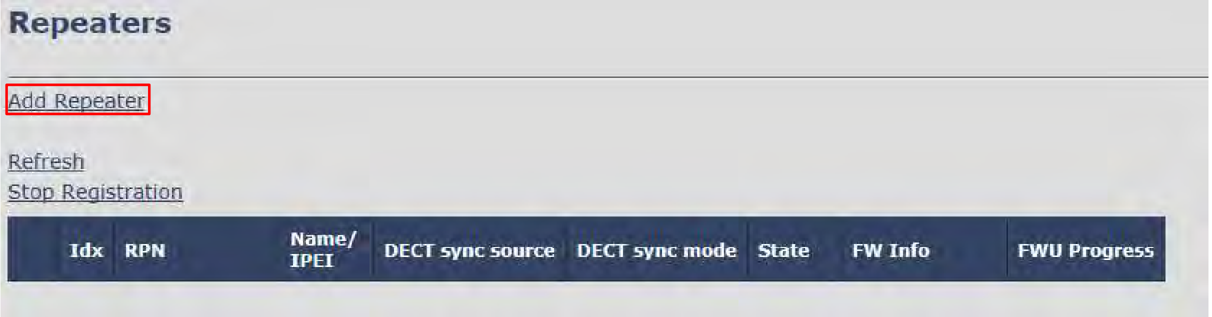
5.14 Repeaters

Within this section we describe the repeater parameter, and how to operate the repeater.

5.14.1 Add repeater

Before registering a repeater to the system, the user first needs to add it. To do so, select **Add Repeater** from the repeater's web menu and fill in the data defined by the table below

Screenshot



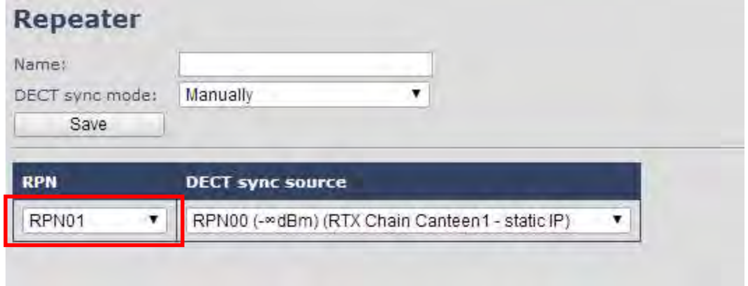
Repeaters

PARAMETERS	DESCRIPTION
NAME	Repeater name. If no name specified, the field will be empty
DECT SYNC MODE	**Manually:** User controlled by manually assign "Repeater RPN" and "DECT sync source RPN" **Local Automatic:** Repeater controlled by auto detects best base signal and auto assign RPN.

5.14.1.1 Manually

User controlled by manually assigning "Repeater RPN" and "DECT sync source RPN". The parameters are selected from the drop-down menu.

Screenshot



Repeater

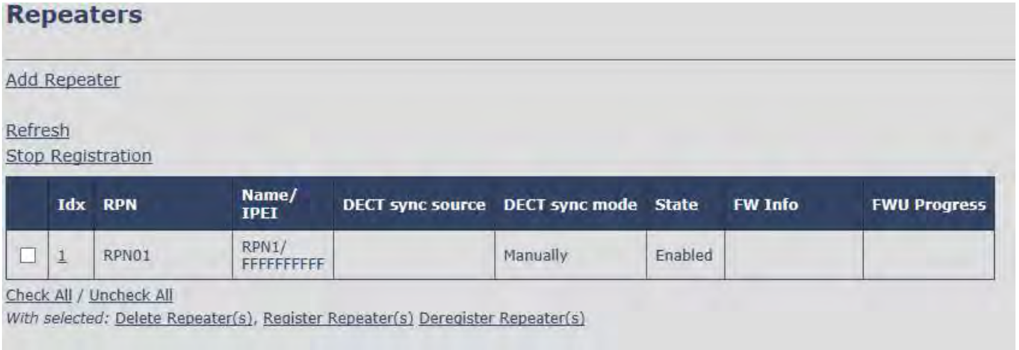
Name:

DECT sync mode: Manually

RPN	DECT sync source
RPN01	RPN00 (-∞dBm) (RTX Chain Canteen1 - static IP)

After saving the configurations above, the information and status of the repeater will be visible on the main **Repeaters** page (please see the image below).

Screenshot



Repeaters

Add Repeater

Refresh
Stop Registration

	Idx	RPN	Name/ IPEI	DECT sync source	DECT sync mode	State	FW Info	FWU Progress
□	1	RPN01	RPN1/ FFFFFFFFFF		Manually	Enabled		

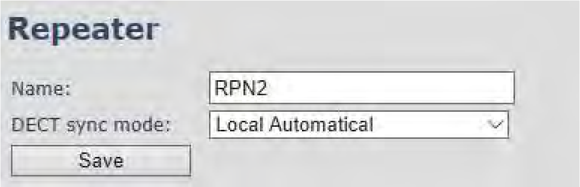
Check All / Uncheck All
With selected: Delete Repeater(s), Register Repeater(s) Deregister Repeater(s)

Good practice when adding repeaters to a Multi Cell system is to use manually registration, because then you can control which Base station the repeater(s) connect to.

5.14.1.2 Local Automatical

Repeater controlled by auto detects best base signal and auto assign RPN. The RPN and DECT sync source are greyed out.

Screenshot



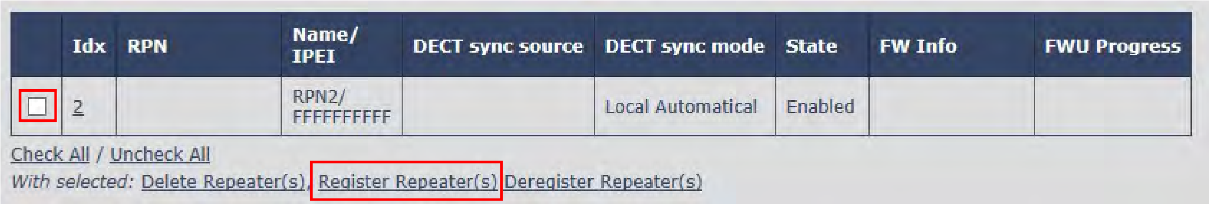
Repeater

Name:	RPN2
DECT sync mode:	Local Automatical

The repeater RPN is dynamic assigned in base RPN range.
With local automatic mode repeater on repeater (chain) is not supported.

5.14.2 Register Repeater

Adding a repeater makes it possible to register the repeater. Registration is made by selecting the repeater and pressing **Register repeater**. The base window for repeater registration will be open until the registration is stopped. By stopping the registration, all registration on the system will be stopped including handset registration.

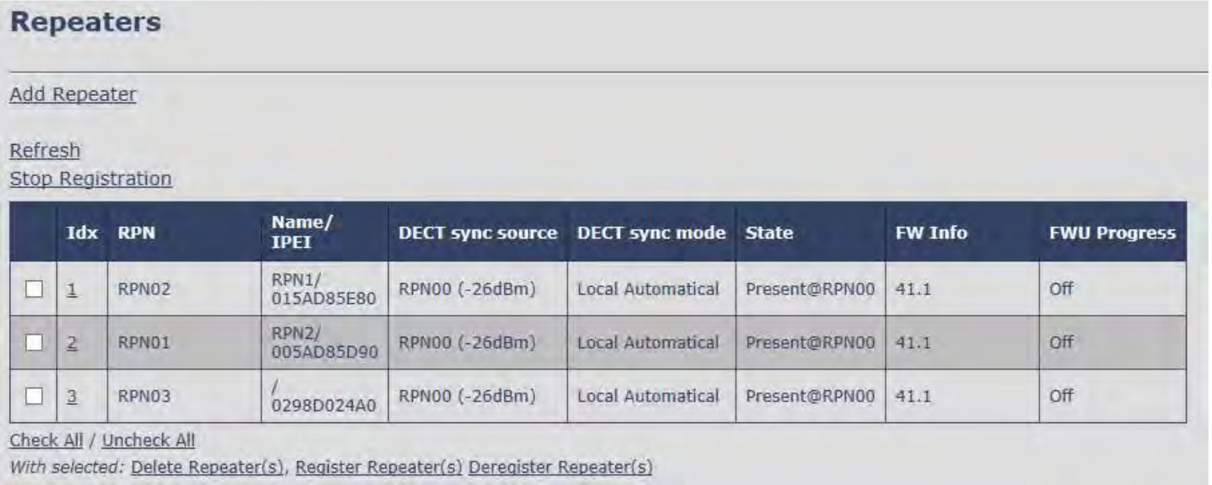


	Idx	RPN	Name/ IPEI	DECT sync source	DECT sync mode	State	FW Info	FWU Progress
□	2		RPN2/ FFFFFFFFFF		Local Automatical	Enabled		

Check All / Uncheck All
With selected: Delete Repeater(s), Register Repeater(s) Deregister Repeater(s)

5.14.3 Repeaters list

Screenshot



Repeaters

Add Repeater

Refresh
Stop Registration

	Idx	RPN	Name/ IPEI	DECT sync source	DECT sync mode	State	FW Info	FWU Progress
□	1	RPN02	RPN1/ 015AD85E80	RPN00 (-26dBm)	Local Automatical	Present@RPN00	41.1	Off
□	2	RPN01	RPN2/ 005AD85D90	RPN00 (-26dBm)	Local Automatical	Present@RPN00	41.1	Off
□	3	RPN03	/ 0298D024A0	RPN00 (-26dBm)	Local Automatical	Present@RPN00	41.1	Off

Check All / Uncheck All
With selected: Delete Repeater(s), Register Repeater(s) Deregister Repeater(s)

The number of repeaters allowed on each Base station is defined on the Multi cell page.
System combination: 50/3 – 127/1 -254/0 (please visit chapter 5.12.3 for more details).
If the system combination is set to 127/1 or 254/0, you can still register more than one repeater, but it will not get a DECT Sync source and will have no function.

Example:
System combination 50/3:
Base stations are named RPN00 – RPN04 – RPN08. Etc. jumping 4 numbers each time (HEX numbers)
Repeaters connect to Base station RPN00 will be called RPN01 – RPN02 – RPN03 (HEX numbers)
Repeaters connect to Base station RPN04 will be called RPN05 – RPN06 – RPN07 (HEX numbers)
Etc.

System combination 127/1:
Base stations are named RPN00 – RPN02 – RPN04. Etc. jumping 2 numbers each time (HEX numbers)
Repeaters connect to Base station RPN00 will be called RPN01 (HEX numbers)
Repeaters connect to Base station RPN02 will be called RPN05 (HEX numbers)
Etc.

System combination 254/0:
Repeater registration not possible

PARAMETERS	DESCRIPTION
IDX	Repeater unit identity in the chained network. **Permitted Output:** Positive Integers
RPN	The Radio Fixed Part Number is an 8-bit DECT cell identity allocated by the installer. The allocated RPN within the SME must be geographically unique. **Permitted Output:** 0 to 255 (DEC) **OR** 0x00 to 0xFF (HEX)
NAME/IPEI	Contains the name and the unique DECT serial number of the repeater. If name is given the field will be empty.
DECT SYNC SOURCE	The “multi cell chain” connection to the specific Base/repeater unit. Maximum number of chain levels is 12. Sync. source format: “RPNyy (-zz dBm)” yy: RPN of source zz: RSSI level seen from the actual repeater
DECT SYNC MODE	**Manually:** User controlled by manually assign “Repeater RPN” and “DECT sync source RPN”

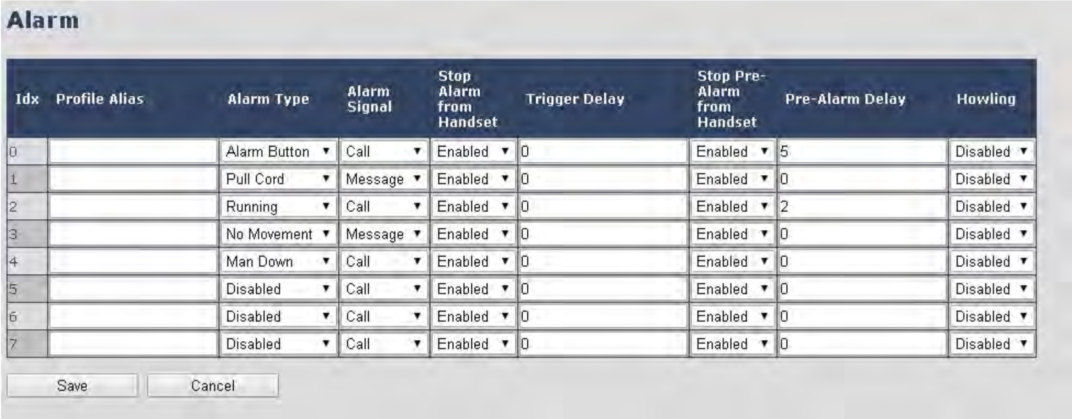
	Local Automatical: Repeater controlled by auto detects best base signal and auto assign RPN. **Chaining Automatical:** Base controlled by auto detects best base or repeater signal and auto assign RPN. This feature will be supported in a future version
STATE	Present@unit means connected to unit with RPN yy
FW INFO	Firmware version
FWU PROGRESS	Possible FWU progress states: **Off:** Means sw version is specified to 0 = fwu is off **Initializing:** Means FWU is starting and progress is 0%. **X% :** FWU ongoing **Verifying X%:** FWU writing is done and now verifying before swap ”**Conn. term. wait**” (Repeater): All FWU is complete and is now waiting for connections to stop before repeater restart. Complete HS/repeater: FWU complete **Error:** Not able to fwu e.g. file not found, file not valid etc.

For detailed description on how to operate repeaters please ask RTX support for the “How to register repeaters” guide.

5.15 Alarm

In the Alarm Settings menu, it is controlled how an alarm appears on the handset. For example, if the handset detects “Man Down”, then it is defined in this menu what alarm signal this type of alarm will send out and if a pre-alarm shall be signaled etc. The Alarm is activated by a long press on the Alarm key (3 sec).

Screenshot



Idx	Profile Alias	Alarm Type	Alarm Signal	Stop Alarm from Handset	Trigger Delay	Stop Pre-Alarm from Handset	Pre-Alarm Delay	Howling
0		Alarm Button	Call	Enabled	0	Enabled	5	Disabled
1		Pull Cord	Message	Enabled	0	Enabled	0	Disabled
2		Running	Call	Enabled	0	Enabled	2	Disabled
3		No Movement	Message	Enabled	0	Enabled	0	Disabled
4		Man Down	Call	Enabled	0	Enabled	0	Disabled
5		Disabled	Call	Enabled	0	Enabled	0	Disabled
6		Disabled	Call	Enabled	0	Enabled	0	Disabled
7		Disabled	Call	Enabled	0	Enabled	0	Disabled

All configuration of the handset Alarm Settings is done from the Base station. The concept is that on the “Alarm” page on the web server, eight different alarm profiles can be configured. Afterwards for each handset, it can be selected which of the configured alarm profiles, the given handset shall subscribe to. When this is done the selected alarm, profiles are sent to the handset.

See section *5.3.3 handset*.

PARAMETERS	DESCRIPTION
IDX	Indicates the index number of a specific alarm.
PROFILE ALIAS	An alias or user-friendly name to help identify the different profiles when selecting which profiles to enable for the individual handsets.
ALARM TYPE	The type of alarm is dependent of what kind of event that has triggered the alarm on the handset. The type of alarms supported is handset related. **RTX8632/RTX8633:**

	Alarm button **RTX8830:** Alarm button Man Down No Movement Running Pull Cord Emergency Button Disabled
ALARM SIGNAL	The way the alarm is signaled as it received on the handset. **Message:** A text message to an alarm server. **Call:** An outgoing call to the specified emergency number.
STOP ALARM FROM HANDSET	**Enable/Disable** the possibility to stop/cancel the alarm from the handset.
TRIGGER DELAY	The period from when the alarm has fired until the handset shows a pre-alarm warning. If set to 0, there will be no pre-alarm warning, and the alarm will be signaled immediately. The alarm algorithm typically needs about 6 sec. to detect e.g. man down etc.
STOP PRE-ALARM FROM HANDSET	**Enable/Disable** the possibility to stop/cancel the pre-alarm from the handset.
PRE-ALARM DELAY	The period from the pre-alarm warning is shown until the actual alarm is signaled. The maximum value is 255.
HOWLING	**Enable/Disable** if howling shall be started in the handset, when the alarm is signaled. If disabled, only the configured signal is sent (call or message).

NOTE: The alarm feature is only available on some types of handsets (e.g. RTX8632, RTX8633 and RTX8830)
After configuration, the handset must be rebooted.

5.15.1 Use of Emergency Alarms

As described above, it can be configured if it shall be possible to stop an alarm from the handset. If the possibility to stop an alarm from the handset is disabled, it is ensured that an alarm is not stopped before someone at e.g. an emergency center has received the alarm and reacted upon it.

The behavior of a handset when an alarm "is sent" depends on the configured Alarm Signal:

- **Call:** When the Alarm Signal is configured as "Call", the handset will make a call to the specified emergency number, and the alarm is considered stopped when the call is terminated. If it is not allowed to stop the alarm from the handset, it will not be possible to terminate the call from handset, and the alarm will be considered as stopped only when the remote end (e.g. the emergency center) terminates the call.
- **Message:** When the Alarm Signal is configured as "Message", the handset will send an alarm message to the specified alarm server, and enable auto answer mode. If Howling is enabled, the handset will also start the Howling tone. The alarm will not stop until a call is made, and since auto answer mode is enabled, the emergency center can make the call, and the person with the handset does not have to do anything to answer the call, it will answer automatically. Again, the alarm is considered stopped, when the call is terminated with the same restrictions as for the Call alarm signal.

All type of alarms has the same priority. This means that once an alarm is active, it cannot be overruled by another alarm until the alarm has been stopped. However, if the alarm is not yet active, i.e. if it is in "pre-alarm" state and an alarm configured with no pre-alarm is fired, then the new alarm will become active and stop the pending alarm. Alarms with no pre-alarm are considered important, and there is no possibility to cancel them before they are sent, and therefore alarms with no pre-alarm, are given higher priority than alarms in pre-alarm state.

The Emergency Button could be an example of an alarm which would be configured without pre-alarm. Thus, when the Emergency Button is pressed you want to be sure the alarm is sent. However, if another alarm was already in pre-alarm state, it could potentially be cancelled, and if the Emergency Button alarm was ignored in this case, no alarm would be sent. This is the reason alarms with no pre-alarm, are given higher priority than alarms in pre-alarm state.

5.16 Statistics

The statistic feature is divided into four administrative web pages, which can be access from any base.

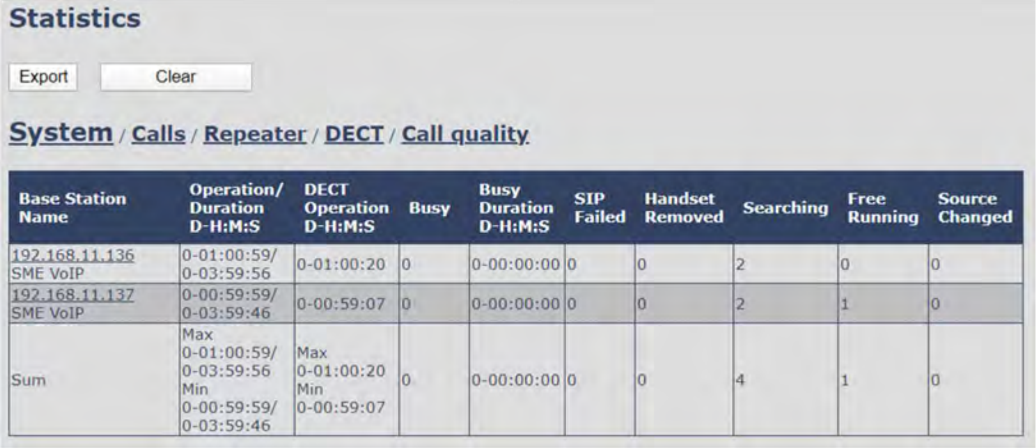
1. System
2. Calls
3. Repeater
4. DECT data
5. Call quality

All five views have an embedded export function, which export all data to comma separated file.
By pressing the clear button all data in the full system is cleared.

5.16.1 System data

Data is organized in a table as shown in the below example.

Screenshot



Base Station Name	Operation/ Duration D-H:M:S	DECT Operation D-H:M:S	Busy	Busy Duration D-H:M:S	SIP Failed	Handset Removed	Searching	Free Running	Source Changed
192.168.11.136 SME VoIP	0-01:00:59/ 0-03:59:56	0-01:00:20	0	0-00:00:00	0	0	2	0	0
192.168.11.137 SME VoIP	0-00:59:59/ 0-03:59:46	0-00:59:07	0	0-00:00:00	0	0	2	1	0
Sum	Max 0-01:00:59/ 0-03:59:56 Min 0-00:59:59/ 0-03:59:46	Max 0-01:00:20 Min 0-00:59:07	0	0-00:00:00	0	0	4	1	0

The table is organized with headline row, data pr. base rows and with last row containing the sum of all base parameters.

PARAMETERS	DESCRIPTION
BASE STATION NAME	Base IP address and Base station name from management settings
OPERATION/DURATION D-H:M:S	Operation is operation time for the base since last reboot. Duration is the operation time for the base since last reset of statistics, or firmware upgrade.
DECT OPERATION D-H:M:S	Displays information about Days, Hours, Minutes and Seconds that the base station has been running
BUSY	Busy Count is the number of times the base has been busy.
BUSY DURATION D-H:M:S	Busy duration is the total time a base has been busy for speech (8 or more calls active).
SIP FAILED	Failed SIP registrations count the number of times a SIP registration has failed
HANDSET REMOVED	Handset removed count is the number of times a handset has been marked as removed
SEARCHING	Base searching is the number of times a base has been searching for its sync source
FREE RUNNING	Base free running is the number of times a base has been free running

DECT SOURCE CHANGED	Number of time a base has changed sync source
IEEE1588 SYNC LOST	Connection is lost to all synchronized Base stations, connection will be lost.
IEEE1588 PRIMARY LOST	Connection is lost to one of the synchronized Base stations, in this case new primary will be selected automatically.

5.16.2 Free Running explained

First, state Free running NOT an error state, but is a simple trigger state, indicating that some changes have to be made to ensure continuous DECT synchronization.

The state Free running, tells the application that the base has not gotten any synchronization data from its synchronization source Base station in the last 10 seconds.

The reason for this can be several:

1. The two bases are using the same DECT slots and can therefore not see each other.
2. Many simultaneous voice or data calls.
3. Suddenly change of environment (Closing a fire door)
4. Distortion of DECT frequency (around 1.8MHz) Either by other DECT systems or other equipment.

When the Free running state is trigged, several recovery mechanisms are activated:

1. Move DECT slot to avoid using same DECT slot as its synchronization source base state.
2. Use information from all other Base station, how they are seeing this Base station in the DECT air. This is marked by changing to state Assisted lock

The state Assisted lock can be stabile for a long time and normally change to state Locked again.
The state Free Running can also change back to state Locked again.

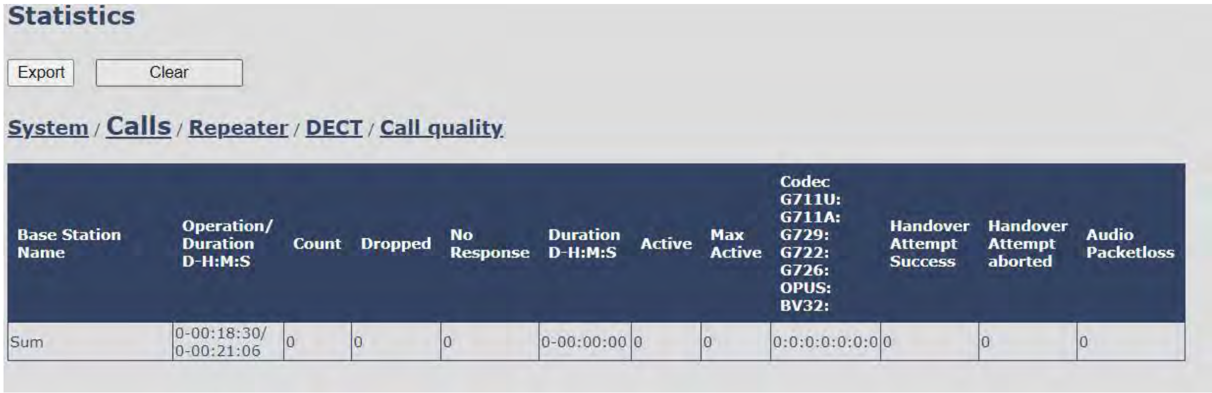
If the base is in state Free running and the synchronization source Base station is not seen and no data is available for the assisted lock mechanism, the Base station will change to a new state after 2 minutes:

1. If the Base station does NOT have any active calls, the base will change to state Searching.
2. If the Base station has an active call, this base will change to state Sync lost. After the call is released, the state will change to state Searching.

5.16.3 Call data

Data is organized in a table as shown in the below example.

Screenshot



Base Station Name	Operation/ Duration D-H:M:S	Count	Dropped	No Response	Duration D-H:M:S	Active	Max Active	Codec G711U: G711A: G729: G722: G726: OPUS: BV32:	Handover Attempt Success	Handover Attempt aborted	Audio Packetloss
Sum	0-00:18:30/ 0-00:21:06	0	0	0	0-00:00:00	0	0	0:0:0:0:0:0:0	0	0	0

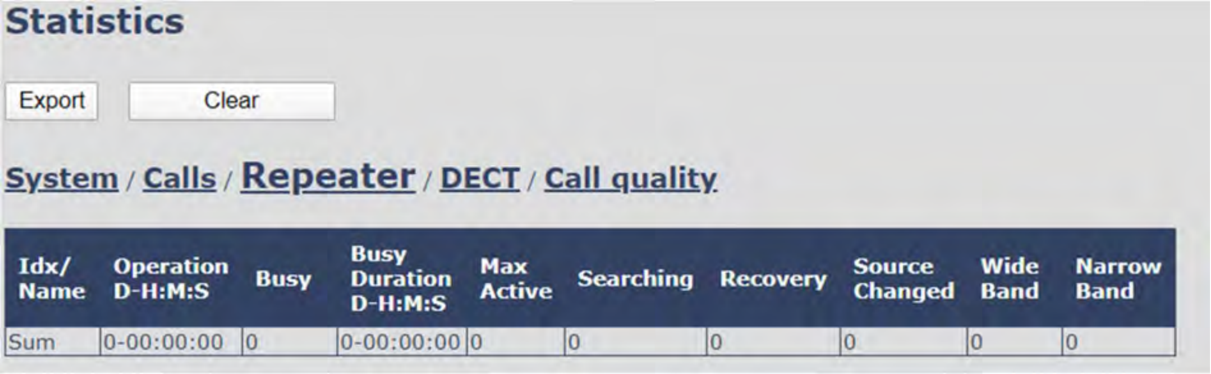
The table is organized with headline row, data pr. base rows and with last row containing the sum of all base parameters.

PARAMETERS	DESCRIPTION
BASE STATION NAME	Base IP address and Base station name from management settings
OPERATION TIME/DURATION	Total operation time for the base since last reboot or reset Duration is the time from data was cleared or system has been firmware upgraded.
COUNT	Counts number of calls on a base.
DROPPED	Dropped calls are the number of active calls that was dropped. E.g. if a user has an active call and walks out of range, the calls will be counted as a dropped call. An entry is stored in the syslog when a call is dropped.
NO RESPONSE	No response calls are the number of calls that have no response, e.g. if an external user tries to make a call to a handset that is out of range the call is counted as no response. An entry is stored in the syslog when a call is no response.
DURATION	Call duration is total time that calls are active on the base.
ACTIVE	Active call shows how many active calls that are active on the base station (Not active DECT calls, but active calls). On one base there can be up to 10 active calls in single mode and 8 in Multi Cell mode.
MAX ACTIVE	Maximum active calls are the maximum number of calls that has been active at the same time.
CODECS	Logging and count of used codec types on each call.
HANDOVER ATTEMPT SUCCESS	Counts the number of successful handovers.
HANDOVER ATTEMPT ABORTED	Counts the number of failed handovers.
AUDIO PACKET LOSS	Counts the number of times where audio connection was not established.

5.16.4 Repeater data

Data is organized in a table as shown in the below example.

Screenshot



Statistics

Idx/ Name	Operation D-H:M:S	Busy	Busy Duration D-H:M:S	Max Active	Searching	Recovery	Source Changed	Wide Band	Narrow Band
Sum	0-00:00:00	0	0-00:00:00	0	0	0	0	0	0

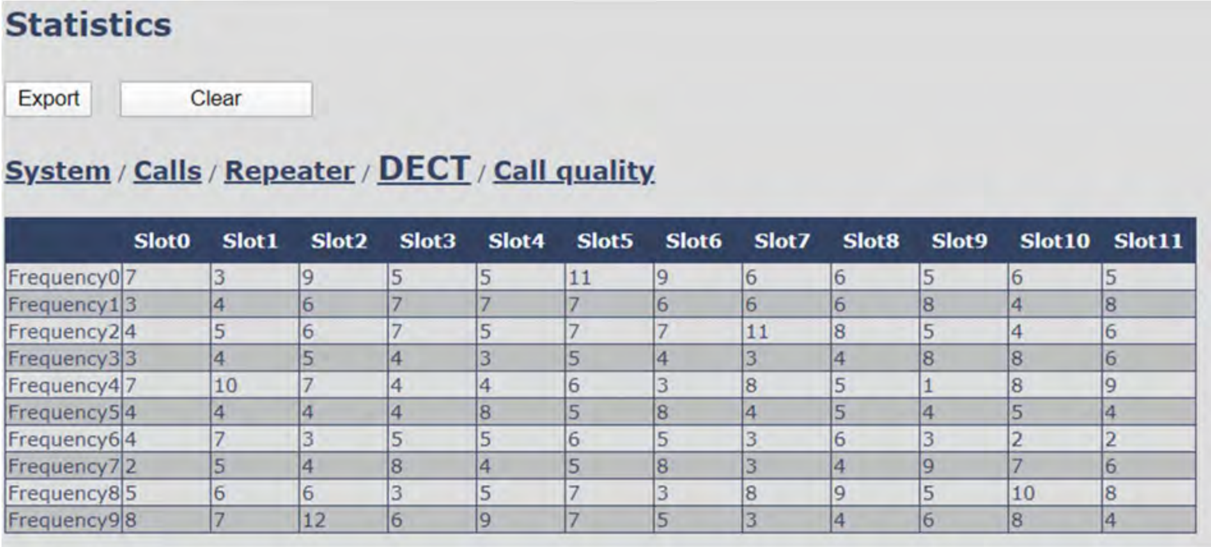
The table is organized with headline row, data pr. base rows and with last row containing the sum of all base parameters.

PARAMETERS	DESCRIPTION
IDX/NAME	Base IP address and Base station name from management settings
OPERATION D-H:M:S	Total operation time for the repeater since last reboot or reset Duration is the time from data was cleared or system has been firmware upgraded.
BUSY	Busy Count is the number of times the repeater has been busy.
BUSY DURATION D-H:M:S	Busy duration is the total time a repeater has been busy for speech (5 or more calls active).
MAX ACTIVE	Maximum active calls are the maximum number of calls that has been active at the same time.
SEARCHING	Repeater searching is the number of times a repeater has been searching for it's sync source
RECOVERY	In case the sync source is not present anymore the repeater will go into lock on another base or repeater and show recovery mode
DECT SOURCE CHANGED	Number of time a repeater has changed sync source
WIDE BAND	Number of wideband calls on repeaters
NARROW BAND	Number of narrow band calls on repeaters

5.16.5 DECT data

Data is organized in a table as shown in the below example.

Screenshot



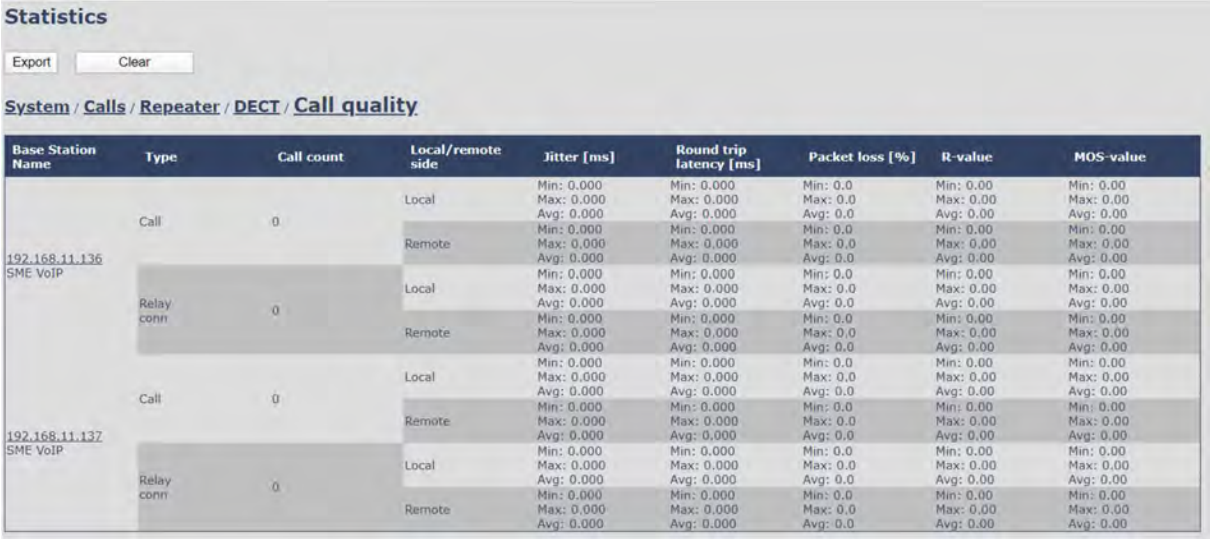
	Slot0	Slot1	Slot2	Slot3	Slot4	Slot5	Slot6	Slot7	Slot8	Slot9	Slot10	Slot11
Frequency0	7	3	9	5	5	11	9	6	6	5	6	5
Frequency1	3	4	6	7	7	7	6	6	6	8	4	8
Frequency2	4	5	6	7	5	7	7	11	8	5	4	6
Frequency3	3	4	5	4	3	5	4	3	4	8	8	6
Frequency4	7	10	7	4	4	6	3	8	5	1	8	9
Frequency5	4	4	4	4	8	5	8	4	5	4	5	4
Frequency6	4	7	3	5	5	6	5	3	6	3	2	2
Frequency7	2	5	4	8	4	5	8	3	4	9	7	6
Frequency8	5	6	6	3	5	7	3	8	9	5	10	8
Frequency9	8	7	12	6	9	7	5	3	4	6	8	4

PARAMETERS	DESCRIPTION
FREQUENCY	Number of the DECT slot frequency
SLOTX	Number of connections that have been active on each frequency

5.16.6 Call quality

Data is organized in a table as shown in the below example.

Screenshot



Statistics

System / Calls / Repeater / DECT / Call quality

Base Station Name	Type	Call count	Local/remote side	Jitter [ms]	Round trip latency [ms]	Packet loss [%]	R-value	MOS-value
192.168.11.136 SME VoIP	Call	0	Local	Min: 0.000 Max: 0.000 Avg: 0.000	Min: 0.000 Max: 0.000 Avg: 0.000	Min: 0.0 Max: 0.0 Avg: 0.0	Min: 0.00 Max: 0.00 Avg: 0.00	Min: 0.00 Max: 0.00 Avg: 0.00
			Remote	Min: 0.000 Max: 0.000 Avg: 0.000	Min: 0.000 Max: 0.000 Avg: 0.000	Min: 0.0 Max: 0.0 Avg: 0.0	Min: 0.00 Max: 0.00 Avg: 0.00	Min: 0.00 Max: 0.00 Avg: 0.00
	Relay conn	0	Local	Min: 0.000 Max: 0.000 Avg: 0.000	Min: 0.000 Max: 0.000 Avg: 0.000	Min: 0.0 Max: 0.0 Avg: 0.0	Min: 0.00 Max: 0.00 Avg: 0.00	Min: 0.00 Max: 0.00 Avg: 0.00
			Remote	Min: 0.000 Max: 0.000 Avg: 0.000	Min: 0.000 Max: 0.000 Avg: 0.000	Min: 0.0 Max: 0.0 Avg: 0.0	Min: 0.00 Max: 0.00 Avg: 0.00	Min: 0.00 Max: 0.00 Avg: 0.00
192.168.11.137 SME VoIP	Call	0	Local	Min: 0.000 Max: 0.000 Avg: 0.000	Min: 0.000 Max: 0.000 Avg: 0.000	Min: 0.0 Max: 0.0 Avg: 0.0	Min: 0.00 Max: 0.00 Avg: 0.00	Min: 0.00 Max: 0.00 Avg: 0.00
			Remote	Min: 0.000 Max: 0.000 Avg: 0.000	Min: 0.000 Max: 0.000 Avg: 0.000	Min: 0.0 Max: 0.0 Avg: 0.0	Min: 0.00 Max: 0.00 Avg: 0.00	Min: 0.00 Max: 0.00 Avg: 0.00
	Relay conn	0	Local	Min: 0.000 Max: 0.000 Avg: 0.000	Min: 0.000 Max: 0.000 Avg: 0.000	Min: 0.0 Max: 0.0 Avg: 0.0	Min: 0.00 Max: 0.00 Avg: 0.00	Min: 0.00 Max: 0.00 Avg: 0.00
			Remote	Min: 0.000 Max: 0.000 Avg: 0.000	Min: 0.000 Max: 0.000 Avg: 0.000	Min: 0.0 Max: 0.0 Avg: 0.0	Min: 0.00 Max: 0.00 Avg: 0.00	Min: 0.00 Max: 0.00 Avg: 0.00

<table>
<tr><th>PARAMETERS</th><th>DESCRIPTION</th></tr>
<tr><td>BASE STATION NAME</td><td>Base IP address and base station name from management settings</td></tr>
<tr><td>TYPE</td><td>Call
Relay conn</td></tr>
<tr><td>CALL COUNT</td><td>Count the number of calls</td></tr>
<tr><td>LOCAL/REMOTE SIDE</td><td>Local:
Remote:</td></tr>
<tr><td>JITTER[MS]</td><td>Measures how the RTP packets are received, the lower the Jitter is the better</td></tr>
<tr><td>ROUND TRIP LATENCY [MS]</td><td>Measures the time it takes for RTP packets to reach it destination.</td></tr>
<tr><td>PACKET LOSS [%]</td><td>Percentages of packets lost.</td></tr>
<tr><td>R-VALUE</td><td>A way to measure call quality, from 0-120
<table>
<tr><th>USER SATISFACTION LEVEL</th><th>MOS</th><th>R-Factor</th></tr>
<tr><td>MAXIMUM USING G.711</td><td>4.4</td><td>93</td></tr>
<tr><td>VERY SATISFIED</td><td>4.3-5.0</td><td>90-100</td></tr>
<tr><td>SATISFIED</td><td>4.0-4.3</td><td>80-90</td></tr>
<tr><td>SOME USERS SATISFIED</td><td>3.6-4.0</td><td>70-80</td></tr>
<tr><td>MANY USERS DISSATISFIED</td><td>3.1-3.6</td><td>60-70</td></tr>
<tr><td>NEARLY ALL USERS DISSATISFIED</td><td>2.6-3.1</td><td>50-60</td></tr>
<tr><td>NOT RECOMMENDED</td><td>1.0-2.6</td><td>Less than 50</td></tr>
</table></td></tr>
<tr><td>MOS-VALUE</td><td><b>MOS</b> measures subjective call quality for a call. MOS scores range from 1 for unacceptable to 5 for excellent.
VOIP calls often are in the 3.5 to 4.2 range
See table above.</td></tr>
</table>

5.17 Generic Statistics

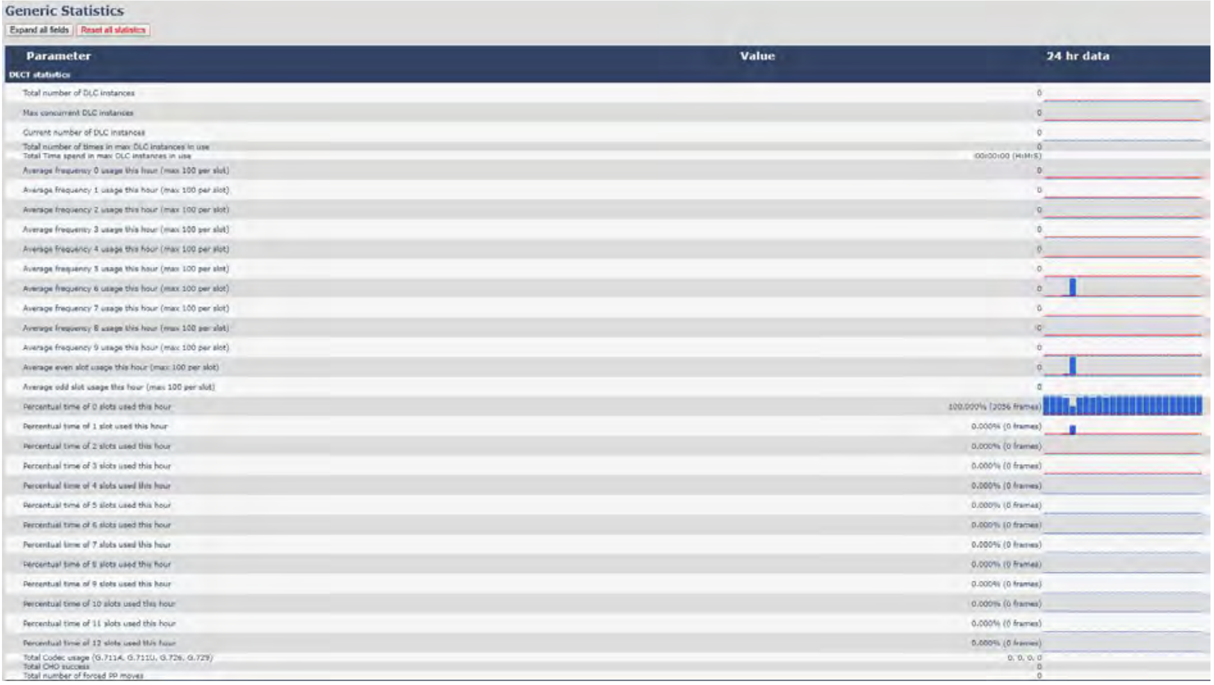
The statistic feature is divided into five sections, which can be access from any base.

1. DECT Statistics
2. DECT Synchronization statistics
3. RTP Statistics
4. IP Stack Statistics
5. System Statistics

By pressing the “Expand all fields” you are able to see statistics hour by hour. “Reset all statistics” button all data in the full system is cleared.

PARAMETER	DEFAULT VALUES	DESCRIPTION
PARAMETER	Vary	Headline of the different statistics
VALUE	Vary	Vary for point to point
24 HR DATA	Vary	Data from the last 24 hours

Screenshot:



Generic Statistics

Parameter	Value	24 hr data
DECT statistics		
Total number of DLC instances	0	
Max concurrent DLC instances	0	
Current number of DLC instances	0	
Total number of times in max DLC instances in use	0	
Total Time spend in max DLC instances in use	00:00:00 (H:M:S)	
Average frequency 0 usage this hour (max 100 per slot)	0	
Average frequency 1 usage this hour (max 100 per slot)	0	
Average frequency 2 usage this hour (max 100 per slot)	0	
Average frequency 3 usage this hour (max 100 per slot)	0	
Average frequency 4 usage this hour (max 100 per slot)	0	
Average frequency 5 usage this hour (max 100 per slot)	0	
Average frequency 6 usage this hour (max 100 per slot)	0	
Average frequency 7 usage this hour (max 100 per slot)	0	
Average frequency 8 usage this hour (max 100 per slot)	0	
Average frequency 9 usage this hour (max 100 per slot)	0	
Average even slot usage this hour (max 100 per slot)	0	
Average odd slot usage this hour (max 100 per slot)	0	
Percentual time of 0 slots used this hour	100.000% (2036 frames)	
Percentual time of 1 slot used this hour	0.000% (0 frames)	
Percentual time of 2 slots used this hour	0.000% (0 frames)	
Percentual time of 3 slots used this hour	0.000% (0 frames)	
Percentual time of 4 slots used this hour	0.000% (0 frames)	
Percentual time of 5 slots used this hour	0.000% (0 frames)	
Percentual time of 6 slots used this hour	0.000% (0 frames)	
Percentual time of 7 slots used this hour	0.000% (0 frames)	
Percentual time of 8 slots used this hour	0.000% (0 frames)	
Percentual time of 9 slots used this hour	0.000% (0 frames)	
Percentual time of 10 slots used this hour	0.000% (0 frames)	
Percentual time of 11 slots used this hour	0.000% (0 frames)	
Percentual time of 12 slots used this hour	0.000% (0 frames)	
Total Codec usage (G.711A, G.711U, G.726, G.729)	0, 0, 0, 0	
Total CHO success	0	
Total number of forced PP moves	0	

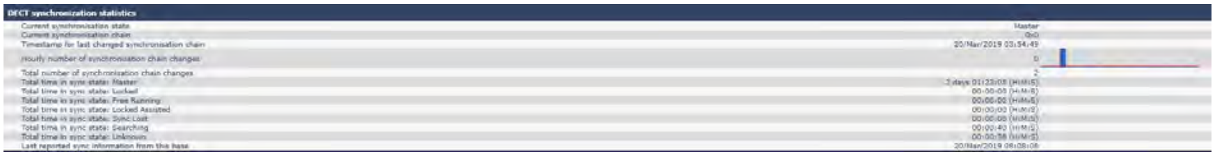
PARAMETERS	DESCRIPTION
TOTAL NUMBER OF DLC INSTANCE	The life time total count of instantiated DLC instances.
MAX CONCURRENT DLC INSTANCES	The life time highest concurrent count of instantiated DLC instances.
CURRENT NUMBER OF DLC INSTANCES	The current count of instantiate DLC instances.
TOTAL NUMBER OF TIMES IN MAX DLC INSTANCES IN USE	The number of times we reach the currently highest count of DLC instances.

TOTAL TIME SPEND IN MAX DLC INSTANCES IN USE	The time we have spent in the highest concurrent number of instantiated DLC instances.
AVERAGE FREQUENCY X USAGE THIS HOUR (MAX 100 PER SLOT)	The average use of frequency number X. The value is 100 if the frequency is fully used by a slot in the measured time frame.
AVERAGE EVEN SLOT USAGE THIS HOUR (MAX 100 PER SLOT)	The average use of even numbered slots.
AVERAGE ODD SLOT USAGE THIS HOUR (MAX 100 PER SLOT)	The average use of odd numbered slots.
PERCENTUAL TIME OF X SLOTS USED THIS HOUR	The percentual time that X number of dect slots are used during the given hour (compared to other slot counts).
TOTAL CHO SUCCESS	The number of times connection handover is successfully made.
Total number of forced PP moves	The life time total count that this base forces PP moves.

5.17.1 DECT Synchronization Statistics

DECT Synchronization statistics is related to this Base station only.

Screenshot:



DECT synchronization statistics

Current synchronisation state	Master
Current synchronisation chain	0x0
Timestamp for last changed synchronisation chain	20/Mar/2019 03:54:49
Hourly number of synchronisation chain changes	0
Total number of synchronization chain changes	2
Total time in sync state: Master	3 days 01:22:08 (H:M:S)
Total time in sync state: Locked	00:00:05 (H:M:S)
Total time in sync state: Free Running	00:00:00 (H:M:S)
Total time in sync state: Locked Assisted	00:00:02 (H:M:S)
Total time in sync state: Sync Lost	00:00:08 (H:M:S)
Total time in sync state: Searching	00:00:40 (H:M:S)
Total time in sync state: Unknown	00:00:58 (H:M:S)
Last reported sync information from this base	20/Mar/2019 08:08:08

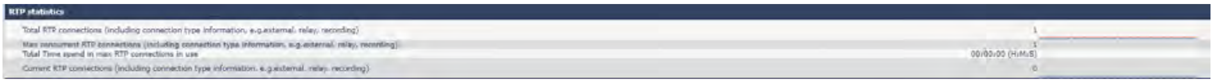
PARAMETERS	DESCRIPTION
CURRENT SYNCHRONISATION STATE	The current DECT sync state (e.g. Master, Searching, Free Running, etc).
CURRENT SYNCHRONISATION CHAIN	The current DECT sync source Fp Id of this base.
TIMESTAMP FOR LAST CHANGED SYNCHRONISATION CHAIN	Timestamp of the last time this base changed DECT sync source.
HOURLY NUMBER OF SYNCHRONISATION CHAIN CHANGES	The number of times this base changed DECT sync source in the current hour.
TOTAL NUMBER OF SYNCHRONISATION CHAIN CHANGES	The life time total count of times this base changed DECT sync source.

TIME IN SYNCHRONISATION STATE: MASTER	Time this hour where this Base station has had the state Master
TIME IN SYNCHRONISATION STATE: LOCKED	Time this hour where this Base station has had the state Locked
TIME IN SYNCHRONISATION STATE: FREE RUNNING	Time this hour where this Base station has had the state Alien Free Running
TIME IN SYNCHRONISATION STATE: LOCKED ASSISTED	Time this hour where this Base station has been in lock assisted
TIME IN SYNCHRONISATION STATE: SYNC LOST	Time this hour where this Base station has not been in Sync
TIME IN SYNCHRONISATION STATE: SEARCHING	Time this hour where this base has been searching for its sync source
TIME IN SYNCHRONISATION STATE: UNKNOWN	Time this hour where this Base station has not been in unknown state
LAST REPORTED SYNC	Time when system, last received sync information from this Base station

5.17.2 RTP Statistics

RTP statistics is related to this Base station only.

Screenshot:



RTP statistics

```
Total RTP connections (including connection type information, e.g.external, relay, recording)          1
Max concurrent RTP connections (including connection type information, e.g.external, relay, recording) 1
Total Time spend in max RTP connections in use                                                          00:00:00 (H:M:S)
Current RTP connections (including connection type information, e.g.external, relay, recording)        0
```

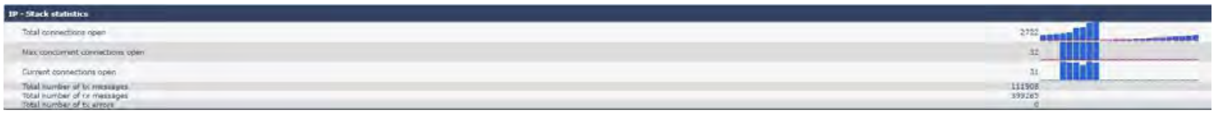
PARAMETERS	DESCRIPTION
TOTAL RTP CONNECTIONS (INCLUDING CONNECTION TYPE INFORMATION, E.G. EXTERNAL, RELAY, RECORDING)	The life time total count of instantiated RTP streams.
MAX CONCURRENT RTP CONNECTIONS (INCLUDING CONNECTION TYPE INFORMATION, E.G. EXTERNAL, RELAY, RECORDING)	The life time highest concurrent count of instantiated RTP streams.
TOTAL TIME SPEND IN MAX RTP	The time we have spent in the highest concurrent count of instantiated RTP streams.

CONNECTIONS IN USE	
CURRENT RTP CONNECTIONS (INCLUDING CONNECTION TYPE INFORMATION, E.G. EXTERNAL, RELAY, RECORDING)	The current count of instantiated RTP streams.
CURRENT BLACKFIN DSP STATUS	Data only available if DSP module is installed

5.17.3 IP - Stack statistics

IP - Stack statistics is related to this Base station only.

Screenshot:



IP - Stack statistics

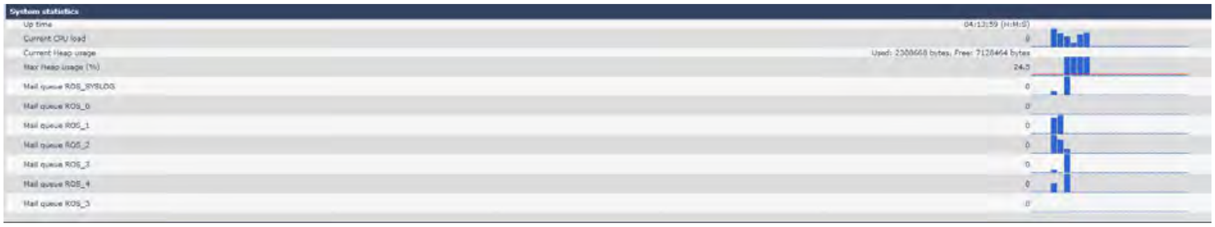
Total connections open	2732
Max concurrent connections open	32
Current connections open	31
Total number of tx messages	111908
Total number of rx messages	399265
Total number of tx errors	0

PARAMETERS	DESCRIPTION
TOTAL CONNECTIONS OPEN	The life time total count of used sockets.
MAX CONCURRENT CONNECTIONS OPEN	The life time highest concurrent count of used sockets.
CURRENT CONNECTIONS OPEN	The current count of used sockets.
TOTAL NUMBER OF TX MESSAGES	The life time total count of transmitted IP packets.
TOTAL NUMBER OF RX MESSAGES	The life time total count of received IP packets.
TOTAL NUMBER OF TX ERRORS	The life time total count of errors occurred during IP packet transmission.

5.17.4 System Statistics

System Statistics is related to this Base station only.

Screenshot:



System statistics

Up time	04:13:59 (H:M:S)
Current CPU load	0
Current Heap usage	Used: 2308668 bytes, Free: 7128464 bytes
Max Heap usage (%)	24.5
Mail queue ROS_SYSLOG	0
Mail queue ROS_0	0
Mail queue ROS_1	0
Mail queue ROS_2	0
Mail queue ROS_3	0
Mail queue ROS_4	0
Mail queue ROS_5	0

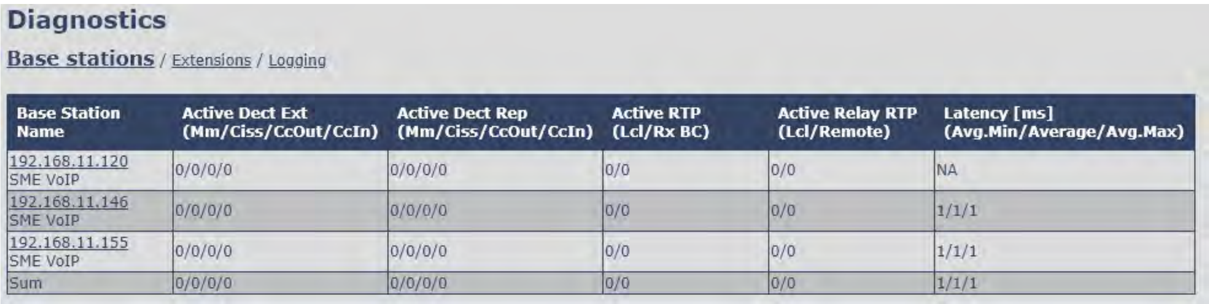
PARAMETERS	DESCRIPTION
UP TIME	The time the base has been running consecutively.
CURRENT CPU LOAD	The current load percentage of CPU. This is refreshed once every 5 seconds.
CURRENT HEAP USAGE	The current use of heap in Bytes.
MAX HEAP USAGE (%)	The peak usage of heap in percentage.
MAIL QUEUE ROS_SYSLOG	Size of internal mail queue for syslogs.
MAIL QUEUE ROS_X	Size of internal mail queue.

5.18 Diagnostics

This page provides information about the Ethernet connection to each Base station and Extension.

5.18.1 Base stations

Screenshot



Diagnostics

Base stations / Extensions / Logging

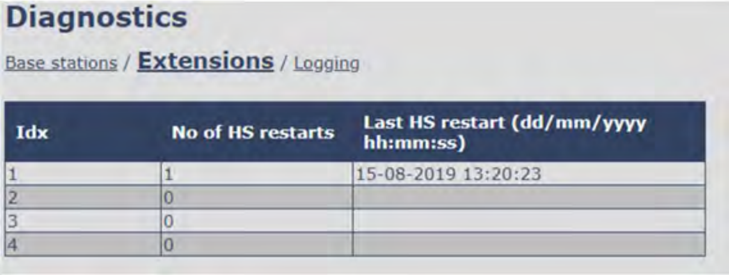
Base Station Name	Active Dect Ext (Mm/Ciss/CcOut/CcIn)	Active Dect Rep (Mm/Ciss/CcOut/CcIn)	Active RTP (Lcl/Rx BC)	Active Relay RTP (Lcl/Remote)	Latency [ms] (Avg.Min/Average/Avg.Max)
192.168.11.120 SME VoIP	0/0/0/0	0/0/0/0	0/0	0/0	NA
192.168.11.146 SME VoIP	0/0/0/0	0/0/0/0	0/0	0/0	1/1/1
192.168.11.155 SME VoIP	0/0/0/0	0/0/0/0	0/0	0/0	1/1/1
Sum	0/0/0/0	0/0/0/0	0/0	0/0	1/1/1

PARAMETERS	DESCRIPTION
BASE STATION NAME	Base IP address and Base station name from management settings
ACTIVE DECT EXT (MM/CISS/CCOUT/CCIN)	Number of active DECT MAC connections to extensions in the different Base stations. Types of connection is (mm/Ciss/CcOut/CcIn)
ACTIVE DECT REP (MM/CISS/CCOUT/CCIN)	Number of active DECT MAC connections to repeaters in the different Base stations. Types of connection is (mm/Ciss/CcOut/CcIn)
ACTIVE RTP (LCL/RX BC)	Number of active RTP Streams used. Types of stream (Local RTP stream/Broadcast Receive RTP stream)
ACTIVE RELAY RTP (LCL/REMOTE)	Number of active RTP Relay Streams used. Types of stream (Local RTP Relay stream/Remote RTP Relay stream)
LATENCY [MS] (AVG.MIN/AVERAGE/AVG.MAX)	Ping latency between Base station performed by base index 0. Average Minimum delay/Average/Average Maximum delay)

5.18.2 Extensions

Information in the table will be visible if there is a handset Crash.

Screenshot



Diagnostics

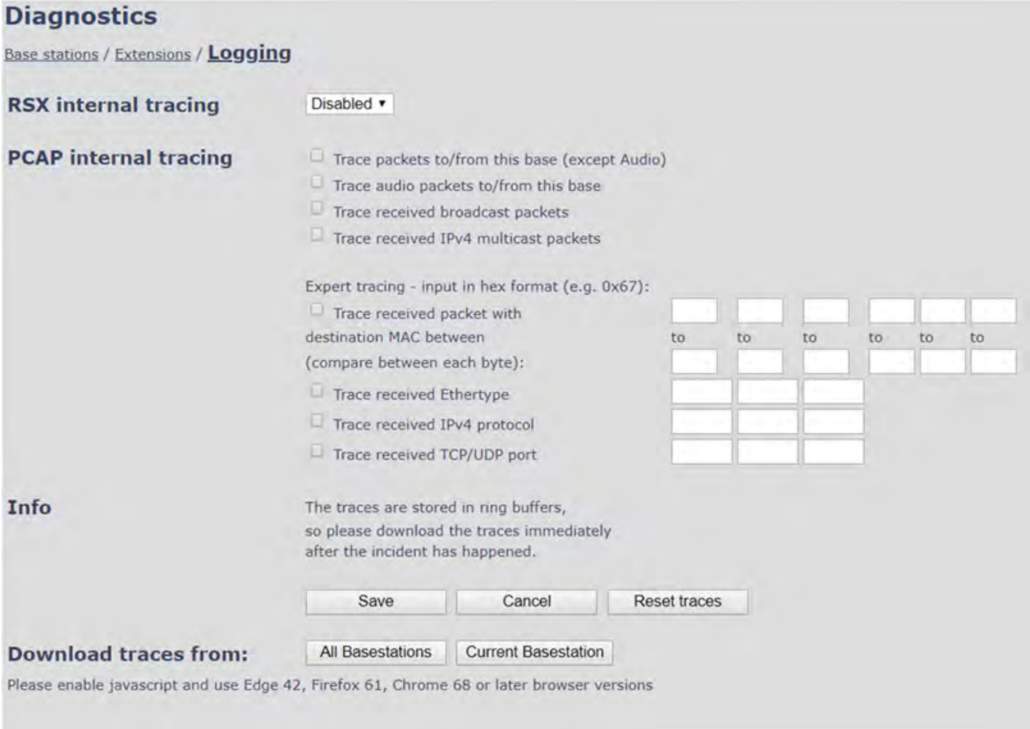
Base stations / Extensions / Logging

Idx	No of HS restarts	Last HS restart (dd/mm/yyyy hh:mm:ss)
1	1	15-08-2019 13:20:23
2	0	
3	0	
4	0	

PARAMETERS	DESCRIPTION
IDX	Extension Index number
NO OF HS RESTARTS	Number of times that the Handset have restarted
LAST HS RESTART (DD/MM/YYYY HH:MM:SS)	Date and time of the last time the Handset have restarted

5.18.3 Logging

The Diagnostics/Logging page allows you to collect system diagnostics information into a zip file.



Diagnostics

Base stations / Extensions / **Logging**

RSX internal tracing Disabled ▾

PCAP internal tracing

□ Trace packets to/from this base (except Audio)
□ Trace audio packets to/from this base
□ Trace received broadcast packets
□ Trace received IPv4 multicast packets

Expert tracing - input in hex format (e.g. 0x67):
□ Trace received packet with destination MAC between (compare between each byte): to to to to to to
□ Trace received Ethertype
□ Trace received IPv4 protocol
□ Trace received TCP/UDP port

Info The traces are stored in ring buffers, so please download the traces immediately after the incident has happened.

Download traces from:

Please enable javascript and use Edge 42, Firefox 61, Chrome 68 or later browser versions

5.18.3.1 RSX internal tracing

RSX internal tracing can be either Enabled or Disabled. When the feature is enabled, the traced data is used by the RTX engineers which are the only ones that can debug the traces.

5.18.3.2 PCAP internal tracing

This feature allows the user to choose which trace to investigate by selecting the desired parameter.

PARAMETERS	DESCRIPTION
TRACE PACKETS TO/FROM THIS BASE (EXCEPT AUDIO)	If selected, all Ethernet packets sent to/from the Base station's MAC address will be traced. Broadcast packets sent from the base are also being traced.
TRACE AUDIO PACKETS TO/FROM THIS BASE	If selected, RTP streams to/from the BS will be traced. Audio packets are filtered by the port number used for RTP packets which is set on the web page
TRACE RECEIVED BROADCAST PACKETS	If selected, all broadcast packets received by the BS will be traced.
TRACE RECEIVED IPV4 MULTICAST PACKETS	If selected, all received IPv4 multicast packets will be traced
TRACE RECEIVED PACKET WITH DESTINATION MAC BETWEEN	If selected, each byte of the received destination MAC is checked if it is in the trace range
TRACE RECEIVED ETHERTYPE	If selected, the user can select 3 received Ethertypes to trace
TRACE RECEIVED IPV4 PROTOCOL	If selected, the user can select 3 received IPv4 protocols to trace

TRACE RECEIVED TCP/UDP PORT	If selected, the user can select 3 received TCP/UDP ports to trace.

5.18.3.3 Info

The section gives information about the traces and allows the user to “Save”, “Cancel” or “Reset traces”.

5.18.3.4 Download traces from

The feature allows the user to choose from which Base stations to download the traces. If it is a Multi cell system, the data can be downloaded from all Base stations, else system diagnostics can be downloaded from the current machine. The zip file includes all type of information, such as RSX trace, Syslog, SIP Log, Config file(s), etc.

5.19 Settings – Configuration File Setup

This page provides non-editable information showing the native format of entire SME VoIP Configuration parameter settings. The **settings** format is exactly what is used in the configuration file. The configuration file is found in the TFTP server.

The filename for the configuration server is **<MAC_Address>.cfg**. The configuration file is saved in the folder **/Config** in the TFTP sever.

There are three ways to edit the configuration file or make changes to the **settings** page:

- Using the SME VoIP Configuration interface to make changes. Each page of the web interface is a template for which the user can customize settings in the configuration file.
- Retrieving the relevant configuration file from the TFTP and modify and enter new changes. This should be done with an expert network administrator.
- Navigate to the settings page of the VoIP SME Configuration interface > copy the contents of settings > save them to any standard text editor e.g. notepad > modify the relevant contents, make sure you keep the formatting intact > Save the file as **<Enter_MAC_Address_of_RFP>.cfg** > upload it into the relevant TFTP server.

An example of contents of settings is as follows:

```
~RELEASE=BEATUS_FP_V0400_B0001
~System Mode=51/51
%GMT_TIME_ZONE%:0x06
%COUNTRY_VARIANT_ID%:0x12
%COUNTRY_REGION_ID%:0x00
%TIMEZONE_BY_COUNTRY_REGION%:0x01
%DST_BY_COUNTRY_REGION%:0x01
%DST_ENABLE%:0x02
%DST_FIXED_DAY_ENABLE%:0x00
%DST_START_MONTH%:0x03
%DST_START_DATE%:0x00
………
```

For detailed description on how to use provisioning please ask RTX support for the “Provisioning of SME VoIP System (24)” guide.

5.20 Sys log

This page shows live feed of system level messages of the current Base station. The messages the administrator see here depends on what is configured at the Management settings. The Debug logs can show only **Boot Log** or **Everything** that is all system logs including boot logs.
The Debug log is saved in the file format **<Time_Stamp>b.log** in a relevant location in the TFTP server as specified in the upload script.

A sample of debug logs is as follows:

```
0101000013 [N](01):DHCP Enabled
0101000013 [N](01):IP Address: 192.168.10.101
0101000013 [N](01):Gateway Address: 192.168.10.254
0101000013 [N](01):Subnet Mask: 255.255.255.0
0101000013 [N](01):TFTP boot server not set by DHCP. Using Static.
0101000013 [N](01):DHCP Discover completed
0101000013 [N](01):Time Server: 192.168.10.11
0101000013 [N](01):Boot server: 10.10.104.63 path: Config/ Type: TFTP
0101000013 [N](01):RemCfg: Download request of Config/00087b077cd9.cfg from 10.10.104.63 using TFTP
0101000014 [N](01):accept called from task 7
0101000014 [N](01):TrelAccept success [4]. Listening on port 10010
0101000019 [N](01):RemCfg: Download request of Config/00087b077cd9.cfg from 10.10.104.63 using TFTP
0101000019 [W](01):Load of Config/00087b077cd9.cfg from 10.10.104.63 failed
```

To dump the log simply copy and paste the full contents.

5.21 SIP Logs

This page shows SIP server related messages that are logged during the operation of the SME system. The full native format of SIP logs is saved in the TFTP server as **<MAC_Address><Time_Stamp>SIP.log**
These logs are saved in 2 blocks of 17Kbytes. When a specific SIP log is fully dumped to one block, the next SIP logs are dumped to the other blocks.

An example of SIP logs is shown below:

```
.....
Sent to udp:192.168.10.10:5080 at 12/11/2010 11:56:42  (791 bytes)
REGISTER sip:192.168.10.10:5080 SIP/2.0
Via: SIP/2.0/UDP 192.168.10.101:5063;branch=z9hG4bKrlga4nkuhimpnj4.qx
Max-Forwards: 70
From: <sip:Ext003@192.168.10.10:5080>;tag=3o5l314
To: <sip:Ext003@192.168.10.10:5080>
Call-ID: p9st.zzrfff66.ah8
CSeq: 6562 REGISTER
Contact: <sip:Ext003@192.168.10.101:5063>
Allow: INVITE, CANCEL, BYE, ACK, REGISTER, OPTIONS, REFER, SUBSCRIBE, NOTIFY, MESSAGE, INFO, PRACK
Expires: 120
User-Agent: Generic-DPV-001-A-XX(Generic_SIPEXT2MLUA_v1)
Content-Type: application/X-Generic_SIPEXT2MLv1
Content-Length: 251
.....
```

To dump the log simply copy and page the full contents.

6 How-To setup a Multi Cell System

This chapter describes how to setup a multi cell system, add and synchronize one or multiple Base stations to the network.

NOTE: It is possible to have RTX8660 and Rove B4 in the same chain, but the features of the system will be reduced to RTX8660. This means that if a user has a multi cell system with 50x Rove B4 and adds 1x RTX8660, the system will run on the RTX8660 features and exclude the extra ones from Rove B4.

6.1 Adding Base stations

Here are the recommended steps to add Base stations to network:

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

STEP 2 Use one of the two methods to determine the Base station IP address.

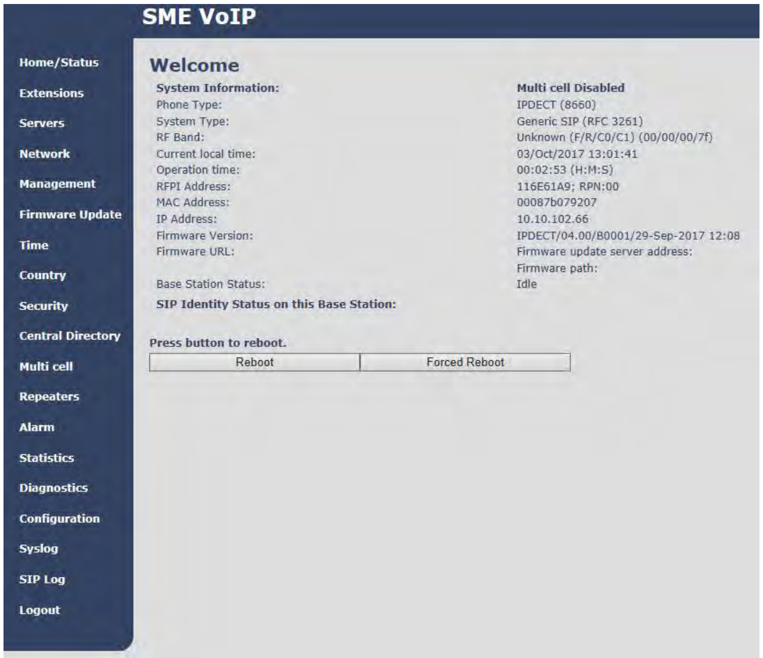
a. Use the IP find menu on the handset (enter the main Menu and type ***47***) to determine the IP address of the Base station by matching the MAC address on the back of the device with the MAC address list on the handset

b. Use the IPdect feature (for more details, go to chapter *3.5.2 Using Browser IPDECT*)

STEP 3 Open browser on the computer and type in the IP address of the base. Press “Enter” to access the base Login to the Base station.

STEP 4 Once you have been authenticated, the browser will display front end of the SME Configuration Interface. The front end will show relevant information of the Base station.

Screenshot



Welcome

System Information:	**Multi cell Disabled**
Phone Type:	IPDECT (8660)
System Type:	Generic SIP (RFC 3261)
RF Band:	Unknown (F/R/C0/C1) (00/00/00/7f)
Current local time:	03/Oct/2017 13:01:41
Operation time:	00:02:53 (H:M:S)
RFPI Address:	116E61A9; RPN:00
MAC Address:	00087b079207
IP Address:	10.10.102.66
Firmware Version:	IPDECT/04.00/B0001/29-Sep-2017 12:08
Firmware URL:	Firmware update server address:
	Firmware path:
Base Station Status:	Idle

SIP Identity Status on this Base Station:

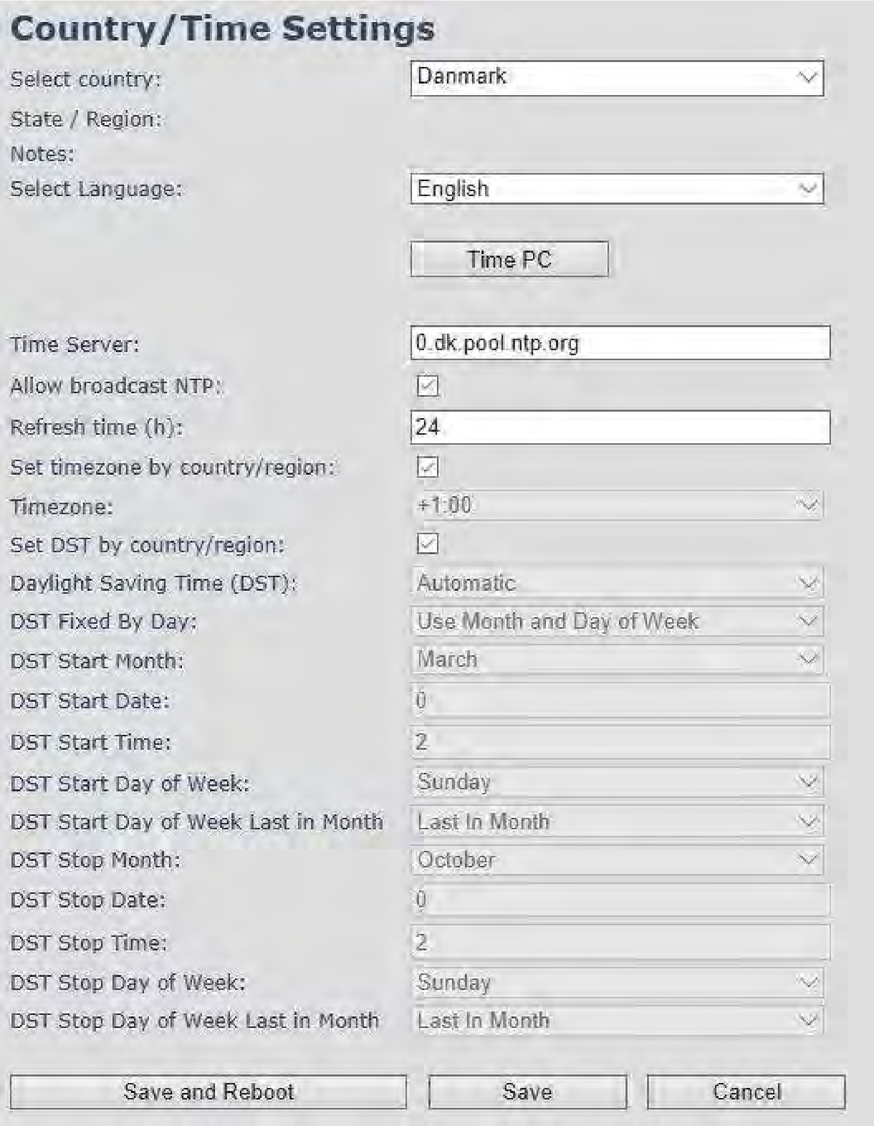
Press button to reboot.

6.1.1 Country and Time Server Setup

STEP 5 Navigate to the “Country” page and configure the country and time settings.
Use the PC time feature or enter the relevant parameters on this page and press the **Save and Reboot** button. Make sure there is contact to the “Time server” otherwise the Multi-cell feature will not work.

You can verify whether the Time server is reachable by rebooting the Base station and verifying that the correct Time Server IP address is still in place.

Screenshot



Country/Time Settings

Select country:	Danmark
State / Region:	
Notes:	
Select Language:	English
	Time PC
Time Server:	0.dk.pool.ntp.org
Allow broadcast NTP:	☑
Refresh time (h):	24
Set timezone by country/region:	☑
Timezone:	+1:00
Set DST by country/region:	☑
Daylight Saving Time (DST):	Automatic
DST Fixed By Day:	Use Month and Day of Week
DST Start Month:	March
DST Start Date:	0
DST Start Time:	2
DST Start Day of Week:	Sunday
DST Start Day of Week Last in Month	Last In Month
DST Stop Month:	October
DST Stop Date:	0
DST Stop Time:	2
DST Stop Day of Week:	Sunday
DST Stop Day of Week Last in Month	Last In Month

6.1.2 SIP Server (or PBX Server) Setup

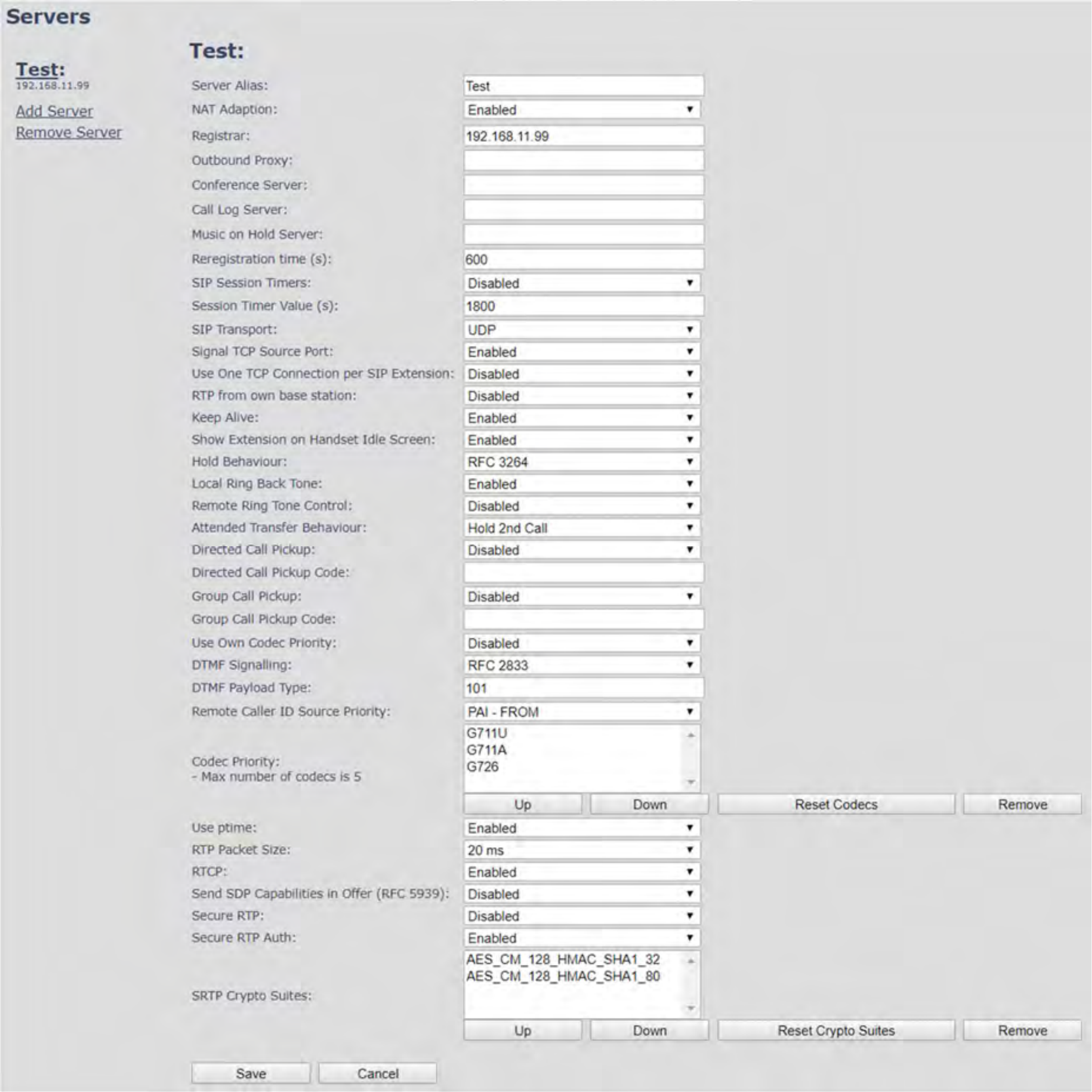
STEP 6 Create the relevant SIP server (or PBX Server) information in the system. Each service provider/customer should refer SIP server vendor on how to setup SIP servers.

a. Click the link **Server** at the left-hand column of home page. This is the place where you can add your SIP server for Base station use

b. Next, from the Server page, click on the **Add Server** URL and enter the relevant SIP server information (an example is shown below).

c. Choose **Disabled** on NAT adaption parameter if NAT function of the SIP aware router is not enabled. Enter the relevant parameters based on the description in the table below. Click **Save**.

Screenshot



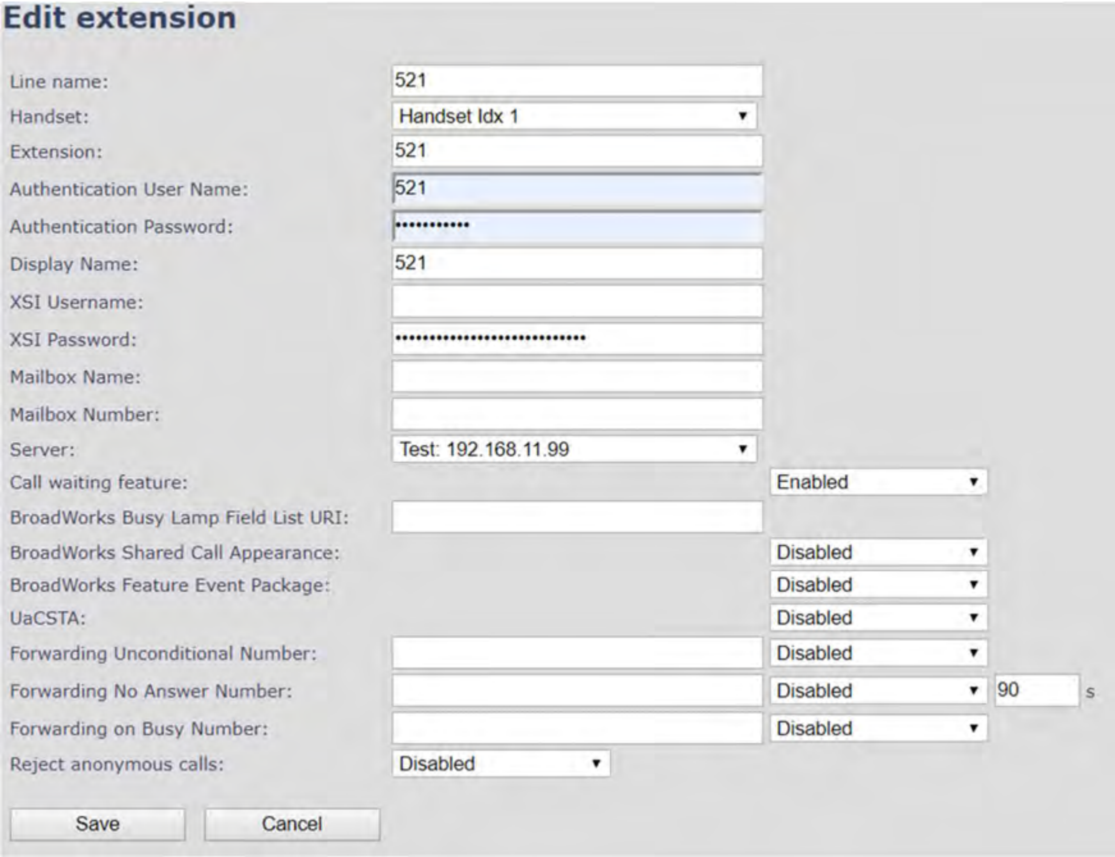
Test:

Server Alias:	Test
NAT Adaption:	Enabled
Registrar:	192.168.11.99
Outbound Proxy:	
Conference Server:	
Call Log Server:	
Music on Hold Server:	
Reregistration time (s):	600
SIP Session Timers:	Disabled
Session Timer Value (s):	1800
SIP Transport:	UDP
Signal TCP Source Port:	Enabled
Use One TCP Connection per SIP Extension:	Disabled
RTP from own base station:	Disabled
Keep Alive:	Enabled
Show Extension on Handset Idle Screen:	Enabled
Hold Behaviour:	RFC 3264
Local Ring Back Tone:	Enabled
Remote Ring Tone Control:	Disabled
Attended Transfer Behaviour:	Hold 2nd Call
Directed Call Pickup:	Disabled
Directed Call Pickup Code:	
Group Call Pickup:	Disabled
Group Call Pickup Code:	
Use Own Codec Priority:	Disabled
DTMF Signalling:	RFC 2833
DTMF Payload Type:	101
Remote Caller ID Source Priority:	PAI - FROM
Codec Priority: - Max number of codecs is 5	G711U G711A G726
Use ptime:	Enabled
RTP Packet Size:	20 ms
RTCP:	Enabled
Send SDP Capabilities in Offer (RFC 5939):	Disabled
Secure RTP:	Disabled
Secure RTP Auth:	Enabled
SRTP Crypto Suites:	AES_CM_128_HMAC_SHA1_32 AES_CM_128_HMAC_SHA1_80

6.1.3 Add an extension

STEP 7 And an extension before you move to the Multi Cell page. Go to **Extensions** – **Add Extension**. Fill out the extension data, and press **Save**

Screenshot

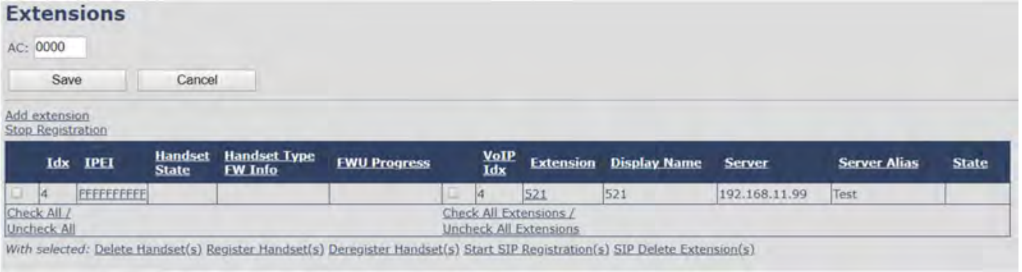


Edit extension

Line name:	521		
Handset:	Handset Idx 1 ▾		
Extension:	521		
Authentication User Name:	521		
Authentication Password:	•••••••••••		
Display Name:	521		
XSI Username:			
XSI Password:	•••••••••••••••••••••••••••		
Mailbox Name:			
Mailbox Number:			
Server:	Test: 192.168.11.99 ▾		
Call waiting feature:		Enabled ▾	
BroadWorks Busy Lamp Field List URI:			
BroadWorks Shared Call Appearance:		Disabled ▾	
BroadWorks Feature Event Package:		Disabled ▾	
UaCSTA:		Disabled ▾	
Forwarding Unconditional Number:		Disabled ▾	
Forwarding No Answer Number:		Disabled ▾	90 s
Forwarding on Busy Number:		Disabled ▾	
Reject anonymous calls:	Disabled ▾		

You will now see the extension on the Extensions page. You do not need to fully register the extension

Screenshot



Extensions

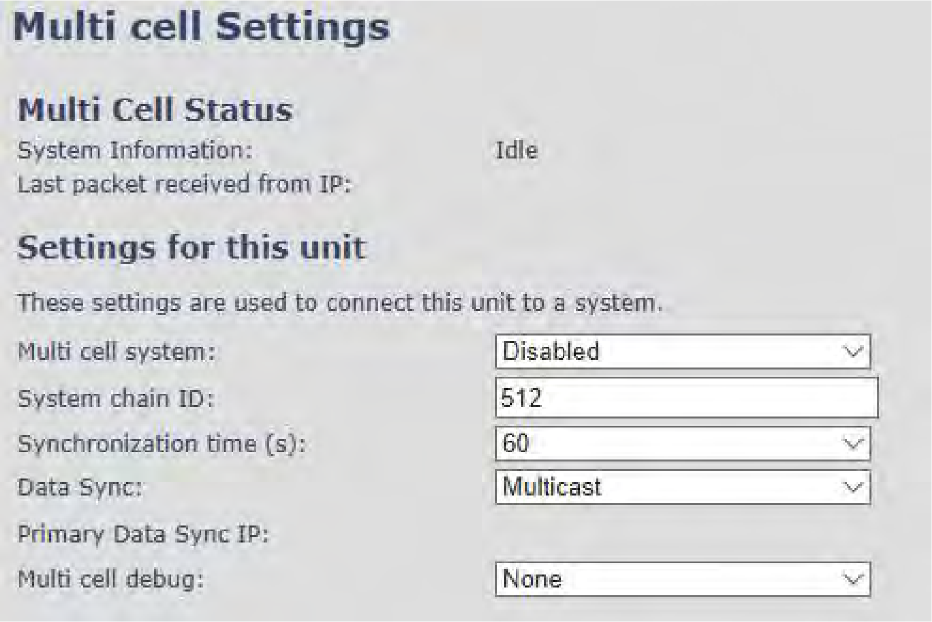
AC: 0000

	Idx	IPEI	Handset State	Handset Type FW Info	FWU Progress		VoIP Idx	Extension	Display Name	Server	Server Alias	State
□	4	FFFFFFFFFF				□	4	521	521	192.168.11.99	Test	

With selected: Delete Handset(s) Register Handset(s) Deregister Handset(s) Start SIP Registration(s) SIP Delete Extension(s)

STEP 8 Click on **Multi Cell** URL link from the left-handed menu to view the current Multi cell settings status of the current Base station. Brand new Base stations have **Multi cell system** feature disabled by default

Screenshot



Multi cell Settings

Multi Cell Status

System Information: Idle

Last packet received from IP:

Settings for this unit

These settings are used to connect this unit to a system.

Multi cell system: Disabled

System chain ID: 512

Synchronization time (s): 60

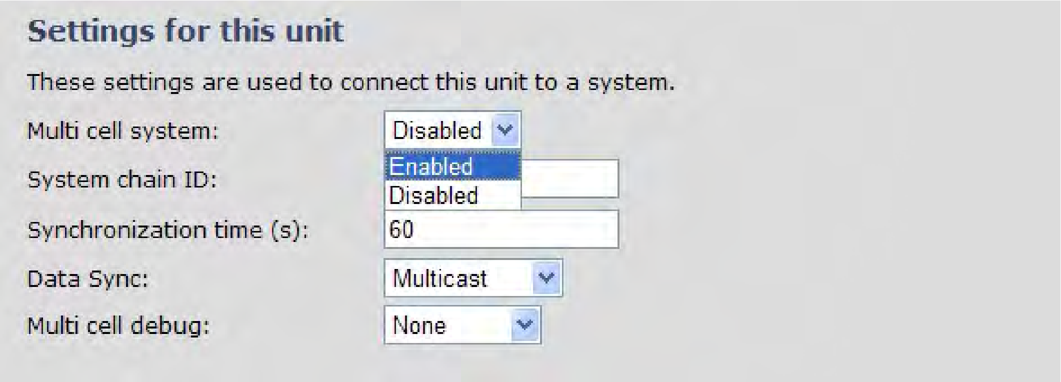
Data Sync: Multicast

Primary Data Sync IP:

Multi cell debug: None

STEP 9 Next, the system administrator needs to create and enable Multi cell Settings profile for the current Base station. On the **Multi Cell settings** Page, choose **Enable** option from the drop-down menu of the **Multi cell system** parameter. Enable the **Multi cell debug** option if the system administrator wants some Multi-cell related logs to be catalogued by the system.

Screenshot



Settings for this unit

These settings are used to connect this unit to a system.

Multi cell system: Disabled

System chain ID:

Synchronization time (s): 60

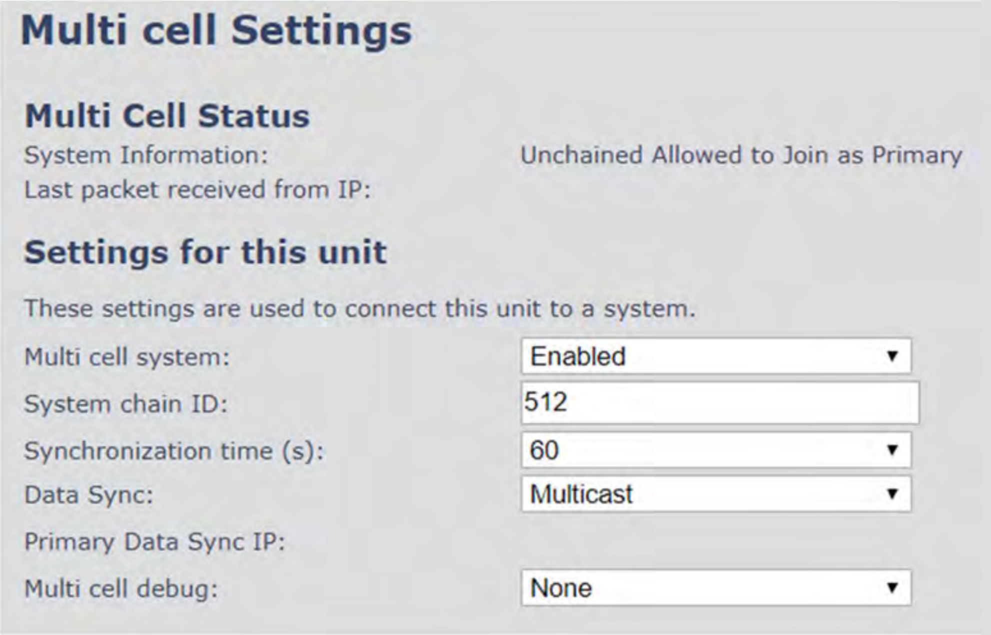
Data Sync: Multicast

Multi cell debug: None

STEP 10 On the same **Multi Cell Settings** page, enter the relevant values for **System chain ID** and **Synchronization time (s)** respectively. The **System chain ID** is a geographically unique DECT cell identity allocated to bridge several Base stations together in a chain. An example is **55555**. The **Synchronization time (s)** parameter is defined as period of time in seconds and ensures that a specific Base station synchronizes to the master Base station unit (by default 60).

NOTE: Do NOT use a chain ID similar to an extension.

Screenshot



Multi cell Settings

Multi Cell Status

System Information: Unchained Allowed to Join as Primary

Last packet received from IP:

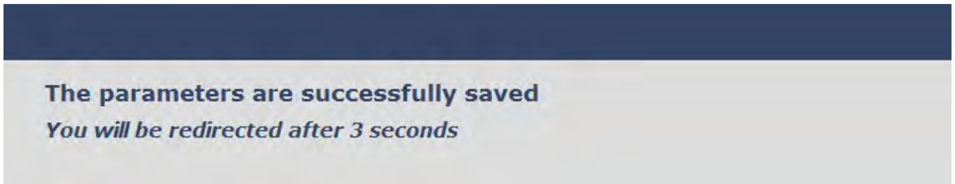
Settings for this unit

These settings are used to connect this unit to a system.

Multi cell system:	Enabled ▼
System chain ID:	512
Synchronization time (s):	60 ▼
Data Sync:	Multicast ▼
Primary Data Sync IP:	
Multi cell debug:	None ▼

Click the **Save** button to keep modified changes of multi cell settings into the Base station.

Screenshot



The parameters are successfully saved

You will be redirected after 3 seconds

NOTE: After you save, the System information changes status to "Unchained Allowed to Join as Primary"

NOTE: The Multi Cell data synchronization ONLY works when the relevant **Time Server** is set in the system before Server/Subscriber profile is added or created. Refer to **STEP 5**.

IMPORTANT: Base stations must be rebooted after the time server has been set.

IMPORTANT: Only the main Base station should have all data entered such as extensions, servers, time, etc. The secondary devices that are joining the Multi cell system should be defaulted.

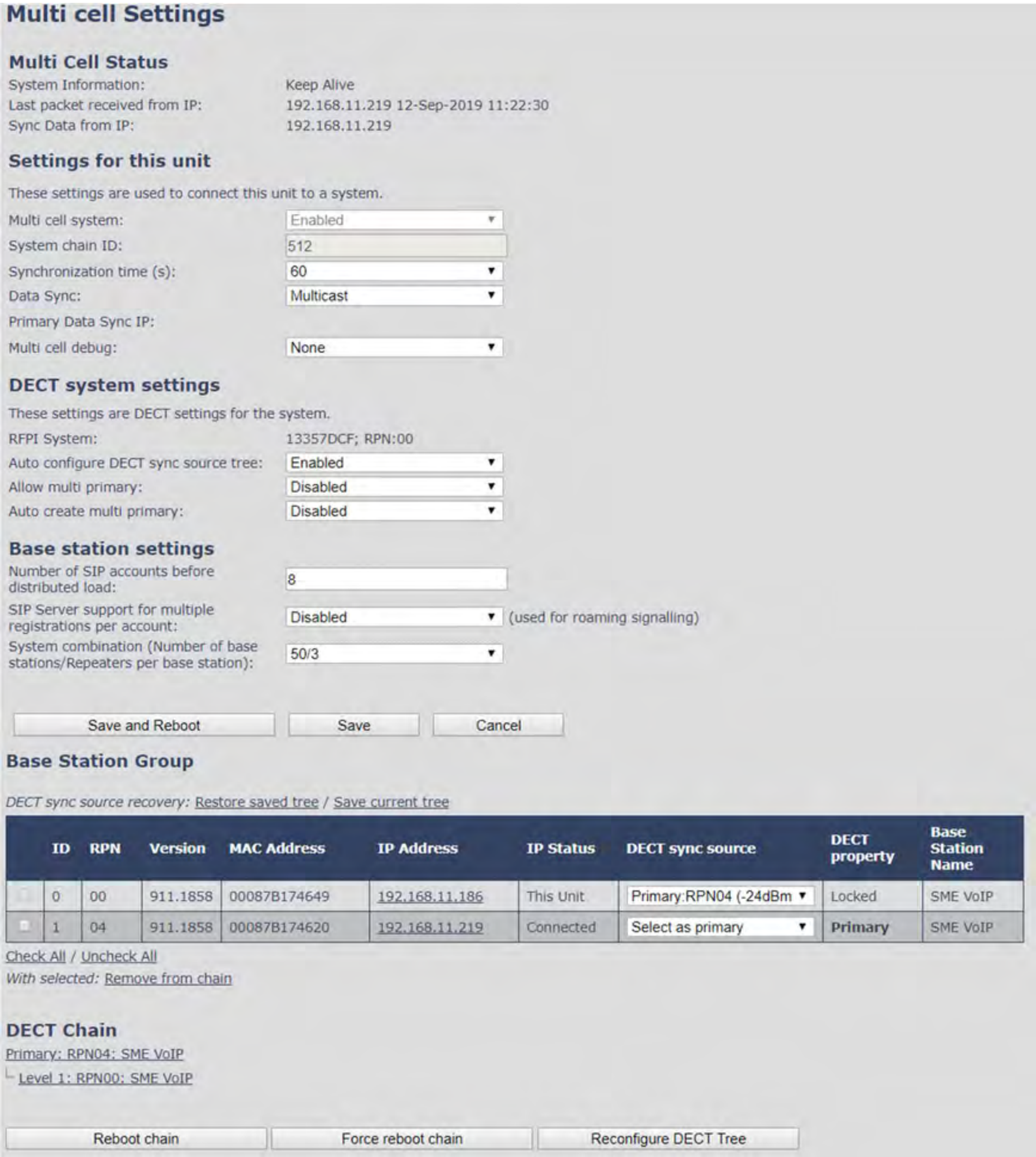
STEP 11 Logon to the Base station that you want to connect to the Multi Cell system.

STEP 12 Navigate to the multi Cell page and "Enable" **Multi Cell system**. Enter the **System Chain ID** that you used on the first Base station.

STEP 13 Press **Save and Reboot**

IMPORTANT: It takes up to 5 minutes (synchronization time) to add a new Base station to a Multi Cell System.

Screenshot



Multi cell Settings

Multi Cell Status

System Information: Keep Alive
Last packet received from IP: 192.168.11.219 12-Sep-2019 11:22:30
Sync Data from IP: 192.168.11.219

Settings for this unit

These settings are used to connect this unit to a system.

Multi cell system: Enabled
System chain ID: 512
Synchronization time (s): 60
Data Sync: Multicast
Primary Data Sync IP:
Multi cell debug: None

DECT system settings

These settings are DECT settings for the system.

RFPI System: 13357DCF; RPN:00
Auto configure DECT sync source tree: Enabled
Allow multi primary: Disabled
Auto create multi primary: Disabled

Base station settings

Number of SIP accounts before distributed load: 8
SIP Server support for multiple registrations per account: Disabled (used for roaming signalling)
System combination (Number of base stations/Repeaters per base station): 50/3

Base Station Group

DECT sync source recovery: Restore saved tree / Save current tree

	ID	RPN	Version	MAC Address	IP Address	IP Status	DECT sync source	DECT property	Base Station Name
□	0	00	911.1858	00087B174649	192.168.11.186	This Unit	Primary:RPN04 (-24dBm	Locked	SME VoIP
□	1	04	911.1858	00087B174620	192.168.11.219	Connected	Select as primary	**Primary**	SME VoIP

Check All / Uncheck All
With selected: Remove from chain

DECT Chain

Primary: RPN04: SME VoIP
└ Level 1: RPN00: SME VoIP

STEP 14 To add more Base stations, repeat **STEP 9-12**.

7 Adding Extensions

This section describes how to register the wireless handset to a Multi Cell system.

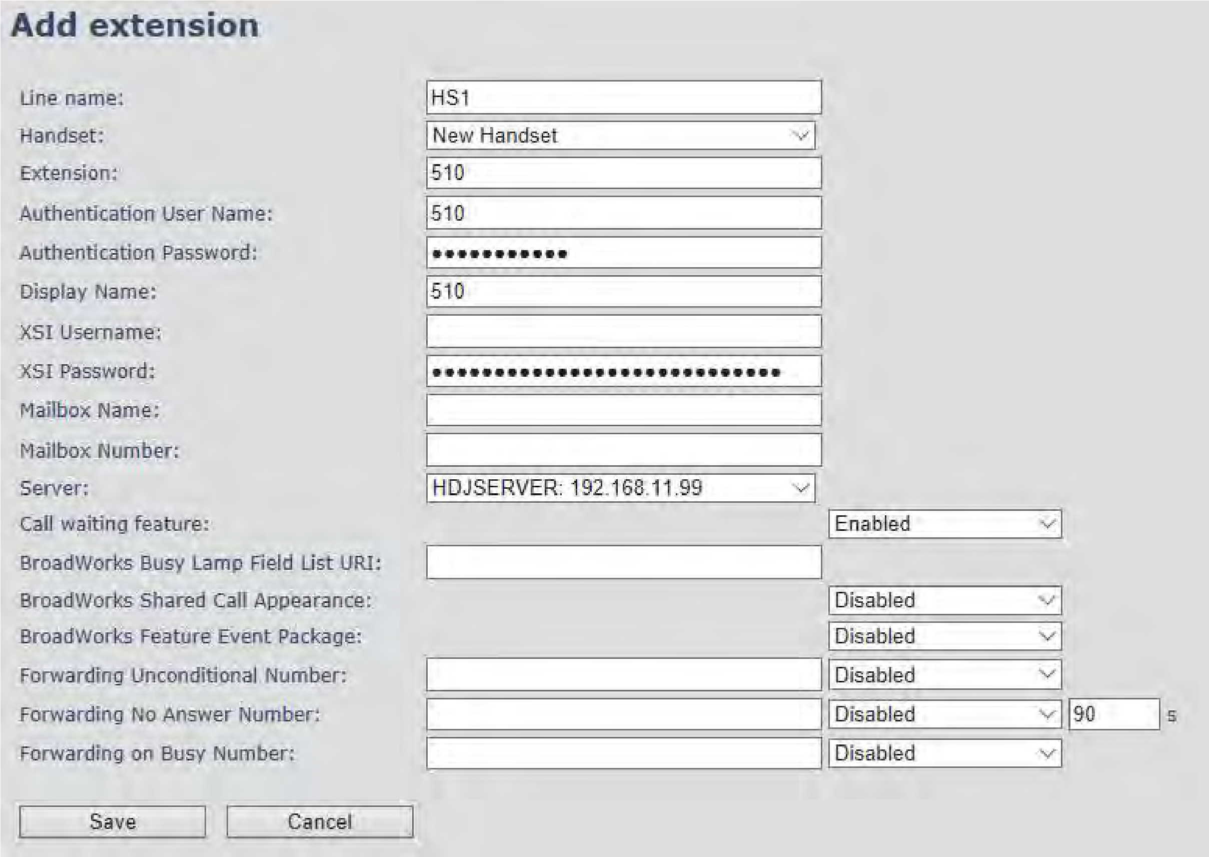
NOTE: Minimum one server must be registered to the base (system), otherwise a handset cannot be registered to the system. Please see chapter 6.1.2.

STEP 1 Login to a Base station.

STEP 2 Select the **Extensions** menu and click **Add extension**

STEP 3 Fill out the form and click **Save**. In the example below, we add the extension "510" and this SIP account got the same number as "Authentication User Name", "Password" and "Display Name".

Screenshot

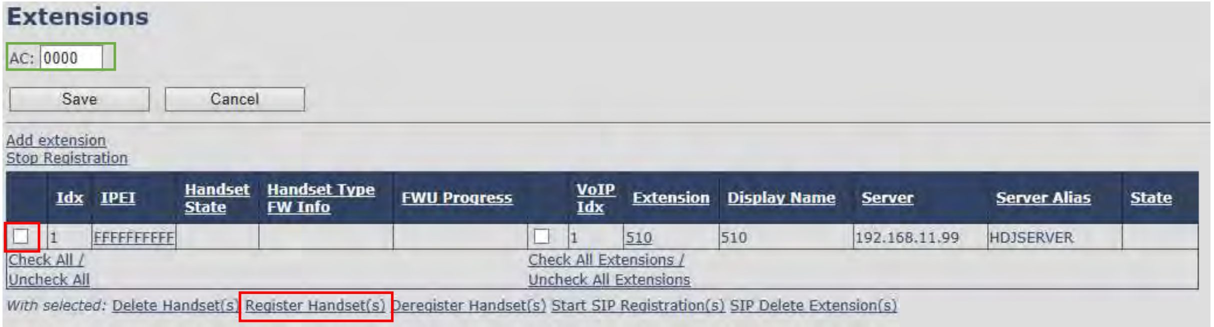


Add extension

Line name:	HS1			
Handset:	New Handset			
Extension:	510			
Authentication User Name:	510			
Authentication Password:	●●●●●●●●●●●			
Display Name:	510			
XSI Username:				
XSI Password:	●●●●●●●●●●●●●●●●●●●●●●●●●●●●●			
Mailbox Name:				
Mailbox Number:				
Server:	HDJSERVER: 192.168.11.99			
Call waiting feature:		Enabled		
BroadWorks Busy Lamp Field List URI:				
BroadWorks Shared Call Appearance:		Disabled		
BroadWorks Feature Event Package:		Disabled		
Forwarding Unconditional Number:		Disabled		
Forwarding No Answer Number:		Disabled	90	s
Forwarding on Busy Number:		Disabled		

STEP 4 In the handset and extensions list set a Check mark on the handset Idx, which you want to register and click **Register handset (s)**. The base is now open (in ready state) for handset registrations for 5 minutes

Screenshot



Extensions

AC: 0000

Save Cancel

Add extension
Stop Registration

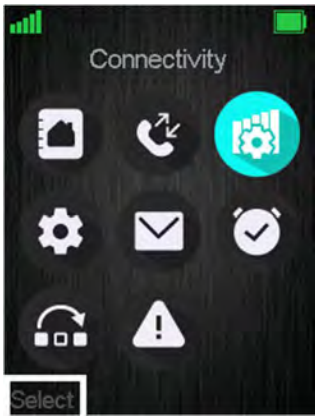
	Idx	IPEI	Handset State	Handset Type FW Info	FWU Progress		VoIP Idx	Extension	Display Name	Server	Server Alias	State
☐	1	FFFFFFFFFF				☐	1	510	510	192.168.11.99	HDJSERVER	

Check All / Uncheck All | Check All Extensions / Uncheck All Extensions

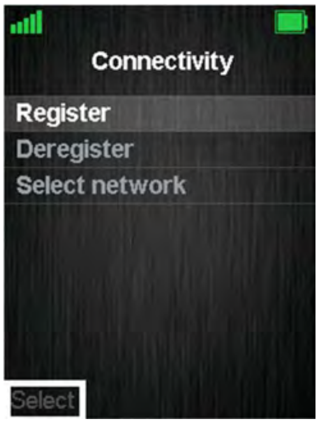
With selected: Delete Handset(s) Register Handset(s) Deregister Handset(s) Start SIP Registration(s) SIP Delete Extension(s)

STEP 5 Start the registration procedure on the handset by following step "a" to "d" below.

a) Select main menu "Connectivity"

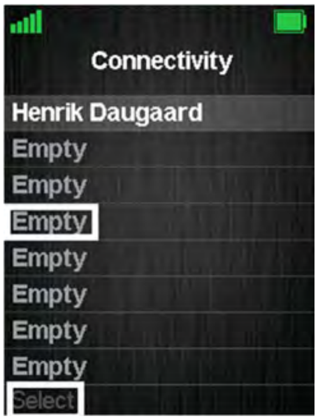


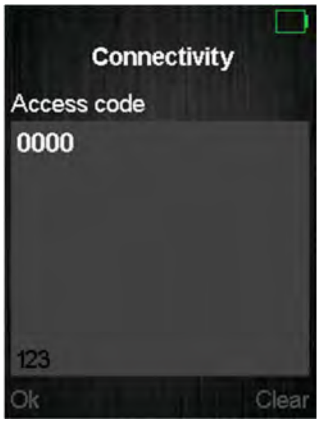
b) Select the menu "Register"



c) Select an empty spot in order to register the handset and enter the "Access code" which by default is "0000".

d) After a while the handset is registered, and the idle display is shown



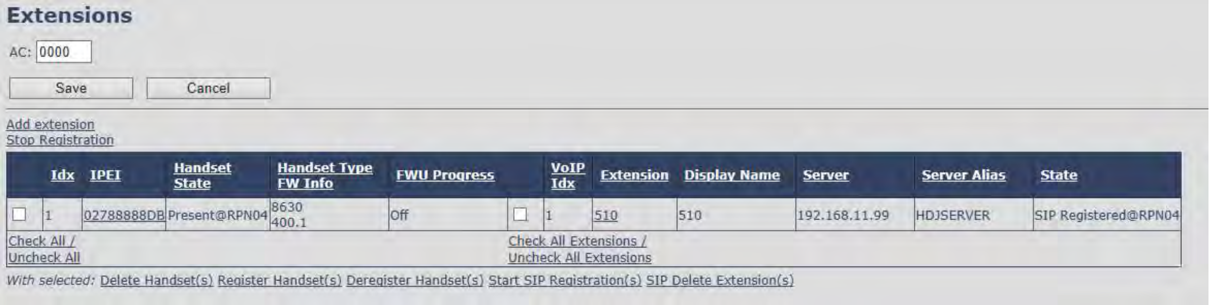


NOTE: The Access code (AC) is used to allow the handset to register to the base station. By default the value is 0000, but the user can change the AC to another numeric value. This can be done by editing the “AC” parameter, marked with green, on the Base screenshot from above.

STEP 6 Confirm the registration from the unique handset IPEI which is displayed in column “IPEI” when the handset is successfully registered.

NOTE: The web page must be manually updated by pressing “F5” to see that the handset is registered; otherwise the handset IPEI (International Portable Equipment Identity) isn’t displayed on the web page.

Screenshot



Extensions

AC: 0000

Save
Cancel
Add extension
Stop Registration

	Idx	IPEI	Handset State	Handset Type FW Info	FWU Progress		VoIP Idx	Extension	Display Name	Server	Server Alias	State
☐	1	02788888DB	Present@RPN04	8630 400.1	Off	☐	1	510	510	192.168.11.99	HDJSERVER	SIP Registered@RPN04

Check All / Uncheck All
Check All Extensions / Uncheck All Extensions
With selected: Delete Handset(s) Register Handset(s) Deregister Handset(s) Start SIP Registration(s) SIP Delete Extension(s)

STEP 7 Confirm the SIP registration by SIP State in right column.

NOTE: The web page must be manually updated by pressing “F5” to see that the handset is SIP registered; otherwise the handset SIP state isn’t displayed on the web page.

Repeat **STEP 2-7** for each handset you want to register.

8 Firmware Upgrade Procedure

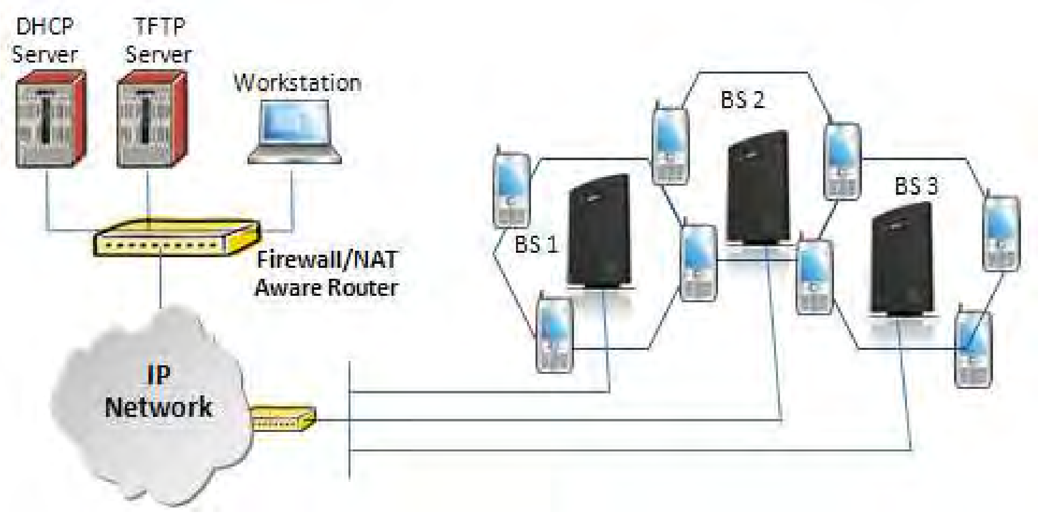
This step-by-step chapter describes how to upgrade or downgrade Base station(s) and/or handset(s) / repeater (s) to the relevant firmware provided by RTX.

8.1 Network Dimensioning

In principle, several hardware and software components should be available or be satisfied before Base station/handset update can be possible.

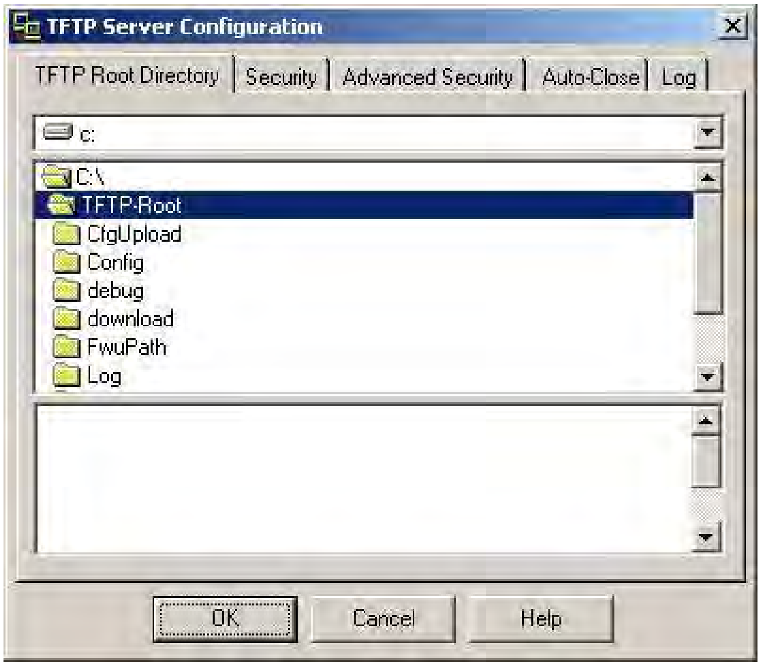
The minimum hardware and software components that are required to be able update via TFTP include the following (but not limited to):

- Handsets
- Base stations
- TFTP Server (Several Windows and Linux applications are available)
- DHCP Server (Several Windows and Linux applications are available)
- Workstation (e.g. Normal terminal or PC)
- Any standard browser (e.g. Firefox)
- Public/Private Network



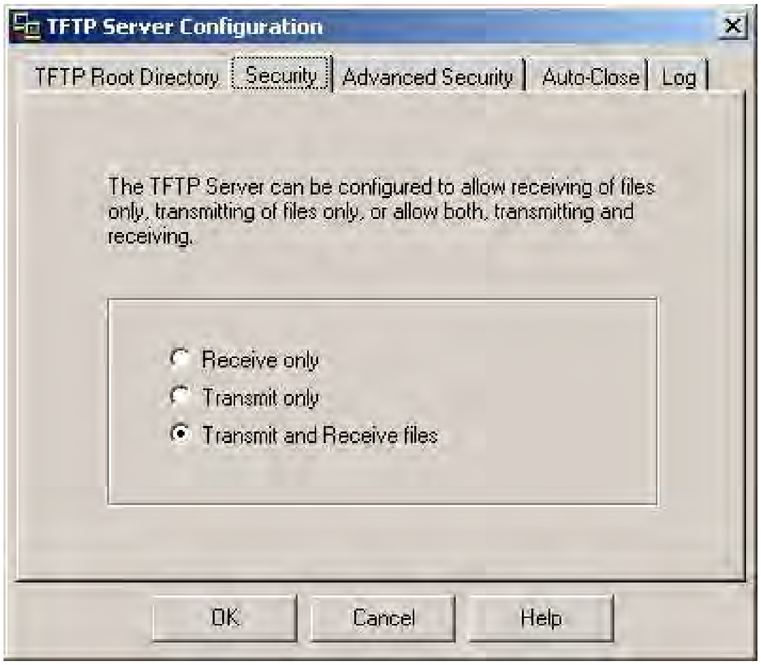
8.2 TFTP Configuration

This section illustrates TFTP Server configuration using “SolarWinds” vendor TFTP Server. Create the following relevant folders as shown in the snap shots and choose defaults settings for the remaining options and save.



c:

- C:\
  - TFTP-Root
    - CfgUpload
    - Config
    - debug
    - download
    - FwuPath
    - Log



The TFTP Server can be configured to allow receiving of files only, transmitting of files only, or allow both, transmitting and receiving.

○ Receive only
○ Transmit only
● Transmit and Receive files

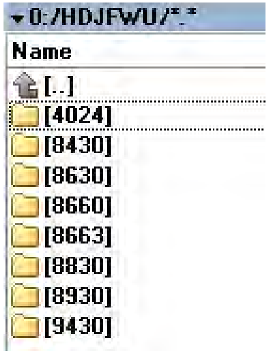
NOTE: If TFTP server timeout settings are too short firmware upgrade might not complete. Recommended time out setting is more than 3 seconds.

8.3 Create Firmware Directories

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)

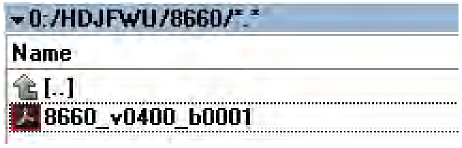
8.3.1 Base:

On the TFTP server root, create directory's as in screenshot.



```
0:/HDJFWU/*.*
Name
[..]
[4024]
[8430]
[8630]
[8660]
[8663]
[8830]
[8930]
[9430]
```

Copy Base station firmware to the named directory.

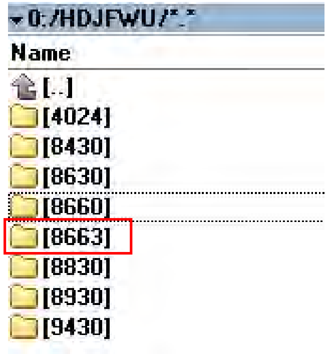


```
0:/HDJFWU/8660/*.*
Name
[..]
8660_v0400_b0001
```

IMPORTANT: The **8663** directory name cannot be changed.

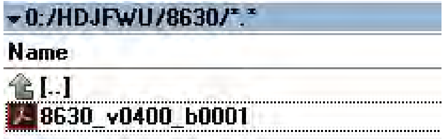
8.3.2 Handsets/Repeaters:

On the TFTP server root, create directory "8430" or "8630" or "8830" or "8930" or "4024" depending on type.



```
0:/HDJFWU/*.*
Name
[..]
[4024]
[8430]
[8630]
[8660]
[8663]
[8830]
[8930]
[9430]
```

Copy handset/repeater firmware to the named directory of each model.



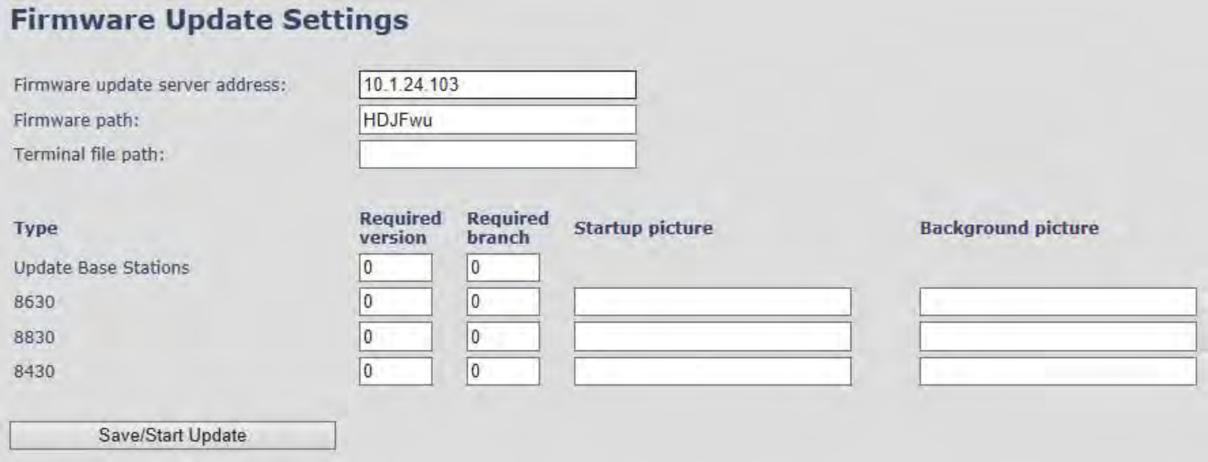
```
0:/HDJFWU/8630/*.*
Name
[..]
8630_v0400_b0001
```

IMPORTANT: The **8430, 8630,8830 and 8930** directory names cannot be changed.

8.4 Handset Firmware Update Settings

Scroll down and click on the **Firmware Update** URL link from the left-handed menu to view the Firmware Update Settings page.

Screenshot



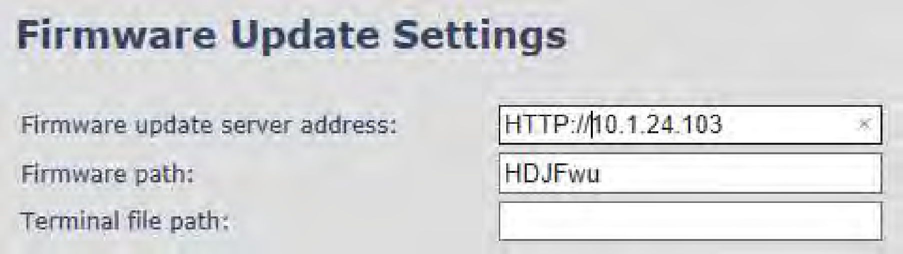
Firmware Update Settings

Firmware update server address:	10.1.24.103
Firmware path:	HDJFwu
Terminal file path:	

Type	Required version	Required branch	Startup picture	Background picture
Update Base Stations	0	0		
8630	0	0		
8830	0	0		
8430	0	0		

Type IP address and firmware path followed by save.
For Http download the firmware update server settings must be entered as follows:

Screenshot



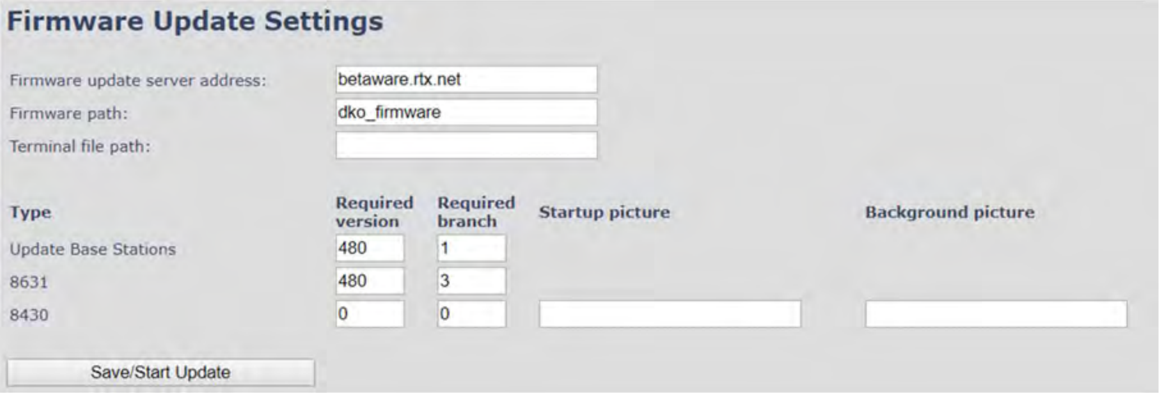
Firmware Update Settings

Firmware update server address:	HTTP://10.1.24.103
Firmware path:	HDJFwu
Terminal file path:	

8.5 Handset(s) and Repeater Firmware Upgrade

On the **Firmware Update Settings** page enter the relevant handset/repeater/Base station firmware for each device. Enter the required version (e.g. 440 for v440) and branch name (e.g. 1 for branch 01) to upgrade or downgrade. Afterwards, press the **Save/Start update** button to initialize the process of updating all devices.

Screenshot



Firmware Update Settings

Firmware update server address:	betaware.rtx.net
Firmware path:	dko_firmware
Terminal file path:	

Type	Required version	Required branch	Startup picture	Background picture
Update Base Stations	480	1		
8631	480	3		
8430	0	0		

NOTE: To disable handset/repeater/Base station firmware process, type version 0 in the required version field, followed by the **Save/Start update** button. It is recommended to use version 0 after all units are upgraded.

NOTE: For handset TFTP/HTTP download only one handset type can be downloaded at the same time. In case two handset models are defined for fwu at the same time, fwu will fail.

8.5.1 Monitor handset firmware upgrade

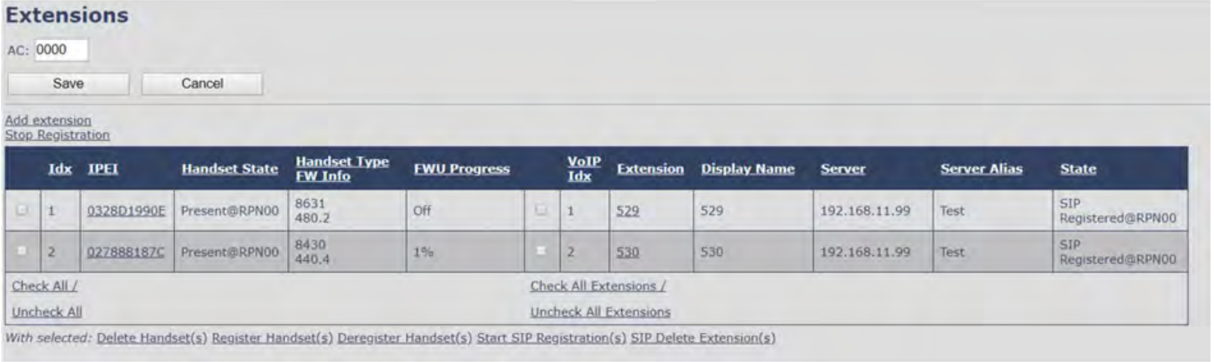
Handset firmware upgrade status is monitored on the **Extensions** page, "FWU Progress" column.

If the status says "Off" it means that the Required Version and Branch is set to "0" as it should be unless you're in process of updating/downgrading the firmware. The handset's firmware updating time is around 20- 40 minutes.

The firmware upgrade/downgrade process has 6 states:

- Initializing
- In progress (% from 0-100)
- Verifying (% 0-100)
- Waiting for charger (The handset must be placed in charge and NOT removed until it reboots)
- Complete
- Off

Screenshot



Extensions

AC: 0000

Save
Cancel
Add extension
Stop Registration

	Idx	IPEI	Handset State	Handset Type FW Info	FWU Progress		VoIP Idx	Extension	Display Name	Server	Server Alias	State
□	1	0328D1990E	Present@RPN00	8631 480.2	Off	□	1	529	529	192.168.11.99	Test	SIP Registered@RPN00
□	2	027888187C	Present@RPN00	8430 440.4	1%	□	2	530	530	192.168.11.99	Test	SIP Registered@RPN00

Check All /
Uncheck All
Check All Extensions /
Uncheck All Extensions
With selected: Delete Handset(s) Register Handset(s) Deregister Handset(s) Start SIP Registration(s) SIP Delete Extension(s)

8.5.2 Monitor Repeater firmware upgrade

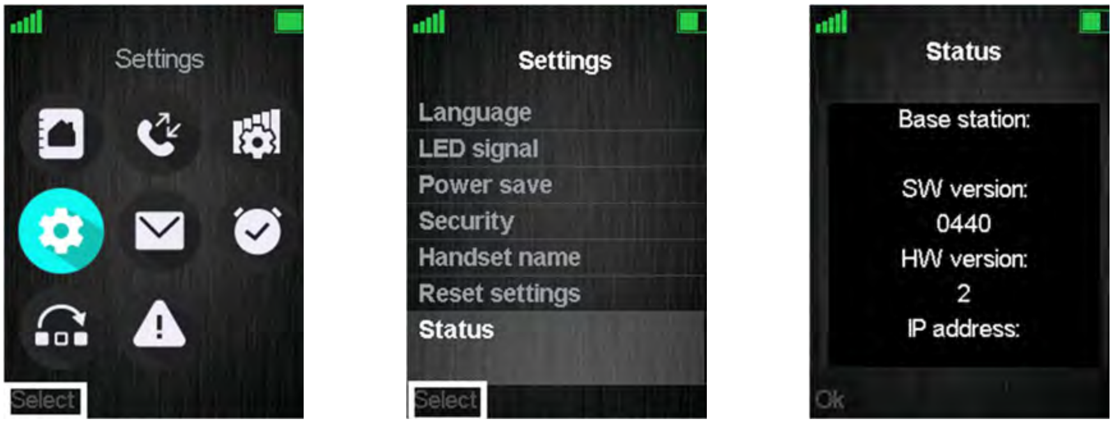
Repeater firmware upgrade status is monitored on the **Repeaters** page, under "FWU Progress".

The repeater's firmware updating time is around 20-30 minutes.

8.5.3 Verification of Firmware Upgrade

The firmware upgrade is confirmed by the "FWU Progress" status in the FWU Colum on the handset extension list or repeater list. The "FWU info" column contains the software version and the "FWU Progress" column contains the status. In case status is "Complete", the unit is firmware upgraded.

Alternatively, the handset firmware can be verified from the Handset **Menu** by navigating to **Settings** and scrolling down to **Status. Entering this menu** will list information regarding Base station and handset firmware versions.



Base station:

SW version:
0440
HW version:
2
IP address:

8.6 Base station(s) Firmware Upgrade

On the **Firmware Update** page, Base stations are updated in the same way as repeaters and handsets.

After entering the required version and required branch, choose **Save/Start update** button and select **OK** 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.

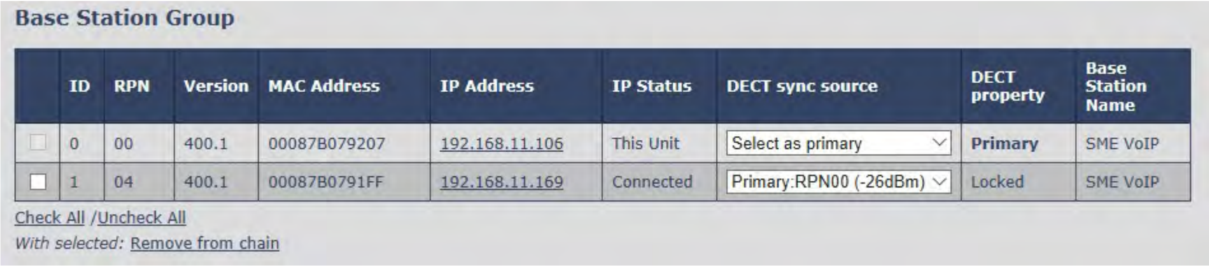
The base firmware update behavior is: Base will fetch the fwu file for approximately 3 minutes, then reboot and start flashing the LED again for approximately 3 minutes. Finally, it reboots in new version.

NOTE: All on-going voice calls are dropped from the Base station(s) immediately after the firmware update procedure has started.

8.6.1 Base firmware confirmation

Base station firmware version status in a multicell environment can be seen in the **Multi Cell** overview page, column 4 (Version).

Screenshot



Base Station Group

	ID	RPN	Version	MAC Address	IP Address	IP Status	DECT sync source	DECT property	Base Station Name
□	0	00	400.1	00087B079207	192.168.11.106	This Unit	Select as primary	Primary	SME VoIP
□	1	04	400.1	00087B0791FF	192.168.11.169	Connected	Primary:RPN00 (-26dBm)	Locked	SME VoIP

Check All /Uncheck All
With selected: Remove from chain

8.6.2 Verification of Firmware Upgrade

If the firmware upgrade/downgrade does not start, you can check the syslog to see if the path is right. First, go to **Management** and set the “Syslog Level” parameter to “Debug”. Press **Save** and afterwards click on the **Syslog** URL from the left-handed menu. On the displayed data it can be checked whether the upgrade/downgrade has been successful. Please see the example below of a failed firmware upgrade due to wrong path

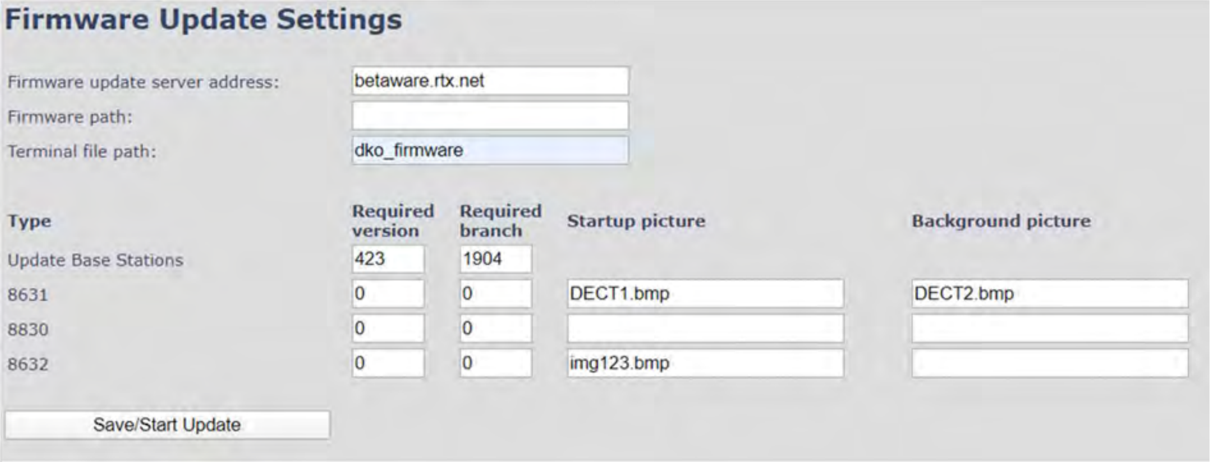
```
[ FWU Downloading File tftp://10.1.24.103/FwuPath/8663/8663_v0440_b0001.fwu]
[ Base FWU started]
[ Base FWU ended with exit code 2101 (NE_FILE_TRANSFER_EOF): End of file]
```

This is the path where the Base station expects to find the firmware:
tftp://10.1.24.103/FwuPath/8663/8663_v0440_b0001.fwu

If such lines can be seen on the output, please check if the path or firmware file is in the correct directory.

8.7 Upload startup/background picture to the handsets

As mentioned in the previous chapter *5.7 Firmware Update Definitions,* the system allows the user to upload a startup and background image to the handset. Before the upload has started, please make sure that the handsets are registered and present to the Base station.
To start the image upload, please go to the **Firmware Update settings** menu and type in the location of the images in the "Terminal file path" field. Afterwards, type in the name of the image you would like to be displayed when the handset is powered on and click **Save/Start Update.**



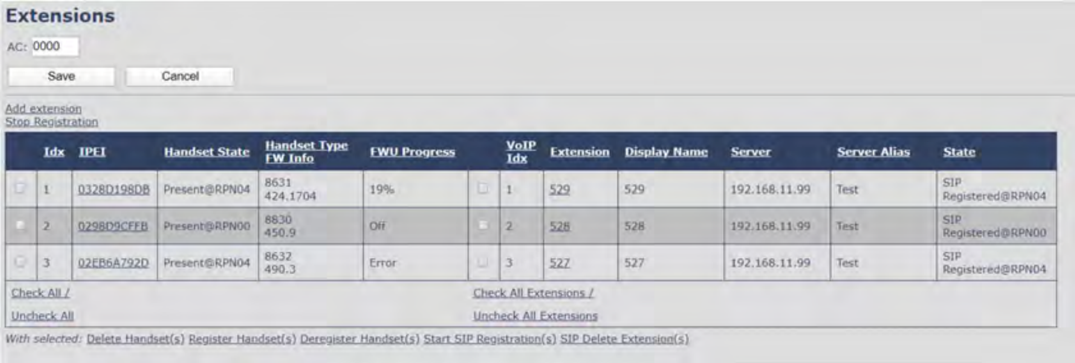
Firmware Update Settings

Firmware update server address:	betaware.rtx.net
Firmware path:	
Terminal file path:	dko_firmware

Type	Required version	Required branch	Startup picture	Background picture
Update Base Stations	423	1904		
8631	0	0	DECT1.bmp	DECT2.bmp
8830	0	0		
8632	0	0	img123.bmp	

The progress of the uploading can be seen on the **Extensions** menu, under the "FW Progress" column. Just like the normal firmware upgrade, the startup/background image upload will show progress in %. Afterwards, the handset should be placed in the charger when "Waiting for charger" message has been displayed. After restarting, the handset will be ready to use.

Note: If the file is not found, the "FWU Progress" column will display "Error".



Extensions

AC: 0000

	Idx	IPEI	Handset State	Handset Type FW Info	FWU Progress		VoIP Idx	Extension	Display Name	Server	Server Alias	State
□	1	0328D198DB	Present@RPN04	8631 424.1704	19%	□	1	529	529	192.168.11.99	Test	SIP Registered@RPN04
□	2	0298D9CFFB	Present@RPN00	8830 450.9	Off	□	2	528	528	192.168.11.99	Test	SIP Registered@RPN00
□	3	02EB6A792D	Present@RPN04	8632 490.3	Error	□	3	527	527	192.168.11.99	Test	SIP Registered@RPN04

Check All /
Uncheck All
Check All Extensions /
Uncheck All Extensions
With selected: Delete Handset(s) Register Handset(s) Deregister Handset(s) Start SIP Registration(s) SIP Delete Extension(s)

NOTE: If the image is not present after restarting, please reset the settings of the handset. Go to **Settings – Reset settings.**

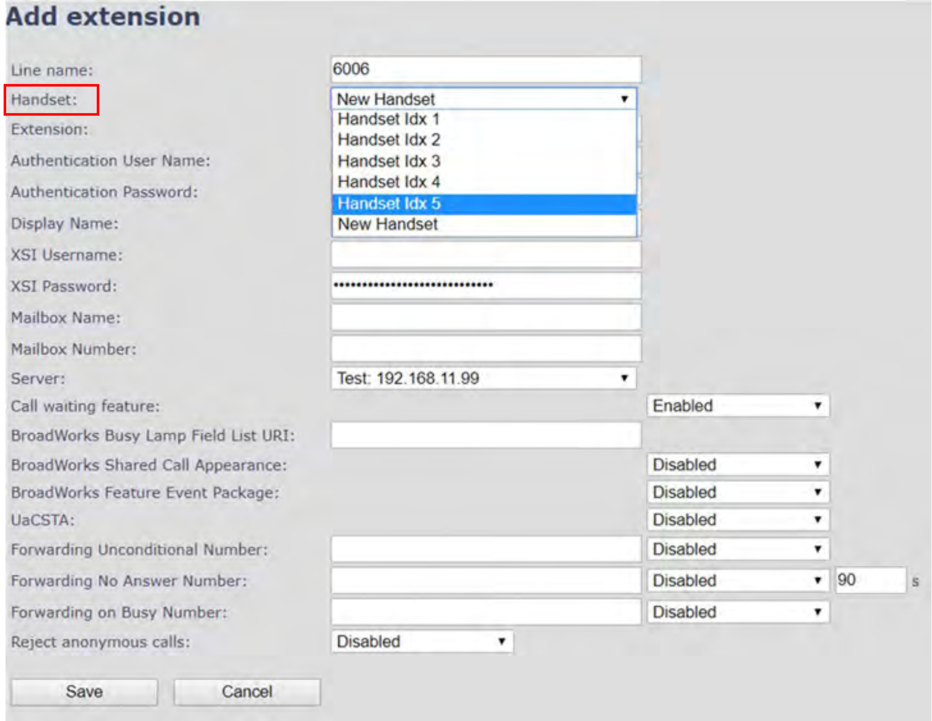
9 Multiline Feature

This section describes how to register the wireless handsets to a system with active multiline feature. One handset will be able to support up to 4 lines (4 different SIP accounts) ... A handset only supports 2 call appearances.
The limitation of maximum 1000 terminals in the system is maintained, and the maximum number of SIP registrations that one Base station can handle, is maintained.
With 4 lines pr. extension maximum number of terminals registered in a system is 250.
With 1-line pr. extension maximum number of terminals registered in a system is 1000.
Still the limitation of 30 SIP accounts registered pr. base is maintained.
With 4 lines (SIP accounts) pr. terminal maximum number of terminals registered pr. base is 7.
The 4 SIP accounts pr. terminal follow the location of the terminal similar.
With multiline feature enabled 200 contacts in contact list is possible.

9.1 How to setup Multiline.

STEP 1 Start by registering a handset as described above (*7 Appendix – Adding extensions*).

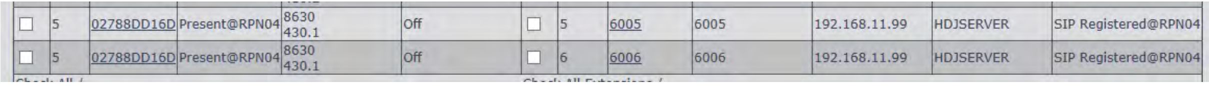
STEP 2 To add a multiline, select the existing handset that you want to add the multiline to, instead of "New handset" (in this case Handset Idx 1).



Add extension

Line name:	6006	
Handset:	New Handset ▾ Handset Idx 1 Handset Idx 2 Handset Idx 3 Handset Idx 4 Handset Idx 5 New Handset	
Extension:		
Authentication User Name:		
Authentication Password:		
Display Name:		
XSI Username:		
XSI Password:	••••••••••••••••••••••••••••	
Mailbox Name:		
Mailbox Number:		
Server:	Test: 192.168.11.99 ▾	
Call waiting feature:		Enabled ▾
BroadWorks Busy Lamp Field List URI:		
BroadWorks Shared Call Appearance:		Disabled ▾
BroadWorks Feature Event Package:		Disabled ▾
UaCSTA:		Disabled ▾
Forwarding Unconditional Number:		Disabled ▾
Forwarding No Answer Number:		Disabled ▾ 90 s
Forwarding on Busy Number:		Disabled ▾
Reject anonymous calls:	Disabled ▾	

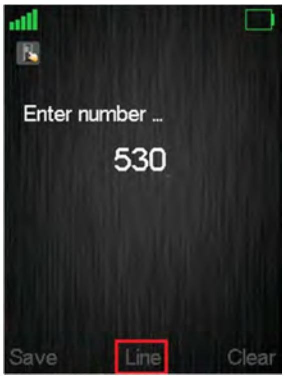
STEP 3 The extension will now show in the extension list with the same Idx and IPEI as the handset selected.
Note: The handset must be rebooted for the changes to take effect.



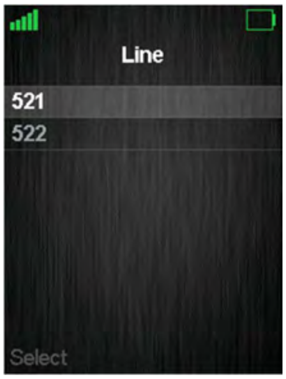
☐	5	02788DD16D	Present@RPN04	8630 430.1	Off	☐	5	6005	6005	192.168.11.99	HDJSERVER	SIP Registered@RPN04
☐	5	02788DD16D	Present@RPN04	8630 430.1	Off	☐	6	6006	6006	192.168.11.99	HDJSERVER	SIP Registered@RPN04

The handset will now have two numbers 521 and 522.

When making call the user can chose which line to call from. Simply enter the number to call and press line. Select the desired line and hook off to place the call from this line.


Enter number ...

530



10 Functionality Overview

So far, a SME VoIP system has been set up. Next, in this chapter we list what features and functionalities are available in the system. The SME VOIP system supports all traditional and advanced features of most telephony networks. In addition, 3rd party components handle features like voice mail, call forward, conference calls, etc. A brief description of SME VOIP network functionalities is:

- **Outgoing/incoming voice call management:** The SME VOIP system can provide multiple priority user classes. Further, up to 3 repeaters can be linked to a Base-station.
- **Internal handover**: User locations are reported to SIP Server to provide differentiated services and tariff management. Within a DECT traffic area, established calls can seamlessly be handovered between Base-stations using connection handover procedures.

- **Security:** The RTX SME VOIP system also supports robust security functionalities for Base-stations. Most security[2] functionalities are intrinsically woven into the SME VOIP network structure so that network connections can be encrypted, and terminal authentication can be performed.

10.1 Gateway Interface

CONNECTOR INTERFACES	
POWER	Connector: Ethernet PoE (Ethernet adaptor for normal power) IEEE 802.3: Power class 2 (3.84 – 6.49W)
LAN INTERFACE	Standard : 10BASE-T(IEEE 802.3 100Mbps) Connector: RJ45 8/8
INTERNET PROTOCOL:	• IPv4 • IPv6
KEYS	
	1 x Reset key
LED INDICATOR	
	One Status LED (multicolor, red, green, orange)
RF	
FREQUENCY BANDS	1880 – 1900 MHz (EMEA) 1910 – 1930 MHz (Latam) 1920 – 1930 MHz (USA) These are software settings and need to be set when the Base station is packed in factory.
OUTPUT POWER	<250 mW (for USA < 140mW)
ANTENNA	Two antennas for diversity
SOFTWARE UPDATE	
DOWNLOADABLE	Remote firmware update HTTPS/TFTP

[2] With active security with authentication 4 channels are supported

10.2 System security support details

10.2.1 TLS 1.2

The base station supports TLS 1.2 with the following algorithms:

TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
TLS_DHE_RSA_WITH_AES_256_CBC_SHA
TLS_DHE_RSA_WITH_AES_128_CBC_SHA256
TLS_DHE_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_AES_256_CBC_SHA256
TLS_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_AES_128_CBC_SHA256
TLS_RSA_WITH_AES_128_CBC_SHA

The base station’s provided server services is limited to the following:

TLS_RSA_WITH_AES_256_CBC_SHA256
TLS_RSA_WITH_AES_128_CBC_SHA256
TLS_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_AES_128_CBC_SHA

10.2.2 SRTP

SRTP is supported according to RFC 3711 and RFC4568 with the following two crypto suites:

AES_CM_128_HMAC_SHA1_32
AES_CM_128_HMAC_SHA1_80

10.2.3 DECT

In terms of DECT, the following is supported:

DECT Standard Authentication Algorithm (DSAA)
DECT encryption services with the DECT Standard Cipher (DSC) with a 35-bit initialization vector and encrypting the voice stream with 64-bit encryption

10.2.4 Certificate support

DER encoded binary X.509 RSA 0-4096 bit (SHA-1 or SHA-256) certificates.

10.2.5 HTTPS

HTTPS can be used for:

Management transfer protocol
FWU download
Configuration download
Build in webserver.

10.2.6 Mutual TLS authentication (mTLS)

SIP via TLS with mutual authentication is supported.
Mutual authentication towards FWU and Configuration https server is supported.

10.2.6.1 mTLS Setup

STEP 1 Prepare an HTTPS web server with Trusted Server Certificates installed and running
STEP 2 Install Device identity Certificates on BASE WebUI / Security
STEP 3 Install Trusted Server Certificates on BASE WebUI / Security
STEP 4 Install Trusted Root Certificates on BASE WebUI / Security
STEP 5 Use Only Trusted Certificates is enabled on BASE WebUI / Security

10.3 Detail Feature List

CODECs	
G.711 PCM A-LAW & U-LAW	Uncompressed voice Silence suppression (No)
G.722	Allows HD sound for the handset
G.726	ADPCM, 32 Kbps
G.729	A G.729.1 (ehem. G.729 EV) Note: Only with additional module - an extra option that requires a board connector mounted in Gateway. Per default not mounted.
OPUS	Support in NB and WB Note: Only with additional module - an extra option that requires a board connector mounted in Gateway. Per default not mounted.
BV32	Reducing delay and complexity, while maintaining high audio quality
SIP	
RFC2327	SDP: Session Description Protocol
RFC2396	Uniform Resource Identifiers (URI): Generic Syntax
RFC2833	In-Band DTMF/Out of band DTMF support
RFC2976	The SIP INFO method
RFC3261	SIP 2.0
RFC3262	Reliability of Provisional Responses in the Session Initiation Protocol (PRACK)
RFC3263	Locating SIP Servers (DNS SRV, redundant server support)
RFC3264	Offer/Answer Model with SDP
RFC3265	Specific Event Notification
RFC3311 RFC3325	The Session Initiation Protocol UPDATE Method P-Asserted Identity
RFC3326	The Reason Header Field for the Session Initiation Protocol (SIP)
RFC3489	STUN
RFC3515	REFER: Call Transfer
RFC3550	RTP: A Transport Protocol for Real-Time Application
RFC3581	Rport
RFC3842	Message Waiting Indication
RFC3891	Replace header support
RFC3892	The Session Initiation Protocol (SIP) Referred-By Mechanism
RFC3960	Early Media and Ringing Tone Generation in the Session Initiation Protocol (SIP)
RFC4475	Session Initiation Protocol (SIP) Torture Test Messages
SIPS	

SRTP	Will limit number of active calls pr. base when enabled.
WEB SERVER	
	Embedded web server HTTP
OTHER FEATURES	
QUALITY OF SERVICE	Type of Service (ToS) including DiffServ Tagging, and QoS per IEEE 802.1p/q
IP QUALITY	Warning – Network outage, VoIP service outage
	Adaptive Jitter Buffer support
AUTOMATIC DST	
TONE SCHEME	Country Depend Tone Scheme
ETHERNET FEATURES	
SPEED DUPLEX	10 & 100 duplex
VLAN	VLAN (802.1p/q)
DHCP SUPPORT	
STATIC IP	
TLS 1.2srtp	For secure connections (SCA-256)
TFTP	For configuration download.
HTTP	For configuration download.
HTTPS	For secure configuration download.
TCP/IP/UDP	
SNTP	For internet clock synchronization
QUALITY OF SERVICE	Type of Service (ToS) including DiffServ Tagging, and QoS per IEEE 802.1p/q
DHCP OPTION	66
DNS SRV	
DECT	
DECT CAP	Connectionless handover, enhanced location registration
CAT-IQ V1.0	Wideband Speech
GENERAL TELEPHONY	
HANDSET SUPPORT	10 simultaneous handsets supported (single cell) (10 call / single cell and 8 call/Multi cell) Total 1000 simultaneous call supported / system
VOIP ACCOUNTS	30 VoIP accounts per base – (maximum 254 bases per installation) Total 1000 VoIP accounts / system
	Maximum 1000 handsets per installation
SIMULTANEOUS CALLS	4 Wideband calls (g.722) or 10 single cell, 8 multi cell narrowband calls (PCMA, PCMU, G.726) or mixed wideband and narrowband.
CALL FEATURES	Codec Negotiation
	Codec Switching
	Missed call notification
	Voice message waiting notification
	Date and Time synchronization
	Parallel calls
	Common parallel call procedures
	Call transfer unannounced
	Call transfer announced
	Conference
	Call Waiting
	Calling line identity restriction
	Outgoing call
	Call Toggle
	Incoming call
	Line identification
	Multiple Lines

	Multiple calls
	Call identification
	Calling Name Identification Presentation (CNIP)
	Calling Line Identification Presentation (CLIP)
	Call Hold
	List of registered handsets
CALL LOG	50 mixed between Incoming, outgoing, missed calls
PHONE BOOK	Common Phonebook with up to 3000 entries (Import via csv format)
	Common Phonebook LDAP V2.0
	Local Phonebook (100 entries 8630 and 50 entries 8430)
DND	Do Not Disturb
CALL FORWARD	All
	No Answer
	Busy
	Individual Speed dial
	Programmable Function keys

Appendix

11 Appendix A: Basic Network Server(s) Configuration

In this chapter, we describe how to setup the various server elements in the system.

11.1 Server setup

In the network, the server environment is installed as a centralized system.
The main server types hosted on the network include SIP, DNS/DHCP and HTTP/TFTP Servers. These servers can be hosted both in one or multiple windows and/or Linux Server environment.
Management servers are normally installed to monitor and manage the network in detail. Each Base-station status can be checked. Each Subscriber Terminal can be monitored over the air from a centralized location.
Further, new software can be uploaded to all system elements from the centralized location (typically a TFTP server) on an individual basis. This includes Subscriber Handsets where the latest software is downloaded over the air.

11.2 Requirements

Regardless of whether you will be installing a centrally provisioned system, you must perform basic TCP/IP network setup, such as IP address and subnet mask configuration, to get your organization's phones up and running.

11.3 DNS Server Installation/Setup

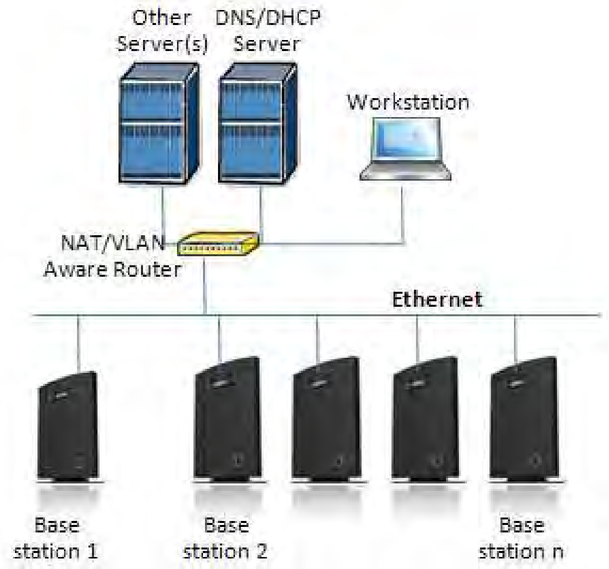
Name server is a name server service installed in a server for mapping or resolution of humanly memorable domain names and hostnames into the corresponding numeric Internet Protocol (IP) addresses.
The customer should refer to the platform vendor either windows or Linux vendor for detail step-by-step guide on how to install and configure Domain Name System for internet access. In this section, we briefly describe hints on how to setup DNS behind NAT or Firewall.

11.3.1.1 Hints on how to Configure DNS behind a Firewall/NAT

Proxy and Network Address Translation (NAT) devices can restrict access to ports. Set the DNS to use UDP port 53 and TCP port 53. For windows Servers, set the RCP option on the DNS Service Management console and configure the RCP to use port 135.
These settings should be enough to resolve some of potential issues that may occur when you configure DNS and firewalls/NAT.

11.4 DHCP Server Setup

A DHCP Server allows diskless clients to connect to a network and automatically obtain an IP address. This server is capable of supplying each network client with an IP address, subnet mask, default gateway, an IP address for a WINS server, and an IP address for a DNS server. This is very often used in enterprise networks to reduce configuration efforts. All IP addresses of all computers/routers/bases are stored in a database that resides on a server machine.



The network administrator should contact the relevant vendors for detail information or step-by-step procedure on how to install and setup DHCP process or service on windows/Linux servers. In this section, we will provide some hints of how to resolve potential problems to be encountered you setup DHCP Servers.

11.4.1 Hint: Getting DHCP Server to Work

Windows Server:

1) **Clients are unable to obtain an IP address**
   If a DHCP client does not have a configured IP address; it generally means that the client has not been able to contact a DHCP server. This is either because of a network problem or because the DHCP server is unavailable. If the DHCP server has started and other clients have been able to obtain a valid address, verify that the client has a valid network connection and that all related client hardware devices (including cables and network adapters) are working properly.
2) **The DHCP server is unavailable**
   When a DHCP server does not provide leased addresses to clients, it is often because the DHCP service has failed to start. If this is the case, the server may not have been authorized to operate on the network. If you were previously able to start the DHCP service, but it has since stopped, use Event Viewer to check the system log for any entries that may explain the cause.

Next, restart the DHCP service, click **Start**, click **Run**, type **cmd**, and then press ENTER. Type
net start dhcpserver, and then press ENTER.

Linux Platform:
Troubleshooting DHCP, check the following:

1) Incorrect settings in the **/etc/dhcpd.conf** file such as not defining the networks for which the DHCP server is responsible;
2) NAT/Firewall rules that block the DHCP **bootp** protocol on UDP ports 67 and 68;
3) Routers failing to forward the **bootp** packets to the DHCP server when the clients reside on a separate network. Always check your /var/logs/messages file for dhcpd errors.
4) Finally restart the **dhcpd** service daemon

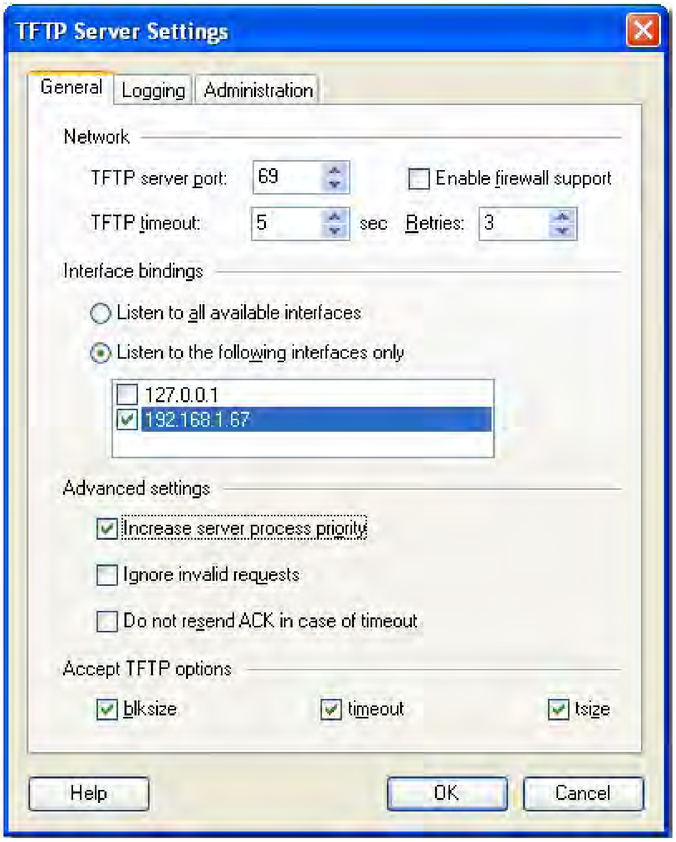
11.5 TFTP Server Setup

There are several TFTP servers in the market place; in this section, we describe how to setup a commonly used TFTP Server.

11.5.1 TFTP Server Settings

The administrator must configure basic parameters of the TFTP application:
Specify UDP 69 port – for TFTP incoming requests and TCP 12000 – for remote management of the server. For file transmission, the server opens UDP ports with random numbers. In case the option **Enable NAT or firewall support** is activated on the server, the server uses the same port for files transmission and listening to the TFTP incoming requests (UDP 69 port on default).
Specify the interface bindings, TFTP root directory, port which the TFTP Server will listen, timeout and number of retries, and TFTP options supported by the server.

Screenshot



Network
TFTP server port: 69 □ Enable firewall support
TFTP timeout: 5 sec Retries: 3

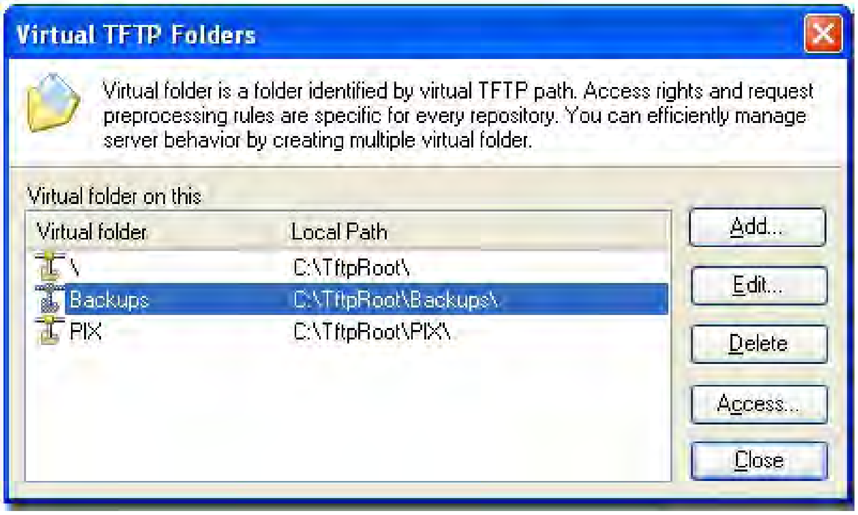
Interface bindings
○ Listen to all available interfaces
● Listen to the following interfaces only
□ 127.0.0.1
☑ 192.168.1.67

Advanced settings
☑ Increase server process priority
□ Ignore invalid requests
□ Do not resend ACK in case of timeout

Accept TFTP options
☑ blksize ☑ timeout ☑ tsize

Configure the relevant TFTP virtual folder in the server. The TFTP virtual folder is the file folder, visible for TFTP clients under a certain name. You can set security settings separately for every virtual TFTP folder. Next, set rights to access TFTP folders according to the relevant clients.

Screenshot



Virtual TFTP Folders

Virtual folder is a folder identified by virtual TFTP path. Access rights and request preprocessing rules are specific for every repository. You can efficiently manage server behavior by creating multiple virtual folder.

Virtual folder on this

Virtual folder	Local Path
\	C:\TftpRoot\
Backups	C:\TftpRoot\Backups\
PIX	C:\TftpRoot\PIX\

11.6 SIP Server Setup

SIP server is one of the main components of a network, dealing with the setup of all SIP calls in the network. A SIP server is also referred to as a SIP Proxy or a Registrar.
Although the SIP server is the most important part of the SIP based phone system, some servers only handles call setup and call tear down. It does not actually transmit or receive any audio. This is done by the media server in RTP.

12 Appendix B: Using Base with VLAN Network

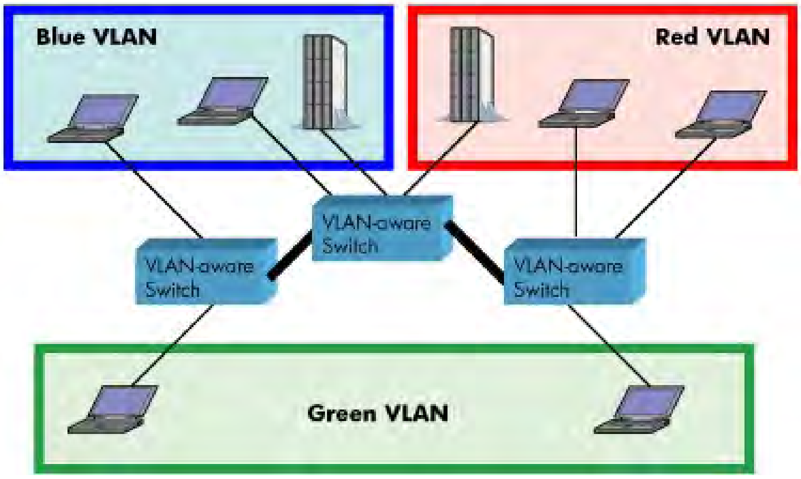
In this chapter, we describe how to setup a typical VLAN in the network.

12.1 Introduction

In this chapter, we describe how to setup VLAN to typical network. There are three main stages involved in this procedure:

a) Configure a VLAN Aware Switch to a specific (un)tagged VLAN ID, so the system can process untagged frames forwarded to it.
b) Setup the Time Server (NTP Server) and other relevant network servers.
c) Configure the HTTP server in the Base station to access the features in the PBX or system.

VLAN allows administrators to separate logical network connectivity from physical connectivity analogous to traditional LAN which is limited by its physical connectivity. Normally, users in a LAN belong to a single broadcast domain-and communicate with each other at the Data Link Layer or “Layer 2”. LANs are segmented into smaller units for each IP subnets and here communication between subnets is possible at the Network Layer or “Layer 3”, using IP routers.
A VLAN can be described as a single physical network that can be logically divided into discrete LANs that can operate independently of each other.
An Illustration of using VLANs to create independent broadcast domains across switches is shown below:



The figure above highlights several key differences between traditional LANs and VLANs.

- All switches are interconnected to each other. However, there are three different VLANs or broadcast domains on the network. Physical isolation is not required to define broadcast domains. If the figure was a traditional LAN without VLAN-aware switches, all stations would belong to one broadcast domain.
- All switch ports can communicate with one another at the Data Link Layer, if they become members of the same VLAN.
- The physical location of an end station does not define its LAN boundary.
  1. An end station can be physically moved from one switch port to another without losing its “view of the network”. That is, the set of stations it can communicate with at the Data Link Layer remains the same, provided that its VLAN membership is also migrated from port to port.
  2. By reconfiguring the VLAN membership of the switch port an end station is attached to, you can change the network view of the end station easily, without requiring a physical move from port to port.

12.2 Backbone/ VLAN Aware Switches

To implement a VLAN in your network, you must use VLAN-aware switches.
Before we continue, let consider two rules to remember regarding the functioning of a regular LAN switch:

1. When the switch receives a broadcast or multicast frame from a port, it floods (or broadcasts) the frame to all other ports on the switch.
2. When the switch receives a unicast frame, it forwards it only to the port to which it is addressed.

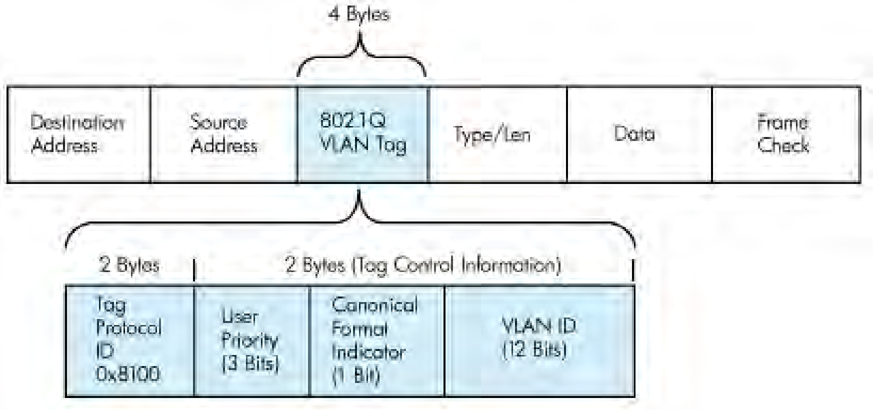
A VLAN-aware switch changes the above two rules as follows:

1. When the switch receives a broadcast or multicast frame from a port, it floods the frame to only those ports that belong to the same VLAN as the frame.
2. When a switch receives a unicast frame, it forwards it to the port to which it is addressed, only if the port belongs to the same VLAN as the frame.
3. A unique number called the VLAN ID identifies each VLAN.

Which VLAN Does a Frame Belong To?
The previous section notes that a frame can belong to a VLAN. The next question is—how is this association made?

- A VLAN-aware switch can make the association based on various attributes of the type of frame, destination of MAC address, IP address, TCP port, Network Layer protocol, and so on.

An illustration of IEEE 802.1Q VLAN tag in Ethernet frame is as follows:



12.3 How VLAN Switch Work: VLAN Tagging

VLAN functionality can be implemented via explicit frame tagging by switches and end stations. Network switches and end stations that know about VLANs are said to be VLAN aware. Network switches and end stations that can interpret VLAN tags are said to be VLAN tag aware. VLAN-tag-aware switches and end stations add VLAN tags to standard Ethernet frames–a process called explicit tagging. In explicit tagging, the end station or switch determines the VLAN membership of a frame and inserts a VLAN tag in the frame header (see figure above for VLAN tagging), so that downstream link partners can examine just the tag to determine the VLAN membership.

12.4 Implementation Cases

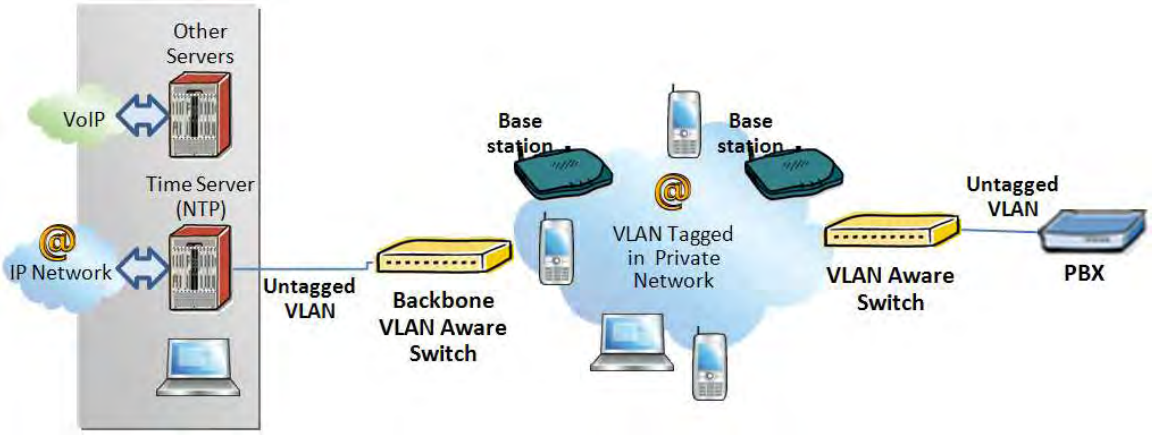
Common types of usage scenarios for VLANs on typical VLAN switches: port-based VLANs, protocol-based VLANs, and IP subnet-based VLANs. Before figuring out which usage scenario suits your needs, you must understand what each type of usage scenario implies.

- **Port-based VLAN:** All frames transmitted by a NIC are tagged using only one VLAN ID. The NIC does not transmit or receive any untagged frames.

All protocols and applications use this virtual interface's virtual PPA to transmit data traffic. Therefore, all frames transmitted by that NIC port are tagged with the VLAN ID of that Virtual Interface.

- **Protocol-based VLAN:** The NIC assigns a unique VLAN ID for each Layer 3 protocol (such as IPv4, IPv6, IPX, and so on). Therefore, the VLAN ID of outbound frames is different for each protocol. An inbound frame is dropped if the protocol and VLAN ID do not match.

- **IP subnet-based VLAN:** The NIC assigns a unique VLAN ID for each IP subnet it belongs to. Therefore, the VLAN ID of outbound frames is different for different destination subnets. An inbound frame is dropped if the IP subnet and VLAN ID do not match.



12.5 Base station Setup

After the admin have setup the Backbone switch, next is to configure the Base station via HTTP interface.

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

STEP 2 Use one of the two methods to find the base IP

STEP 3 On the Login page, enter your authenticating credentials (the username and password is **admin** by default unless it is changed). Click **OK** button.

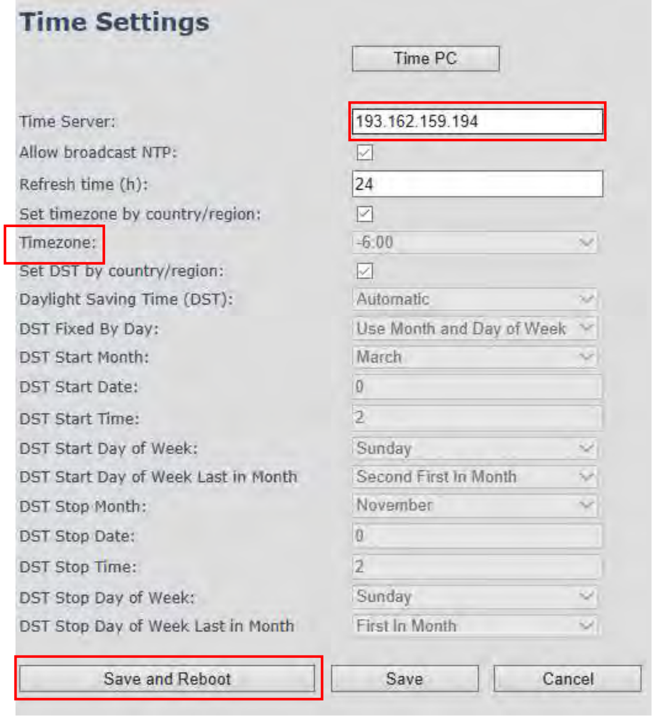
STEP 4 Once you have authenticated, the browser will display front end of the Configuration Interface. The front end will show relevant information of the base station.

STEP 5 Create the relevant SIP server information in the system. Each service provider/customer should refer SIP server vendor on how to setup SIP servers.

12.6 Configure Time Server

STEP 6 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.

Screenshot



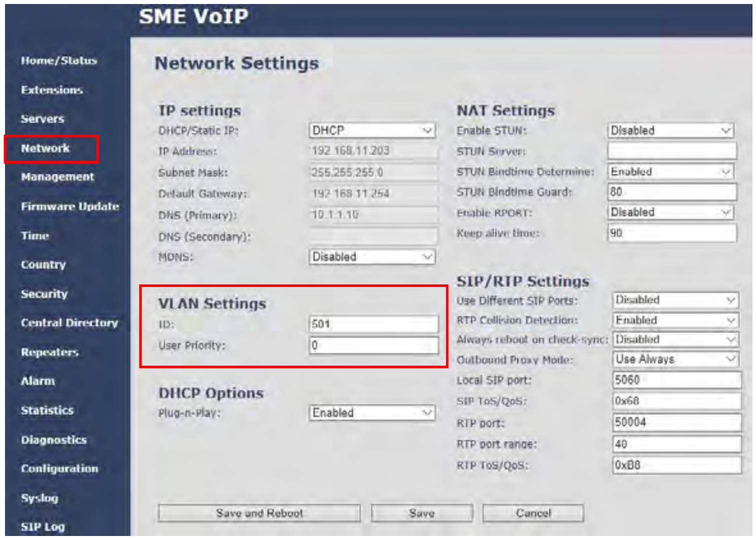
Time Settings

Time Server:	193.162.159.194
Allow broadcast NTP:	☑
Refresh time (h):	24
Set timezone by country/region:	☑
Timezone:	-6:00
Set DST by country/region:	☑
Daylight Saving Time (DST):	Automatic
DST Fixed By Day:	Use Month and Day of Week
DST Start Month:	March
DST Start Date:	0
DST Start Time:	2
DST Start Day of Week:	Sunday
DST Start Day of Week Last in Month	Second First In Month
DST Stop Month:	November
DST Stop Date:	0
DST Stop Time:	2
DST Stop Day of Week:	Sunday
DST Stop Day of Week Last in Month	First In Month

12.7 VLAN Setup: Base station

STEP 7 Navigate to the **Network** url > On the network page enter the relevant settings in the VLAN section > VLAN Id should be the same as those configured into the backbone.

Screenshot



Network Settings

IP settings
- DHCP/Static IP: DHCP
- IP Address: 192.168.11.203
- Subnet Mask: 255.255.255.0
- Default Gateway: 192.168.11.254
- DNS (Primary): 10.1.1.10
- DNS (Secondary):
- MDNS: Disabled

VLAN Settings
- ID: 501
- User Priority: 0

DHCP Options
- Plug-n-Play: Enabled

NAT Settings
- Enable STUN: Disabled
- STUN Server:
- STUN Bindtime Determine: Enabled
- STUN Bindtime Guard: 80
- Enable RPORT: Disabled
- Keep alive time: 90

SIP/RTP Settings
- Use Different SIP Ports: Disabled
- RTP Collision Detection: Enabled
- Always reboot on check-sync: Disabled
- Outbound Proxy Mode: Use Always
- Local SIP port: 5060
- SIP ToS/QoS: 0x68
- RTP port: 50004
- RTP port range: 40
- RTP ToS/QoS: 0xB8

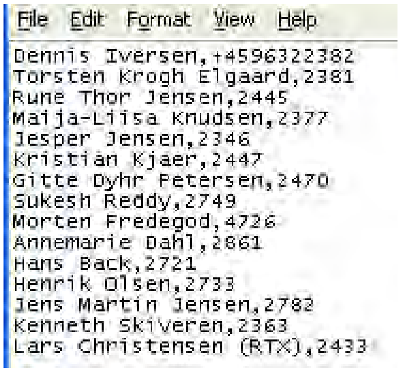
13 Appendix C: Local Central directory file handling

In this appendix, the Local Central Directory file format, import and configuration is described.

13.1 Central Directory Contact List Structure

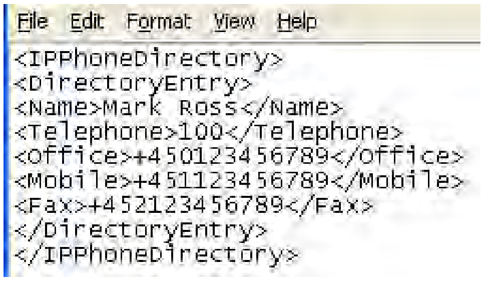
The structure of Contact List is simple. The figure below shows an example of structure of Contact List in Text format and in Xml format. ***Contact name must not contain more than 23 characters and contact number must not contain more than 21 digits.***

.csv or .txt



```
Dennis Iversen,+4596322382
Torsten Krogh Elgaard,2381
Rune Thor Jensen,2445
Maija-Liisa Knudsen,2377
Jesper Jensen,2346
Kristian Kjaer,2447
Gitte Dyhr Petersen,2470
Sukesh Reddy,2749
Morten Fredegod,4726
Annemarie Dahl,2861
Hans Back,2721
Henrik Olsen,2733
Jens Martin Jensen,2782
Kenneth Skiveren,2363
Lars Christensen (RTX),2433
```

.xml



```
<IPPhoneDirectory>
<DirectoryEntry>
<Name>Mark Ross</Name>
<Telephone>100</Telephone>
<Office>+4501234567 89</Office>
<Mobile>+4511234567 89</Mobile>
<Fax>+4521234567 89</Fax>
</DirectoryEntry>
</IPPhoneDirectory>
```

Txt file limitations:

- Contact name must NOT be longer than 23 characters (name will be truncated)
- Contact name must NOT contain ","
- Contact number must be limited to 21 digits (entry will be discarded, no warning)
- Contact number digits must be: +0123456789
- Contact number does not support SIP-URI
- Spaces between name section "," and number section is not supported

13.2 Central Directory Contact List Filename Format

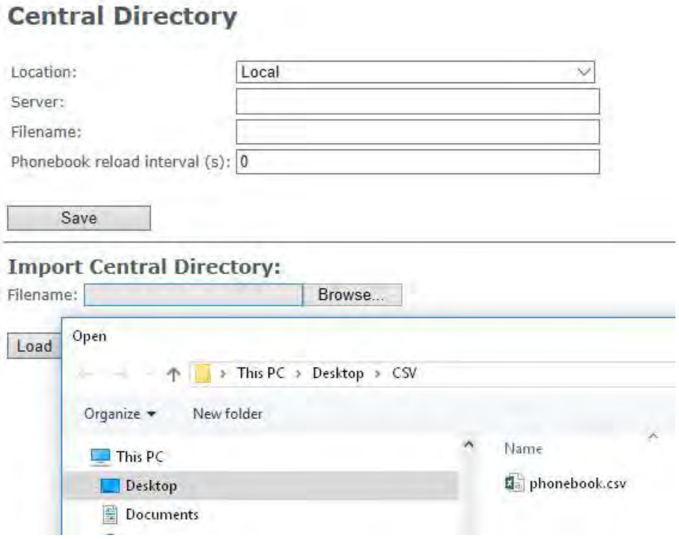
The Contact list is saved as file format: **.txt .csv** or **.xml**

13.3 Import Contact List to Central Directory

On the **Central Directory** page, the admin should click on **Browse** button and the **Choose File to Load** dialog window will be shown.

On the **Choose File to Upload** dialog window, navigate to the directory or folder that contains the right file to be imported to the base station > Click on **Open** button.

Screenshot



Central Directory

Location: Local

Server:

Filename:

Phonebook reload interval (s): 0

Import Central Directory:

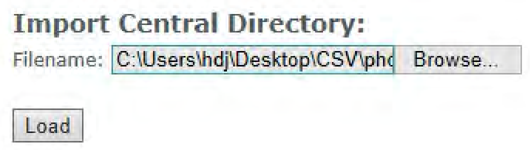
Filename:

Open

This PC > Desktop > CSV

Next, click on the **Load** button. This will import the contents of contacts in the selected file into the relevant Base station.

Screenshot

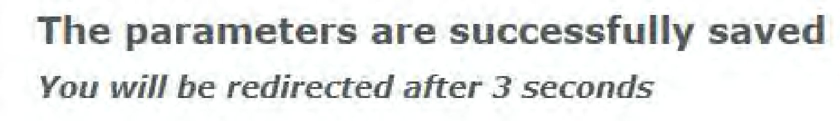


Import Central Directory:

Filename: C:\Users\hdj\Desktop\CSV\phc

The figure below shows the import procedure is in process.

Screenshot



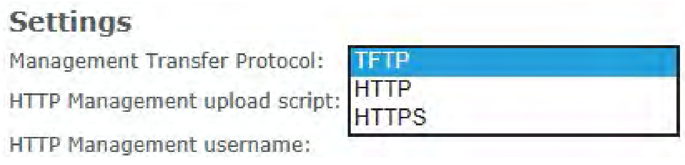
The parameters are successfully saved

You will be redirected after 3 seconds

13.4 Central directory using server

Alternative way to import a Contact List is to get it from a server. First click on Management url to get Management Settings page, then select the protocol of your server (TFTP/HTTP/HTTPS) in Management Transfer Protocol, then save the setting by clicking Save.

Screenshot



Settings

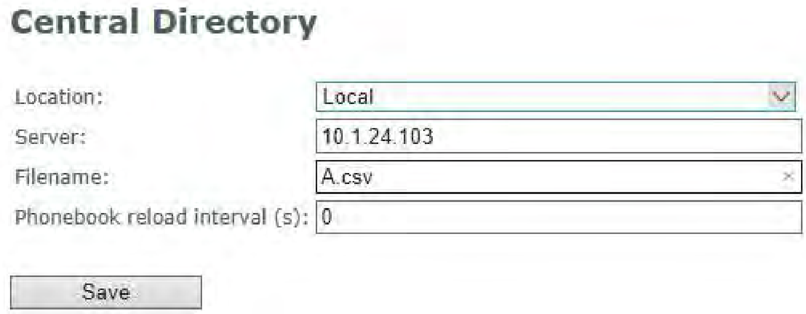
Management Transfer Protocol: TFTP

HTTP Management upload script:

HTTP Management username:

Go back to Central Directory page and enter Server IP address (inclusive the path in the end of the address) and Filename of the contact list, then save the setting by clicking Save. (See example below).

Screenshot



Central Directory

Location: Local

Server: 10.1.24.103

Filename: A.csv

Phonebook reload interval (s): 0

Then reboot the Base station to ensure that the changes take effect.

13.5 Verification of Contact List Import to Central Directory

On the Handset, navigate to Central Directory where the correct contact list should populate to the contacts uploaded to the Base station.

14 Appendix D: Provisioning.

Before provisioning, you should be aware of the file size limit. The Rove B4 base station supports files with size up to 1M.

14.1 Provisioning approaches.

There are three ways of configuring the system.

1. Manual configuration by use of the Web server in the base station.
2. By use of configuration files that are uploaded from a disk via the “Configuration” page on the Web server.
3. By use of configuration files which the base station download from a configuration server.

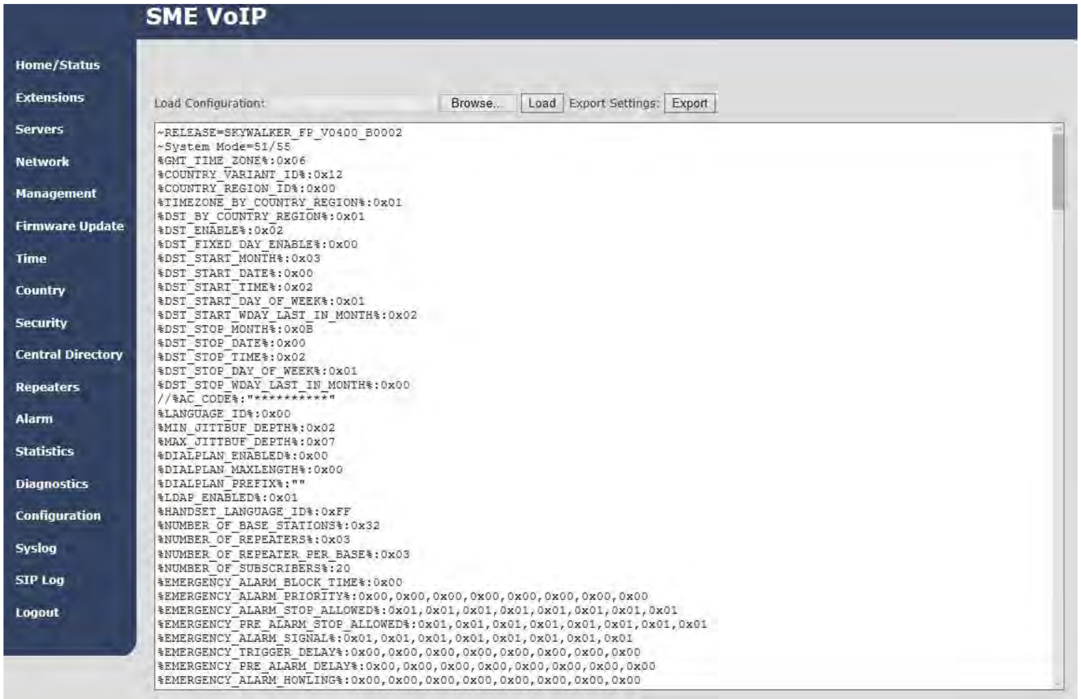
14.2 Manual Configuration by use of Web Server.

Configuring the system manually we use of web server is basically what is described earlier in this manual. With this approach, you must go through all steps to setup a complete system.

14.3 Configuration by use of Uploaded Configuration Files.

Instead of configuring the base stations manually by entering the parameter values on the Web server, it is possible to use a configuration file that is uploaded from e.g. a PC. This can be done from the “Configuration” page on the Web server.

Screenshot



```
~RELEASE=SKYWALKER_FP_V0400_B0002
~System Mode=51/55
%GMT_TIME_ZONE%:0x06
%COUNTRY_VARIANT_ID%:0x12
%COUNTRY_REGION_ID%:0x00
%TIMEZONE_BY_COUNTRY_REGION%:0x01
%DST_BY_COUNTRY_REGION%:0x01
%DST_ENABLE%:0x02
%DST_FIXED_DAY_ENABLE%:0x00
%DST_START_MONTH%:0x03
%DST_START_DATE%:0x00
%DST_START_TIME%:0x02
%DST_START_DAY_OF_WEEK%:0x01
%DST_START_WDAY_LAST_IN_MONTH%:0x02
%DST_STOP_MONTH%:0x0B
%DST_STOP_DATE%:0x00
%DST_STOP_TIME%:0x02
%DST_STOP_DAY_OF_WEEK%:0x01
%DST_STOP_WDAY_LAST_IN_MONTH%:0x00
//%AC_CODE%:"**********"
%LANGUAGE_ID%:0x00
%MIN_JITTBUF_DEPTH%:0x02
%MAX_JITTBUF_DEPTH%:0x07
%DIALPLAN_ENABLED%:0x00
%DIALPLAN_MAXLENGTH%:0x00
%DIALPLAN_PREFIX%:""
%LDAP_ENABLED%:0x01
%HANDSET_LANGUAGE_ID%:0xFF
%NUMBER_OF_BASE_STATIONS%:0x32
%NUMBER_OF_REPEATERS%:0x03
%NUMBER_OF_REPEATER_PER_BASE%:0x03
%NUMBER_OF_SUBSCRIBERS%:20
%EMERGENCY_ALARM_BLOCK_TIME%:0x00
%EMERGENCY_ALARM_PRIORITY%:0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00
%EMERGENCY_ALARM_STOP_ALLOWED%:0x01,0x01,0x01,0x01,0x01,0x01,0x01,0x01
%EMERGENCY_PRE_ALARM_STOP_ALLOWED%:0x01,0x01,0x01,0x01,0x01,0x01,0x01,0x01
%EMERGENCY_ALARM_SIGNAL%:0x01,0x01,0x01,0x01,0x01,0x01,0x01,0x01
%EMERGENCY_TRIGGER_DELAY%:0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00
%EMERGENCY_PRE_ALARM_DELAY%:0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00
%EMERGENCY_ALARM_HOWLING%:0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00
```

STEP 1 Chose configuration file

STEP 2 Press Load to load the file.

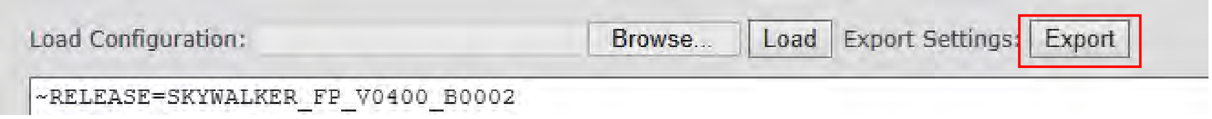
The base station will now load the file and the settings will be as in the configuration file.

14.4 How to create a configuration file.

To create a configuration file, you must use the web server interface and do a full setup, and set all settings as needed.

When the base station is setup and ready, go to the configuration page.

Screenshot



```
~RELEASE=SKYWALKER_FP_V0400_B0002
```

Press Export and save the cfg file.

NOTE: You must save the file as “Mac-address name.cfg” (e.g 00087b13ae79.cfg)

To load the configuration into another base station, rename the fil with the base stations MAC address and load it, as described in 11.3.

14.5 Configuration via Configuration Server.

It is also possible to use configuration files that are downloaded from a configuration server. To be able to use configuration files instead of manual configuration, the base stations must be set up to use configuration files. This can be done by use of DHCP option 66, or it can be configured via the Web server.

14.5.1 DHCP option 66 (TFTP Boot up server):

1. Upload of configuration file with setting the below parameter to 0 for option 66

NETWORK_DHCP_CLIENT_BOOT_SERVER /* Select scheme for detecting the DHCP server 0: Option 66 1: Custom 3: Custom + Option.66 */ Default value defined: 2

2. Configuration by web interface as described in the below configuration for web server section

In the configuration file, you must change CONFIGURATION_DOWNLOAD_CTRL%:0x00 to CONFIGURATION_DOWNLOAD_CTRL%:0x01

Find the needed setting in the configuration file

%CONFIGURATION_DOWNLOAD_CTRL%:0x00 change to %CONFIGURATION_DOWNLOAD_CTRL%:0x01

And

%NETWORK_DHCP_CLIENT_BOOT_SERVER %:0x02 change to (default=disabled)
%NETWORK_DHCP_CLIENT_BOOT_SERVER %:0x00 = DHCP 66
%NETWORK_DHCP_CLIENT_BOOT_SERVER %:0x01 = Custom
%NETWORK_DHCP_CLIENT_BOOT_SERVER %:0x03 = DHCP 66 + Custom

14.5.2 Configuration for web server:

A given base station is set up to use configurations files on the “Management Settings” page on the Web server.

STEP 1 Select the Management transfer protocol needed. (TFTP, HTTP, HTTPS)

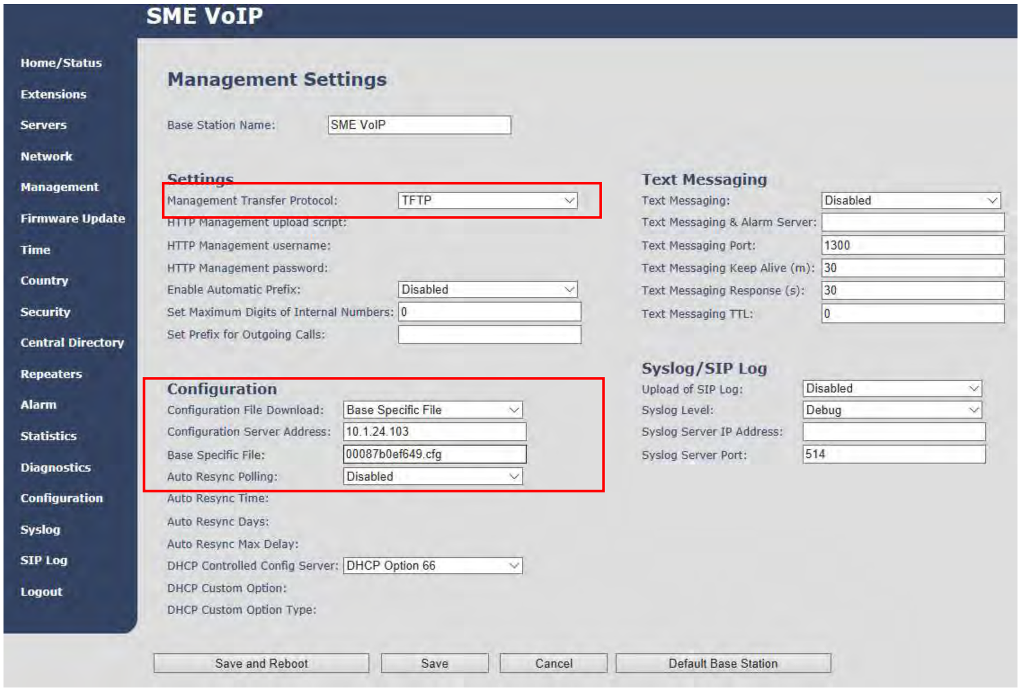
STEP 2 Select “Configuration file download” (Base specific file)

STEP 3 Enter IP of the server where the file is located

STEP 4 Enter the file name.

Save and reboot

Screenshot



Management Settings

Base Station Name: SME VoIP

Settings
Management Transfer Protocol: TFTP
HTTP Management upload script:
HTTP Management username:
HTTP Management password:
Enable Automatic Prefix: Disabled
Set Maximum Digits of Internal Numbers: 0
Set Prefix for Outgoing Calls:

Configuration
Configuration File Download: Base Specific File
Configuration Server Address: 10.1.24.103
Base Specific File: 00087b0ef649.cfg
Auto Resync Polling: Disabled
Auto Resync Time:
Auto Resync Days:
Auto Resync Max Delay:
DHCP Controlled Config Server: DHCP Option 66
DHCP Custom Option:
DHCP Custom Option Type:

Text Messaging
Text Messaging: Disabled
Text Messaging & Alarm Server:
Text Messaging Port: 1300
Text Messaging Keep Alive (m): 30
Text Messaging Response (s): 30
Text Messaging TTL: 0

Syslog/SIP Log
Upload of SIP Log: Disabled
Syslog Level: Debug
Syslog Server IP Address:
Syslog Server Port: 514

NOTE: When downloading configuration file from web server the file MUST be placed in a directory called Config.

FCC Warning

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

For Handset

SAR tests are conducted using standard operating positions accepted by the FCC with device transmitting at its highest certified power level in all tested frequency bands, although the SAR is determined at the highest certified power level, the actual SAR level of the device while operating can be well below the maximum value. Before a new model device is an available for sale to the public, it must be tested and certified to the FCC that it does not exceed the exposure limit established by the FCC, tests for each device are performed in positions and locations as required by the FCC. For body

worn operation, this model device has been tested and meets the FCC RF exposure guidelines when used with an accessory designated for this product or when used with an accessory that contains no metal.

For Base

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator& your body. This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter located or operating in conjunction with any other antenna or transmitter.

Any Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

ISEDC Warning：

This device complies with ISEDC license-exempt RSS standard(s). Operation is subject to the following two conditions:

(1) this device may not cause interference, and

(2) this device must accept any interference, including interference that may cause undesired operation of the device.

Le présent appareil est conforme aux CNR d'ISEDC applicables aux appareils radio exempts de licence.L'exploitation est autorisée aux deux conditions suivantes :

(1) l'appareil nedoit pas produire de brouillage, et

(2) l'utilisateur de l'appareil doit accepter tout brouillage radioélectrique subi, même si le brouillage est susceptible d'en compromettre le fonctionnement.

ISEDC Specific Absorption Rate (SAR) information

For Handset

SAR tests are conducted using standard operating positions accepted by the ISEDC with device transmitting at its highest certified power level in all tested frequency bands, although the SAR is determined at the highest certified power level, the actual SAR level of the device while operating can be well below the maximum value. Before a new model device is a available for sale to the public, it must be tested and certified to the ISEDC that it does not exceed the exposure limit established by the ISEDC, tests for each device are performed in positions and locations as required by the ISEDC. For body worn operation, this model device has been tested and meets the ISEDC RF exposure guidelines when used with an accessory designated for this product or when used with an accessory that contains no metal.

For Base

This equipment complies with ISEDC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body. This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

ISEDC Radiation Exposure Statement:

For Handset
SAR l'utilisation des règles sma l'emplacement Le matériel de transmission et fonctionnant dans tous les essais à la certification, même si la puissance suprême a décidé le niveau, utilisation spécifique peut être très en deçà de la valeur de référence maximale.Types de matériel sont vendus au public un ancien, d'essai et de certification de l'exposition, limite maximum sma, chaque document et l'emplacement du materiel d'essai et conformément au document.Le modèle en physique, matériel d'essai et conforme aux directives d'exposition des radiofréquences sma quand une annexe désigné pour ce produit lors de leur utilisation ou
des pièces de rechange ne contiennent pas de métal.

For Base
Cet équipement est conforme aux limites d'exposition aux radiations ISEDC définies pour un environnement non contrôlé. Cet équipement doit être installé et utilisé avec une distance minimale de 20 cm entre le radiateur et votre corps. Cet émetteur ne doit pas être situé ou fonctionner conjointement avec une autre antenne ou un autre émetteur.

This product meets the applicable Innovation, Science and Economic Development Canada technical specifications.