



Multicell DECT System Guide For mi-MCB8663W

Installation & Configuration
Network Deployment
Operation & Management

Technical Reference Document
Version 5.3
© Apr-2022 miALERT

Contents

1	About This Document	7
1.1	Audience	7
1.2	When Should I Read This Guide	7
1.3	Important Assumptions.....	7
1.4	What's Inside This Guide.....	7
1.5	What's Not in This guide	8
1.6	Abbreviations	8
2	Introduction – System Overview	9
2.1	Hardware Setup	9
2.2	Components of SME VoIP System	10
2.2.1	Multicell Base stations	10
2.2.2	SME VoIP Administration Server/Software.....	10
2.2.3	Multicell Wireless Handset	10
2.3	Wireless Bands	11
2.4	System Capacity (in Summary).....	11
2.5	Advantages of SME VoIP System.....	12
3	Installation of Base stations/Repeater	13
3.1	Package – Contents/Damage Inspection.....	13
3.2	Multicell Base station Mechanics.....	14
3.3	Multicell Base Unit – Reset feature.....	14
3.4	Installing the Base station	15
3.4.1	Mounting the Base stations/Repeaters:	15
3.5	Find IP of Base station	16
3.5.1	Using handset Find IP feature.....	16
3.5.2	Using browser IPDECT.....	16
3.6	Login to Base SME Configuration Interface.....	16
4	Making Handset Ready	18
4.1	Package – Contents/Damage Inspection.....	18
4.2	Before Using the Phone	18
4.3	Using the Handset	19
5	SME VoIP Administration Interface	20
5.1	Web navigation	20
5.2	Home/Status	22
5.3	Extensions	23
5.3.1	Add extension	24
5.3.2	Edit Extension	28
5.3.3	Edit Handset.....	30
5.4	Servers.....	32

5.5	Network.....	36
5.5.1	IP Settings	37
5.5.2	VLAN Settings.....	38
5.5.3	DHCP Options.....	38
5.5.4	TCP Options.....	38
5.5.5	Discovery.....	39
5.5.6	NAT Settings.....	39
5.5.7	SIP/RTP Settings.....	40
5.6	Management Settings Definitions.....	42
5.6.1	Settings:	42
5.6.2	Configuration:	43
5.6.3	Text messaging:	44
5.6.4	Terminal:.....	44
5.6.5	Syslog/SIP Log:	45
5.6.6	Location Gateway	45
5.6.7	License	46
5.7	Firmware Update Definitions	46
5.7.1	Warning message when firmware upgrading.....	47
5.8	Location Gateways	47
5.8.1	Register Location gateway	47
5.9	Country/Time Settings	49
5.10	Security.....	51
5.10.1	Device identity.....	52
5.10.2	Trusted Server Certificates	52
5.10.3	Trusted Root Certificates.....	52
5.10.4	Password	53
5.10.5	Secure Web Server	53
5.11	Central Directory and LDAP.....	53
5.11.1	Local Central Directory	54
5.11.2	Import Central Directory	54
5.11.3	LDAP	55
5.11.4	Characters supported	56
5.11.5	XML Server.....	56
5.12	Multi-cell Parameter Definitions.....	56
5.12.1	Settings for this unit	57
5.12.2	DECT System Settings	58
5.12.3	Base station settings.....	59
5.12.4	Base station Group	60
5.12.5	DECT Chain	61

5.12.6	mi-MCB0158 – mi-MCB8663 Mixed mode.....	62
5.13	LAN SYNC.....	63
5.13.1	LAN sync feature.....	63
5.13.2	Zone LAN sync setup	64
5.13.3	External LAN sync setup	65
5.13.4	Base station group.....	66
5.13.5	This unit debug	67
5.14	Repeaters	68
5.14.1	Add repeater	68
5.14.2	Register Repeater	69
5.14.3	Repeaters list.....	70
5.15	Alarm	71
5.15.1	Use of Emergency Alarms.....	72
5.16	Statistics	73
5.16.1	System data	73
5.16.2	Free Running explained	74
5.16.3	Call data.....	74
5.16.4	Repeater data	75
5.16.5	DECT data	76
5.16.6	Call quality	77
5.17	Generic Statistics	78
5.17.1	DECT Synchronization Statistics	79
5.17.2	RTP Statistics.....	80
5.17.3	IP - Stack statistics	82
5.17.4	System Statistics	82
5.18	Diagnostics	83
5.18.1	Base stations.....	83
5.18.2	Extensions.....	83
5.18.3	Logging	84
5.19	Settings – Configuration File Setup	85
5.20	Sys log.....	86
5.21	SIP Logs.....	86
6	How-To setup a Multi Cell System	87
6.1	Adding Base stations	87
6.1.1	Country and Time Server Setup	88
6.1.2	SIP Server (or PBX Server) Setup.....	89
6.1.3	Add an extension	90
7	Adding Extensions.....	94
8	Firmware Upgrade Procedure	97

8.1	Network Dimensioning.....	97
8.2	TFTP Configuration.....	98
8.3	Create Firmware Directories	99
8.3.1	Base:.....	99
8.3.2	Handsets/Repeaters:	99
8.4	Handset Firmware Update Settings	100
8.5	Handset(s) and Repeater Firmware Upgrade.....	100
8.5.1	Monitor handset firmware upgrade	101
8.5.2	Monitor Repeater firmware upgrade	101
8.5.3	Verification of Firmware Upgrade	101
8.6	Base station(s) Firmware Upgrade	102
8.6.1	Base firmware confirmation	102
8.6.2	Verification of Firmware Upgrade	102
8.7	Upload startup/background picture to the handsets	103
9	Multiline Feature	104
9.1	How to setup Multiline.....	104
STEP 1	Start by registering a handset as described above (7 Appendix – Adding extensions).	104
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).	104
10	Functionality Overview	106
10.1	Gateway Interface	106
10.2	System security support details	107
10.2.1	TLS 1.2.....	107
10.2.2	SRTP	107
10.2.3	DECT	107
10.2.4	Certificate support.....	107
10.2.5	HTTPS.....	107
10.2.6	Mutual TLS authentication (mTLS)	108
10.3	Detail Feature List	108
Appendix.....		111
11	Appendix A: Basic Network Server(s) Configuration	111
11.1	Server setup	111
11.2	Requirements.....	111
11.3	DNS Server Installation/Setup.....	111
11.4	DHCP Server Setup	112
11.4.1	Hint: Getting DHCP Server to Work.....	112
11.5	TFTP Server Setup	113
11.5.1	TFTP Server Settings	113
11.6	SIP Server Setup	114

12	Appendix B: Using Base with VLAN Network.....	115
12.1	Introduction	115
12.2	Backbone/ VLAN Aware Switches	116
12.3	How VLAN Switch Work: VLAN Tagging	116
12.4	Implementation Cases.....	117
12.5	Base station Setup.....	117
12.6	Configure Time Server.....	118
12.7	VLAN Setup: Base station	119
13	Appendix C: Local Central directory file handling.....	119
13.1	Central Directory Contact List Structure	119
13.2	Central Directory Contact List Filename Format	120
13.3	Import Contact List to Central Directory	120
13.4	Central directory using server	121
13.5	Verification of Contact List Import to Central Directory	121
14	Appendix D: Provisioning.....	122
14.1	Provisioning approaches.	122
14.2	Manual Configuration by use of Web Server.	122
14.3	Configuration by use of Uploaded Configuration Files.	122
14.4	How to create a configuration file.	123
14.5	Configuration via Configuration Server.....	123
14.5.1	DHCP option 66 (TFTP Boot up server):.....	123
14.5.2	Configuration for web server:	124

1 About This Document

This document describes the configuration, customization, management, operation, maintenance and troubleshooting of the SME VoIP System (mi-MCB8663W base, mi-MCT385 handset, mi-MCT8633W handset, and mi-MCR4024W Repeater).

1.1 Audience

Who should read this guide? First, this guide is intended for networking professionals responsible for designing and implementing MULTICELLbased enterprise networks.

Second, network administrators and IT support personnel that need to install, configure, maintain, and monitor elements in a “live” SME VoIP network will find this document helpful. Furthermore, anyone who wishes to gain knowledge on fundamental features in the Beatus system can also benefit from this material.

1.2 When Should I Read This Guide

Read this guide before you install the core network devices of VoIP SME System and when you are ready to setup or configure SIP server, NAT aware router, advanced VLAN settings, Base stations, and multi cell setup.

This manual will enable you to set up components in your network to communicate with each other and deploy a fully functionally VoIP SME System.

1.3 Important Assumptions

This document was written with the following assumptions in mind:

- 1) You understand network deployment in general
- 2) You have working knowledge of basic TCP/IP/SIP protocols, Network Address Translation, etc...
- 3) A proper site survey has been performed, and the administrator have access to these plans

1.4 What’s Inside This Guide

We summarize the contents of this document in the table below:

WHERE IS IT?	CONTENT	PURPOSE
CHAPTER 2	Introduction to the SME VoIP Network	To gain knowledge about the different elements in a typical SME VoIP Network
CHAPTER 3	Installation of Base station/Repeater	Considerations to remember before unwrapping and installing base units and repeaters
CHAPTER 4	Making Handsets Ready	To determine precautions to take in preparing handsets for use in the system
CHAPTER 5	SME VoIP Administration Interface	To learn about the Configuration Interface and define full meaning of various parameters needed to be set up in the system.
CHAPTER 6	Multi-Cell Setup & Management	Learn how to add servers and setup multiple bases into a multi-cell network
CHAPTER 7	Registration Management - Handsets	Learn how to register handset and extensions to Base stations

CHAPTER 8	Firmware Upgrade/Downgrade Management	Provides the procedure of how to upgrade firmware to Base stations and/or handsets and/or repeaters
CHAPTER 9	Multiline Feature	Allows the same handset to have more than one number/line
CHAPTER 10	Functionality overview	To gain detail knowledge about the system features.
APPENDIX A	Server configuration	Basic understanding of a server configuration
APPENDIX B	VLAN Setup Management	Examines how to setup VLAN in the network
APPENDIX C	Local central directory file handling	Detailed description of central directory file format and upload.
APPENDIX D	Provisioning	How to do provisioning on the 9430 single cell base station.

1.5 What's Not in This guide

This guide provides overview material on network deployment, how-to procedures, and configuration examples that will enable you to begin configuring your VoIP SME System.

It is not intended as a comprehensive reference to all detail and specific steps on how to configure other vendor specific components/devices needed to make the SME VoIP System functional. For such a reference to vendor specific devices, please contact the respective vendor for documentation.

1.6 Abbreviations

For this document, the following abbreviations hold:

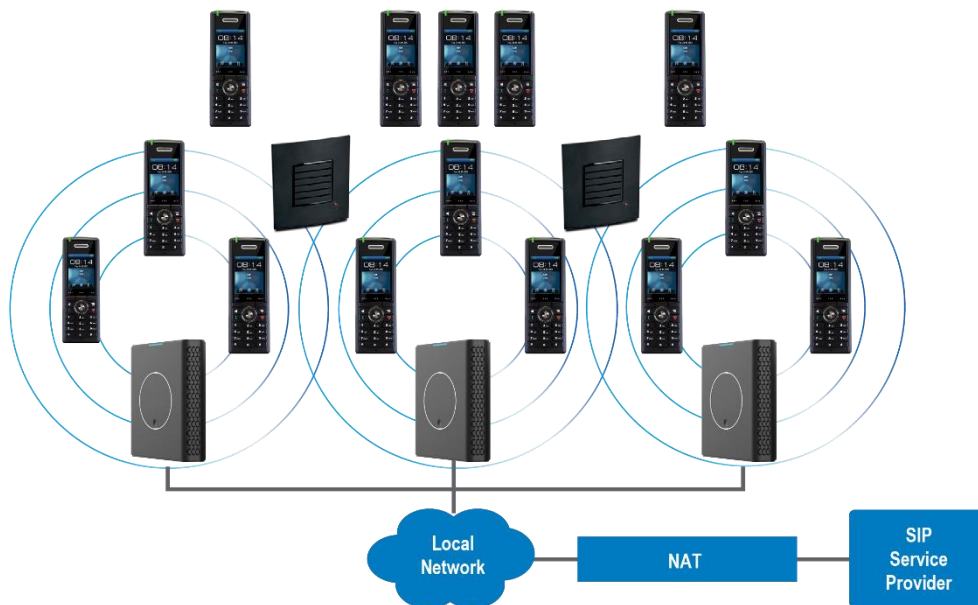
DHCP:	Dynamic Host Configuration Protocol
DNS:	Domain Name Server
DLC:	Data Link Control
HTTP(S):	Hyper Text Transfer Protocol (Secure)
(T)FTP:	(Trivial) File Transfer Protocol
IOS:	Internetworking Operating System
PCMA:	A-law Pulse Code Modulation
PCMU:	mu-law Pulse Code Modulation
PoE:	Power over Ethernet
RTP:	Real-time Transport Protocol
RPORT:	Response Port (Refer to RFC3581 for details)
SIP:	Session Initiation Protocol
SME:	Small and Medium scale Enterprise
VLAN:	Virtual Local Access Network
TOS:	Type of Service (policy based routing)
URL:	Uniform Resource Locator
UA:	User Agent
PTT:	Push-to-talk

2 Introduction – System Overview

In a typical telephony system, the network setup is the interconnection between Base stations, “fat” routers, repeaters, portable parts, etc. The backbone of the network depends on the deployment scenario, but a ring or hub topology is used. The network has centralized monitoring and maintenance system.

The system is easy to scale up and supports from 1 to 249 bases in the same network. Further it can support up to 1000 registered handsets (mi-MCT385 and mi-MCT8633). The Small and Medium Scale Enterprise (SME) VoIP system setup is illustrated below. Based on PoE interface, each Base station is easy to install without additional wires other than the LAN cable. The system supports the IP DECT CAT-IQ repeater mi-MCR4024 with support up to 5 channels simultaneous call sessions.

The following figure gives a graphical overview of the architecture of the SME VoIP System:



2.1 Hardware Setup

SME network hardware setup can be deployed as follows:

Base station(s) are connected via Layer 3 and/or VLAN Aware Router depending on the deployment requirements. The Layer 3 router implements the switching function.

The Base stations are mounted on walls or lamp poles so that each base-station is separated from each other by up to 50m indoor¹ (300m outdoor). Radio coverage can be extended using repeaters that are installed with same distance to Base station(s). Repeaters are range extenders and cannot be used to solve local call capacity issues. In this case additional bases must be used.

The Base station’s antenna mechanism is based on space diversity feature which improves coverage. The Base station uses complete DECT MAC protocol layer and IP media stream audio encoding feature to provide up to 10 simultaneous calls.

¹ Measured with European DECT radio and depends on local building layout and material
MULTICELL SYSTEM GUIDE 5.3
Proprietary and Confidential

2.2 Components of SME VoIP System

MULTICELLSME VoIP system is made up of (but not limited to) the following components:

- At least one Multicell Base station is connected over an IP network and using DECT as air-core interface.
- Multicell IP DECT wireless Handset.
- Multicell SME VoIP Configuration Interface; is a management interface for SME VoIP Wireless Solution. It runs on all IP DECT Base stations. Each Base station has its own unique settings.

2.2.1 Multicell Base stations

The Base station converts IP protocol to DECT protocol and transmits the traffic to and from the end-nodes (i.e. wireless handsets) over a channel. It has 12 available channels.

In a multi-cell setup, each Base station has:

- 8 channels have associated DSP resources for media streams.
- The remaining 4 channels are reserved for control signaling between IP Base stations and the SIP/DECT end nodes (or phones).

Base stations are grouped into clusters. Within each Cluster, Base stations are synchronized to enable a seamless handover when a user moves from one Base station coverage to another. For synchronization purposes, it is not necessary for Base stations to communicate directly with each other in the system. E.g. a Base station may only need to communicate with the next in the chain. It is advisable for a Base station to identify more than one Base station to guarantee synchronization in the situation that one of the Base stations fails.

The 4 control signaling channels are used to carry bearer signals that enable a handset to initiate a handover process.

2.2.2 SME VoIP Administration Server/Software

This server is referred to as SME VoIP Configuration Interface.

The SME VoIP Configuration Interface is a web-based administration page used for configuration and programming of the Base station and relevant network end-nodes. E.g. handsets can be registered or de-registered from the system using this interface.

The configuration interface can be used as a setup tool for software or firmware download to Base stations, repeaters and handsets. Further, it is used to check relevant system logs that can be useful to the administrator. These logs can be used to troubleshoot the system when the system faces unforeseen operational issues.

The web-based administration page is compatible with the following browsers:

- Chrome 68+
- Edge 42+
- Firefox 61+
- Safari 11.1.2+

2.2.3 Multicell Wireless Handset

The handset is a lightweight, ergonomically, and portable unit compatible with Wideband Audio (G.722), DECT, GAP standard, CAT-iq audio compliant.

The handset includes color display with graphical user interface. It can also provide the subscriber with most of the features available for a wired phone, in addition to its roaming and handover capabilities. Refer to the relevant handset manuals for full details handset features.

2.3 Wireless Bands

The bands supported in the SME VoIP are summarized as follows:

Frequency bands:

1880 – 1930 MHz (DECT)

1880 – 1900 MHz (10 carriers) Europe/ETSI

1910 – 1930 MHz (10 carriers) LATAM

1920 – 1930 MHz (5 carriers) US

2.4 System Capacity (in Summary)

SME network capacity of relevant components can be summarized as follows:

DESCRIPTION	CAPACITY
Min ## of Bases Single Cell Setup	1
Max ## of Bases in Multi-cell Setup (configurable)	50/127/254
Single/Multi Cell Setup: Max ## of Repeaters	50 bases and 3 repeaters per Base 127 bases and 1 repeater per Base 254 bases and 0 repeaters
Multi-cell Setup: Total Max ## of Repeaters	100
Max ## of Users (SIP registrations) per Base	40
Max ## of Users per SME VoIP System	limited to 1000
Multi-cell Setup: Max ## of Synchronization levels	24
Single Cell Setup: Max ## Simultaneous Calls	10* per Base station
Multi-cell Setup: Max ## of Calls	8* per Base station
Total Max ## Simultaneous Calls (Multi-cell Setup)	Limited to 1000
Repeater: Max ## of Calls (Narrow band)	5
Repeater: Max ## of Calls (G722)	2

* If G722 is in the codec list, it will reserve audio resources to be able to handle the possible G722 call. This means, that the maximum number of possible narrowband calls is reduced by one extra.

NOTE: Allowing a maximum of 40 extensions per base, makes it possible for different combinations of terminals and SIP extensions, where the following rule applies:

Every “SIP account” occupies one “extension instance”. However, as a terminal instance cannot exist without a SIP instance, a terminal associated with a SIP account, occupies only one extension instance in total. A terminal associated with two SIP accounts occupies two extension instances, etc. This means that in order to have 40 SIP accounts, you can have the following combinations:

- 40 handsets, each with 1 line (i.e. 1 SIP account)
- 20 handsets, each with 2 lines (i.e. 2 SIP accounts)
- 10 handsets, each with 4 lines (i.e. 4 SIP accounts)
- 8 handsets, each with 5 lines (i.e. 5 accounts)

Single Cell Setup: SME telephony network composed of one Base station

Multi-cell Setup: Telephony network that consists of more than one Base station

Synchronization Level: Is the air core interface between two Base stations.

NOTE: Please note that if there are over 150 base stations in a multicell, the “Multicast” data sync should be used

2.5 Advantages of SME VoIP System

They include (but not limited to):

- 1. Simplicity.** Integrating functionalities leads to reduced maintenance and troubleshooting, and significant cost reductions.
- 2. Flexibility.** Single network architecture can be employed and managed. Furthermore, the architecture is amenable to different deployment scenarios, including Isolated buildings for in-building coverage, location with co-located partners, and large to medium scale enterprises deployment for wide coverage.
- 3. Scalability.** SME network architecture can easily be scaled to the required size depending on customer requirement.
- 4. Performance.** The integration of different network functionalities leads to the collapse of the protocol stack in a single network element and thereby eliminates transmission delays between network elements and reduces the call setup time and packet fragmentation and aggregation delays.

3 Installation of Base stations/Repeater

After planning the network, next is to determine the proper places or location where the relevant Base stations will be installed. Therefore, we briefly describe how to install the Base station in this chapter.

3.1 Package – Contents/Damage Inspection

Before Package Is Opened:

Examine the shipping package for evidence of physical damage or mishandling prior to opening. If there is a proof of mishandling prior to opening, you must report it to the relevant support center of the regional representative or operator.

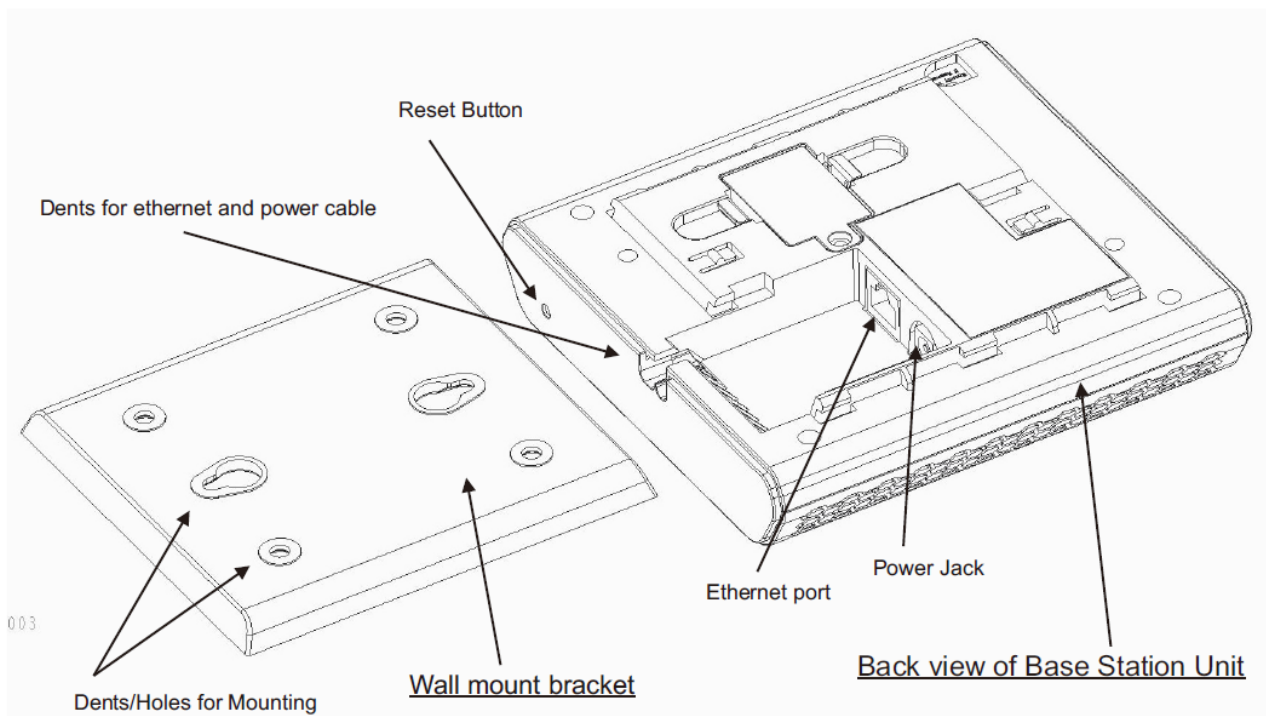
Contents of Package:

Make sure all relevant components are available in the package before proceeding to the next step.

Every shipped base unit package/box contains the following items:

- 2 x mounting screws and 2 x Anchors
- 1 x Plastic Wall mount
- Base unit

There is a possibility of using the device in a standalone mode via the power cable (without PoE).



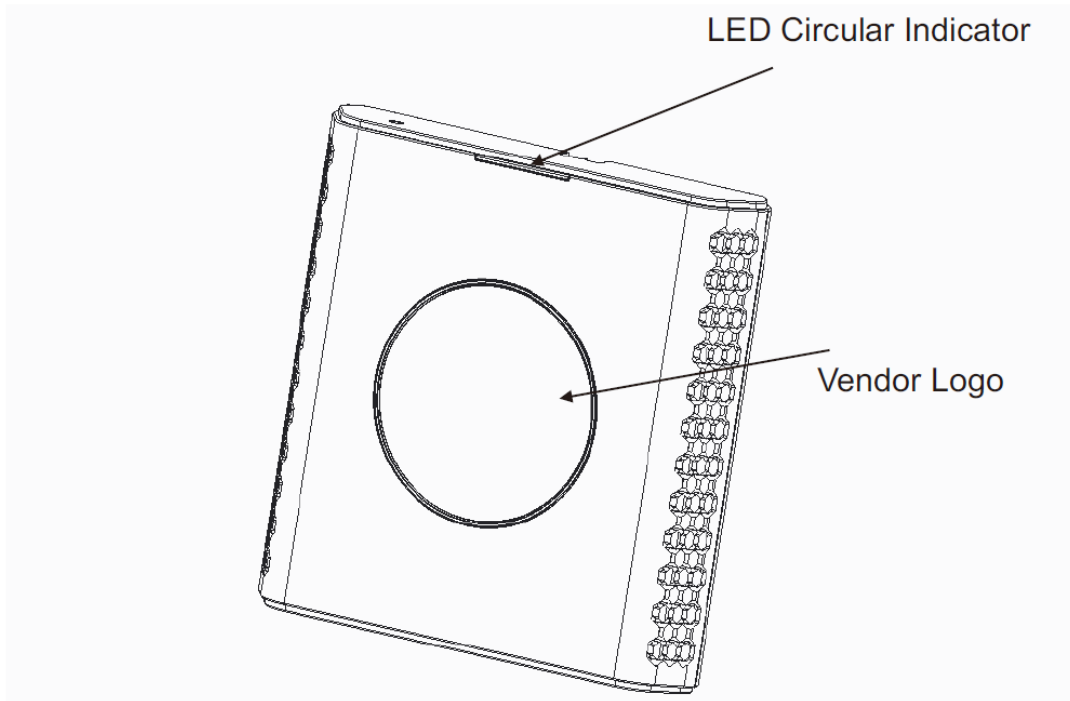
Damage Inspection:

The following are the recommended procedure for you to use for inspection:

1. Examine all relevant components for damage.
2. Make a “defective on arrival – DOA” report or RMA to the operator. Do not move the shipping carton until the operator has examined it. If possible, send pictures of the damage. The operator/regional representative will initiate the necessary procedure to process this RMA. They will guide the network administrator on how to return the damaged package if necessary.
3. If no damage is found, then unwrap all the components and dispose of empty package/carton(s) in accordance with country specific environmental regulations.

3.2 Multicell Base station Mechanics

The Base station front end shows an LED indicator that signals different functional states of the base unit and occasionally of the overall network. The indicator is off when the base unit is not powered.



The table below summarizes the various LED states:

LED STATE	STATE
UNLIT	No power in unit
UNLIT/SOLID RED	Error condition Unacceptable RSSI below -90dBm Critical error (can only be identified by miALERT Engineers. Symptoms include no system/SIP, etc.) Factory reset warning or long press in BS reset button
SOLID GREEN	Ethernet connection available Normal operation with good RSSI equal to or better than -75dBm
SOLID ORANGE	Normal operation with pure RSSI between -75dBm and -90dBm.
BLINKING GREEN	Initialization Searching for Base stations
BLINKING RED	Factory setting in progress Firmware upgrade/downgrade in progress Ethernet connection not available OR handset SIP registration failed
BLINKING ORANGE	Initialization Searching for IP

3.3 Multicell Base Unit – Reset feature

It is possible to restart or reset the Base station unit by pressing a knob at the rear side of the unit. Alternatively, it can be reset from the SME Configuration Interface. We do not recommend this; but unplugging and plugging the Ethernet cable back to the PoE port of the Base station also resets the base unit.

3.4 Installing the Base station

First determine the best location that will provide an optimal coverage taking account the construction of the building, architecture, and choice of building materials.

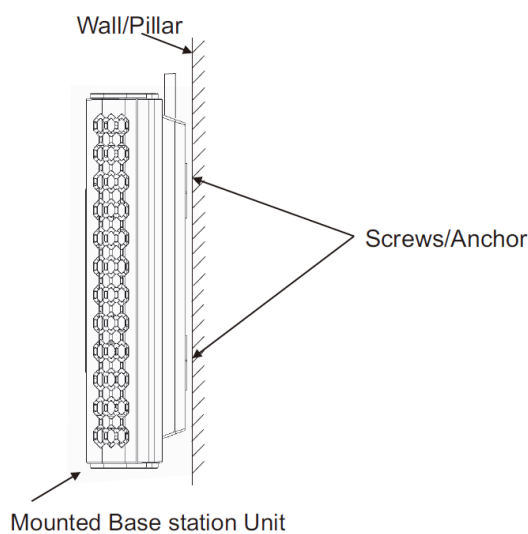
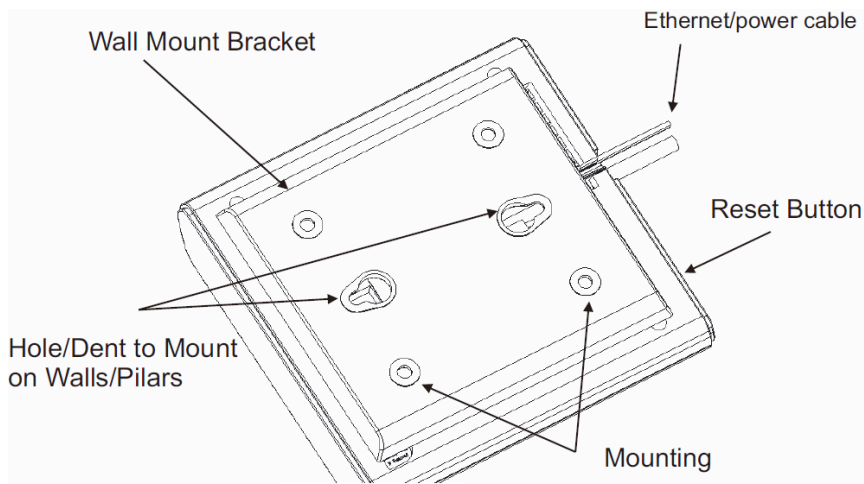
Next, mount the Base station on a wall to cover range between 50 – 300 meters (i.e. 164 to 984 feet), depending whether it's an indoor or outdoor installation.

3.4.1 Mounting the Base stations/Repeaters:

We recommend the Base station be mounted an angle other than vertical on both concrete/wood/plaster pillars and walls for optimal radio coverage. Avoid mounting the base unit's upside down as it significantly reduces radio coverage.

Mount the base unit as high as possible to clear all nearby objects (e.g. office cubicles and cabinets, etc.). Occasionally extend coverage to remote offices/halls with lower telephony users by installing Repeaters.

Make sure that when you fix the Base stations with screws, the screws do not touch the PCB on the unit. Secondly, avoid all contacts with any high voltage lines.



3.5 Find IP of Base station

To find IP of the installed Base station two methods can be used; Using handset Find IP feature or browser IPDECT feature.

3.5.1 Using handset Find IP feature

On the handset press “Menu” key followed by the keys: *47* to get the handset into find bases menu. The handset will now scan for bases. Depending on the amount of powered on bases with active radios and the distance to the base it can take up to minutes to find a base.

- Use the cursor down/up to select the base MAC address for the base
- The base IP address will be shown in the display

The feature is also used for deployment.

3.5.2 Using browser IPDECT

Open any standard browser and enter the address:

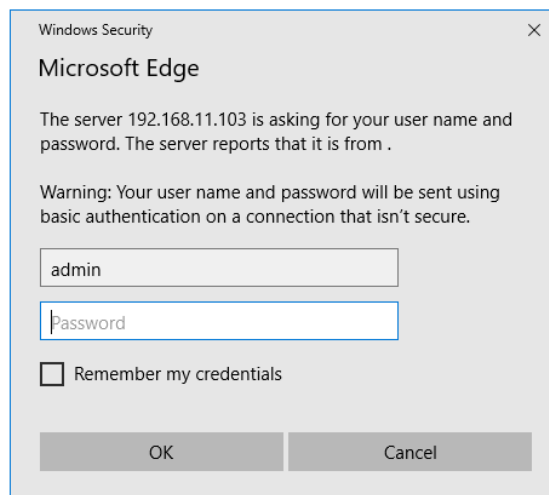
`http://ipdect<MAC-Address-Base-Station>`

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

This feature requires an available DNS server.

3.6 Login to Base SME Configuration Interface

- STEP 1** Connect the Base station to a private network via standard Ethernet cable (CAT-5).
- STEP 2** Use the IP find menu in the handset (Menu * 4 7 *) to determine the IP-address of the Base station by matching the MAC address on the back of the Base station with the MAC address list in the handset.
- STEP 3** On the Login page, enter your authenticating credentials (i.e. username and password). By default, the username and password are **admin**. Click **OK** button.



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:

The screenshot displays the SME VoIP configuration interface. On the left is a dark blue sidebar with a menu of options: Home/Status, Extensions, Servers, Network, Management, Firmware Update, Time, Country, Security, Central Directory, Multi cell, LAN Sync, Repeaters, Alarm, Statistics, Diagnostics, Configuration, Syslog, SIP Log, and Logout. The main content area has a dark blue header with the text 'SME VoIP' and a 'Welcome' message. Below the welcome message, there are two columns of system information. The left column is titled 'System Information:' and lists various parameters like Phone Type, System Type, RF Band, Current local time, Operation time, RFPI Address, MAC Address, IP Address, Firmware Version, and Firmware URL. The right column is titled 'Multi cell Unchained(Unchained) Allowed to Join as Secondary' and lists parameters like IPDECT-V2 (8663), Generic SIP (RFC 3261), EU, and Firmware path: HDJFwu. Below the system information, there is a section titled 'SIP Identity Status on this Base Station:' which is currently empty. At the bottom of the main content area, there is a prompt 'Press button to reboot.' followed by two buttons: 'Reboot' and 'Forced Reboot'.

4 Making The Handset Ready

In this chapter, we briefly describe how to prepare the handset for use, install, insert and charge new batteries. Please refer to an accompanying Handset User Guide for more information of the features available in the Handset.

4.1 Package – Contents/Damage Inspection

Before Package Is Opened:

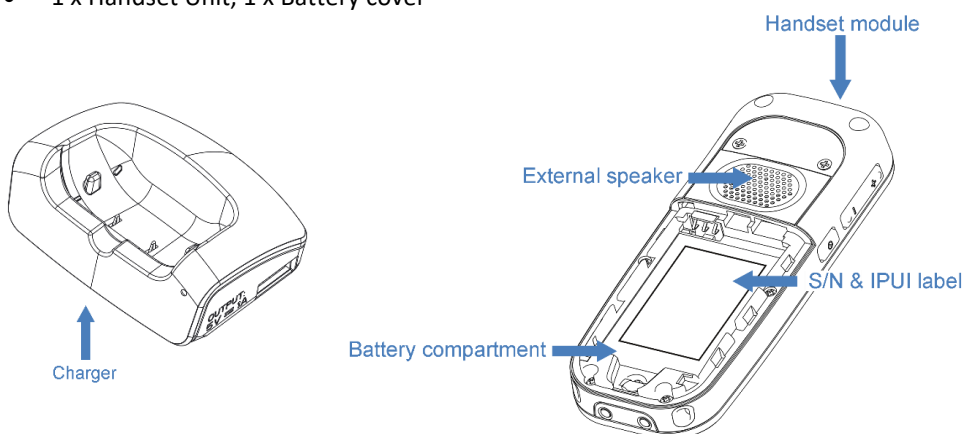
Examine the shipping package for evidence of physical damage or mishandling prior to opening. If there is a proof of mishandling prior to opening, you must report it to the relevant support center of the regional representative or operator.

Contents of Package:

Make sure all relevant components are available in the package before proceeding to the next step.

Every shipped base unit package/box contains the following items:

- 2 x mounting screws and 2 x Anchors
- 1 x Handset hook
- 1 x A/C Adaptor
- 1 x Battery
- 1 x charger
- 1 x Handset Unit, 1 x Battery cover



Damage Inspection:

The following are the recommended procedure for you to use for inspection:

1. Examine all relevant components for damage.
2. Make a “defective on arrival – DOA” report or RMA to the operator. Do not move the shipping carton until the operator has examined it. The operator/regional representative will initiate the necessary procedure to process this RMA. They will guide the network administrator on how to return the damaged package if necessary.
3. If no damage is found, then unwrap all the components and dispose of empty package/carton(s) in accordance with country specific environmental regulations.

4.2 Before Using the Phone

Here are the pre-cautions users should read before using the Handset:

Installing the Battery

1. Never dispose battery in fires, otherwise it will explode.
2. Never replace the batteries in potentially explosive environments, e.g. close to inflammable liquids/ gases.
3. ONLY use approved batteries and chargers from the vendor or operator.
4. Do not disassemble, customize, or short circuit the batter

Using the Charger

Each handset is charged using a handset charger. The charger is a compact desktop unit designed to charge and automatically maintain the correct battery charge levels and voltage.

The charger Handset is powered by AC supply from 110-240VAC that supplies 5.5VDC at 600mA.

When charging the battery for the first time, it is necessary to leave the handset in the charger for at least 10 hours before the battery is fully charged and the handset ready for use.

Handset in the Charger

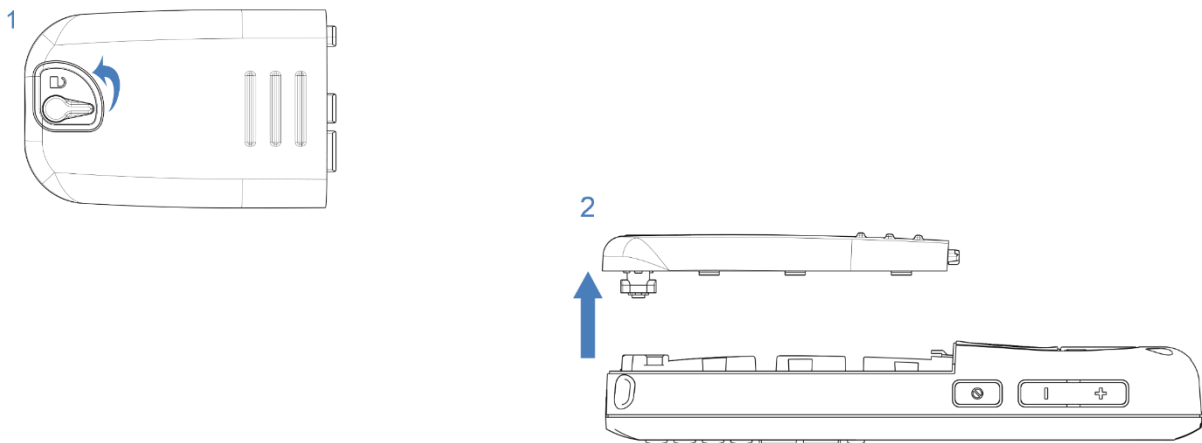
For correct charging, ensure that the room temperature is between 5°C and 25°C/41°F and 77°F. Do not place the handset in direct sunlight. The battery has a built-in heat sensor which will stop charging if the battery temperature is too high.

If the handset is turned off when placed in charger, only the LED indicates the charging. When handset is turned off, the LED flashes at a low frequency while charging and lights constantly when the charging is finished. There will be response for incoming calls.

If the handset is turned on when charging, the display shows the charging status.

Open Back Cover

1. Press down the back cover and slide it towards the bottom of the handset.
2. Remove the Back Cover from the handset



Handset Serial Number

The serial number (IPEI/IPUI number) of each handset is found either on a label, which is placed behind the battery, or on the packaging label. First, lift off handset back cover and lift the battery and read the serial number.

The serial number is needed to enable service to the handset. It must be programmed into the system database via the SME VoIP Configuration interface.

Replace Battery

Remove Back Cover from Handset. Remove the old battery and replace with a new one.

4.3 Using the Handset

Please refer to the handset manual for detailed description of how to use the handset features

5 SME VoIP Administration Interface

The SME VoIP Administration Interface is also known as SME VoIP Configuration. It is the main interface through which the system is managed and debugged.

The SME VoIP Configuration Interface is an in-built HTTP Web Server service residing in each Base station. This interface is a user-friendly interface and easy to handle even to a first-time user.

NOTE: Enabling secure web is not possible. For secure configuration, use secure provisioning. From v460 the base station supports configuration files up to 1MB

This chapter seeks to define various variables/parameters for configuration in the network, by going through the available settings of the base station. Certain pages (Extensions, Repeaters, Location and Multi cell) support an auto refresh feature, which allows the user to easily monitor the system. The pages are automatically refreshed every 5 seconds.

5.1 Web navigation

We describe the left menu in the front end of the SME VoIP Administration Interface.

Screenshot

The screenshot displays the SME VoIP Administration Interface. On the left is a dark blue navigation menu with the following items: Home/Status, Extensions, Servers, Network, Management, Firmware Update, Location Gateways, Country, Security, Central Directory, Multi cell, LAN Sync, Repeaters, Alarm, Statistics, Generic Statistics, Diagnostics, Configuration, Syslog, SIP Log, and Logout. The main content area has a dark blue header with 'SME VoIP' in white. Below the header, the page is titled 'Welcome' and contains the following sections:

- System Information:**
 - Phone Type: IPDECT-V2 (8663)
 - System Type: Generic SIP (RFC 3261)
 - RF Band: EU
 - Current local time: 27-Mar-2019 07:55:39
 - Operation time: 17:14:01 (H:M:S)
 - RFPI Address: 13214231; RPN:04
 - MAC Address: 00087b1573ba
 - IP Address: 192.168.11.146
 - Firmware Version: IPDECT-V2/03.22/B1858/22-Mar-2019 19:03
 - Firmware URL: Firmware update server address: http://betaware.rtx.net
- Multi cell Ready (Keep Alive) Primary**
- Reboot History:**
 - Reboot: 2019-03-26 14:41:20 (146) Forced Reboot (81) Firmware Version 0322.1858 (RESET_CAUSE_HARDWARE_RESET)
 - Reboot: 2019-03-25 09:05:57 (145) Normal Reboot (21) Firmware Version 0322.1858 (RESET_CAUSE_SYNC_RESET)
 - Reboot: 2019-03-25 09:04:32 (144) Normal Reboot (21) Firmware Version 0322.1858 (RESET_CAUSE_WBM_NORMAL_REBOOT)
 - Reboot: 2019-03-25 09:03:22 (143) Normal Reboot (21) Firmware Version 0322.1858 (RESET_CAUSE_WBM_NORMAL_REBOOT)
 - Reboot: 2019-03-25 08:58:52 (142) Forced Reboot (81) Firmware Version 0450.0005 (RESET_CAUSE_MAIN_CODE_UPDATE)
 - Reboot: 2019-03-25 08:32:44 (141) Normal Reboot (21) Firmware Version 0450.0005 (RESET_CAUSE_HARDWARE_RESET)
- Base Station Status:** Idle
- SIP Identity Status on this Base Station:**
 - 511@192.168.11.99 (HDJ Server) Status: OK
 - 515@192.168.11.99 (HDJ Server) Status: OK
 - 512@192.168.11.99 (HDJ Server) Status: OK
 - 6000000@192.168.11.99 (HDJ Server) Status: OK
 - 513@192.168.11.99 (HDJ Server) Status: OK

At the bottom, there is a section titled 'Press button to reboot.' containing two buttons: 'Reboot' and 'Forced Reboot'.

FEATURE	DESCRIPTION
HOME/STATUS	This is the front end of the Base station's HTTP web interface. This page shows the summary of current operating condition and settings of the Base station and Handset(s).
EXTENSIONS	Administration of extensions and handsets in the system
SERVERS	On this page, the user can define which SIP/NAT server the network should connect to.
NETWORK	Typically, the user configures the Network settings from here. NAT provisioning: allows configuration of features for resolving of the NAT – Network Address Translation. These features enable interoperability with most types of routers. DHCP: allows changes in protocol for getting a dynamic IP address. Virtual LAN: specifies the Virtual LAN ID and the User priority. IP Mode: specifies using dynamic (DHCP) or static IP address for your SME network. IP address: if using DHCP leave it empty. Only write in, when you use static IP address. Subnet mask: if using DHCP, leave it empty. Only write in, when you use static IP address. DNS server: specify if using DHCP, leave it empty. Only write in the DNS server address of your Internet service provider, when you use static IP address. (DNS = Dynamic Name Server) Default gateway: if using DHCP, leave it empty. Write in the IP address of your router, when you use static IP address.
MANAGEMENT	Defines the Configuration server address, Management transfer protocol, sizes of logs/traces that should be catalogued in the system.
FIRMWARE UPDATE	Remote firmware updates (HTTP(s)/TFTP) settings of Base stations and handsets.
LOCATION GATEWAY	Administration of Location Gateways
COUNTRY	Specifying the country/territory where the SME network is located ensures that your phone connection functions properly. Note: The base language and country setting are independent of each other. Time settings: Here the user can configure the Time server. It should be used as time server in relevant country for exact time. The time servers have to deliver the time to conform to the Network Time Protocol (NTP). Handsets are synchronised to this time. Base units synchronise to the master using the Time server.
SECURITY	The users can administrate certificates and create account credentials with which they can log in or log out of the embedded HTTP web server.
CENTRAL DIRECTORY	Interface to common directory load of up to 3000 entries using *csv format or configuration of LDAP directory. Note: LDAP and central directory cannot operate at the same time.
MULTI CELL	Specify to connect Base station or chain of Base stations to the network. Make sure the system ID for the relevant Base stations are the same otherwise the multi-cell feature will not work.
LAN SYNC	Allows Base stations to connect over LAN PTP Sync, this makes it possible to have greater distance between the Base stations, compared to Air Sync.
REPEATERS	Administration and configuration of repeaters of the system
ALARM	Administration and configuration of the alarm settings on the system. This controls the settings for alarms that can be sent to the handsets. This feature is only available on certain types of handsets.
STATISTICS	Overview of system and call statistics for a system.
GENERIC STATISTICS	Overview of general parameter statistics of the system
DIAGNOSTICS	Overview of Base stations and Extensions diagnostics
CONFIGURATION	This shows detail and complete SME network settings for Base station(s), HTTP/DNS/DHCP/TFTP server, SIP server, etc.
SYSLOG	Overall network related events or logs are displayed here (only live feed is shown).
SIP LOG	SIP related logs can be retrieved from URL link. It is also possible to clear logs from this feature.

5.2 Home/Status

We describe the parameters found in the Welcome front-end home/status of the SME VoIP Administration Interface.

Screenshot:

Welcome

<p>System Information:</p> <p>Phone Type: System Type: RF Band: Current local time: Operation time: RFPI Address: MAC Address: IP Address: Firmware Version: Firmware URL:</p>	<p>Multi cell Ready (Keep Alive) Primary</p> <p>IPDECT-V2 (8663) Generic SIP (RFC 3261) EU 20-Mar-2019 07:09:56 03:15:47 (H:M:S) 13214231; RPN:00 00087b1573bb 192.168.11.120 IPDECT-V2/04.50/B0005/06-Mar-2019 08:22 Firmware update server address: http://betaware.rtx.net Firmware path: hdjfwu</p>
---	--

Reboot: 2019-03-20 03:52:08 (120)	Forced Reboot (81) Firmware Version 0450.0004 (RESET_CAUSE_MAIN_CODE_UPDATE)
Reboot: 2019-03-18 06:39:33 (119)	Forced Reboot (81) Firmware Version 0440.0004 (RESET_CAUSE_MAIN_CODE_UPDATE)
Reboot: 2019-03-14 09:10:59 (118)	Forced Reboot (81) Firmware Version 0450.0004 (RESET_CAUSE_UNKNOWN_RESET_CAUSE)
Reboot: 2019-03-14 08:56:20 (117)	Forced Reboot (81) Firmware Version 0440.0004 (RESET_CAUSE_UNKNOWN_RESET_CAUSE)
Reboot: 2019-03-13 06:48:11 (116)	Normal Reboot (00) Firmware Version 0450.0004 (RESET_CAUSE_UNKNOWN_RESET_CAUSE)
Reboot: 2019-03-12 04:42:29 (115)	Normal Reboot (21) Firmware Version 0450.0004 (RESET_CAUSE_UNKNOWN_RESET_CAUSE)

Base Station Status: Idle

SIP Identity Status on this Base Station:

6000000@192.168.11.99 (HDJ Server)	Status: OK
515@192.168.11.99 (HDJ Server)	Status: OK

Press button to reboot.

Reboot	Forced Reboot
--------	---------------

PARAMETER	DESCRIPTION
SYSTEM INFORMATION	This base current multi-cell state
PHONE TYPE	Always IPDECT
SYSTEM TYPE	This base customer configuration
RF BAND	This base RF band setting. The parameter is defined in production and relates to the radio approvals shown on the label of the base.
CURRENT LOCAL TIME	This base local time
OPERATION TIME	Operation is operation time for the base since last reboot
RFPI-ADDRESS	This base RFPI address
MAC-ADDRESS	This base MAC address
IP-ADDRESS	This base IP address
FIRMWARE VERSION	This base firmware version
FIRMWARE URL	Firmware update server address and firmware path on server
REBOOT	Shows the last reboots of the Base station and the reason for reboot
BASE STATION STATUS	“Idle”: When no calls on base “In use”: When active calls on base
SIP IDENTITY STATUS	List of extensions present at this Base station. Format: “extension”@“this base IP address”(“server name”) followed by status to the right. Below is listed possible status: OK: Handset is ok SIP Error: SIP registration error
REBOOT	Reboot after all connections is stopped on base. Connections are active calls, directory access, firmware update active
FORCED REBOOT	Reboot immediately.

5.3 Extensions

In this section, we describe the different parameters available whenever the administrator is creating extensions for handsets. Note that it is not possible to add extensions if no servers are defined (to add a server please see chapter 6.1.2 *SIP server (or PBX Server) Setup*). Furthermore, the section describes the administration of extensions and handsets using the extension list and the extension list menu.

The system can handle maximum 1000 extensions matching 1000 handsets which can be divided between servers. When 1000 handsets are registered it is not possible to add more extensions. With active multiline feature, the system can handle maximum 1000 extensions. With 4 active lines in multiline maximum 200 handsets can be active in the system.

Note: Within servers or even with multi servers, extensions must always be unique. This means that the same extension number on server 1 cannot be re-used on server 2.

Note: To view a step-by-step setup of Extensions and handsets, please see chapter 7 *Appendix – Adding Extensions*

5.3.1 Add extension

STEP 1 Click add extension

Screenshot:

Note: The “AC” parameter below the **Extensions** header is the Access code used when registering a handset. For more information, please go to chapter 7 *Adding Extensions*

STEP 2 Fill in the required information

Screenshot

PARAMETER	DEFAULT VALUE(S)	DESCRIPTION
LINE NAME	Empty	Name of line shown to be used to show from which line the incoming call is coming and used when user must select from which line to make outgoing call.
HANDSET	New Handset	The extension must be associated to a handset. By default, a new handset can be configured, alternatively the user can select an already existing handset Idx.
PUSH-TO-TALK (PTT)	Disabled	The feature allows having P2P walkie-talkie, like voice calls between handsets and headsets on the VoIP system. Enable the feature to broadcast a PTT conference call to all portable devices.
EXTENSION	Empty	Handset phone number or SIP username depending on the setup. Possible value(s): 8-bit string length Example: 1024, etc. Note: The Extension must also be configured in SIP server in order for this feature to function.
AUTHENTICATION USER NAME	Empty	Username: SIP authentication username Permitted value(s): 8-bit string length
AUTHENTICATION PASSWORD	Empty	Password: SIP authentication password. Permitted value(s): 8-bit string length
DISPLAY NAME	Empty	Human readable name used for the given extension Permitted value(s): 8-bit string length
XSI USERNAME	Empty	Username: SIP authentication username Permitted value(s): 8-bit string length
XSI PASSWORD	Empty	Password: SIP authentication password. Permitted value(s): 8-bit string length
MAILBOX NAME	Empty	Name of centralized system used to store phone voice messages that can be retrieved by recipient later. Valid Input(s): 8-bit string Latin characters for the Name
MAILBOX NUMBER	Empty	Dialed mail box number by long key press on key 1. Valid Input(s): 0 – 9, *, # Note: Mailbox Number parameter is available only when it's enabled from SIP server.
SERVER	Server 1 IP	FQDN or IP address of SIP server. Drop down menu to select between the defined Servers of SME VoIP Service provider.
CALL WAITING FEATURE:	Enabled	Used to enable/disable Call Waiting feature. If disabled, a second incoming call will be rejected. If enabled, a second incoming call will be presented as call waiting. The feature is only valid when there is an active call. Note: An extension can only receive 1 alerting call. Therefore, during an alerting call that is not yet answered, the Call Waiting feature is not valid. Therefore, all other calls will be rejected and not queued.
BROADWORKS BUSY LAMP FIELD LIST URI	Empty	The "BLF" feature on the IP phones allows a specific extension to be monitored for state changes. BLF monitors the status (busy or idle) of extensions on the IP phone Permitted value(s): URL String Note: This feature does not work with Group call. Therefore, Group call should be disabled.
BROADWORKS SHARED CALL APPEARANCE	Disabled	Enable Shared Call Appearance (SCA) to allow a group of SIP phones to receive inbound calls directed to a single destination (shared line); that way, any phone from this group can answer the call, barge-in to the active call, or retrieve the call placed on hold. Note: Must be supported by SIP server

BROADSOFT FEATURE EVENT PACKAGE	Disabled	If enabled the given SIP extension subscribes for the Broadsoft Application Server Feature Event Package, and it becomes ready for reception of SIP NOTIFY with status on the following Broadsoft Server Services: -Do Not Disturb -Call Forwarding (Always, Busy, No answer) The received status will be displayed in the handset idle display.
UACSTA	Disabled	Enable/Disable uaCSTA support
FORWARDING UNCONDITIONAL NUMBER	Empty	Number to which incoming calls must be re-routed to irrespective of the current state of the handset. Forwarding Unconditional must be enabled to function.
	Disabled	Note: Feature must be enabled in the SIP server before it can function in the network
FORWARDING NO ANSWER NUMBER	Empty	Number to which incoming calls must be re-routed to when there is no response from the SIP end node.
	Disabled	Forwarding No Answer Number must be enabled to function.
	90	Note: Feature must be enabled in the SIP server before it can function in the network Specify delay from call to forward in seconds.
FORWARDING ON BUSY NUMBER	Empty	Number to which incoming calls must be re-routed to when SIP node is busy.
	Disabled	Forwarding on Busy Number must be enabled to function. Note: Feature must be enabled in the SIP server before it can function in the network
REJECT ANONYMOUS CALLS	Disabled	Calls from anonymous numbers will automatically be rejected. Enable to rejects anonymous calls

NOTE: Call forwarding can as well be configured from the handset by the user (for operation refer to the handset guide).

Screenshot

5.3.1.1 Extension list

The added extensions will be shown in the extension lists.

The list can be sorted by any of the top headlines, by mouse click on the headline link.

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
<input type="checkbox"/>	1	0276A584DA	Present@RPN00	8630 400.2	Off	<input type="checkbox"/> 1	510	510	192.168.11.99	HDJSERVER	SIP Registered@RPN00
<input type="checkbox"/>	2	02788888DB	Present@RPN00	8630 400.2	Off	<input type="checkbox"/> 2	511	511	192.168.11.99	HDJSERVER	SIP Registered@RPN00
<input type="checkbox"/>	3	02779C7F09	Present@RPN00	8630 400.2	Off	<input type="checkbox"/> 3	514	514	192.168.11.99	HDJSERVER	SIP Registered@RPN00
<input type="checkbox"/>	4	027792D0FE	Present@RPN00	8630 400.2	Off	<input type="checkbox"/> 4	513	513	192.168.11.99	HDJSERVER	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)

PARAMETER	DESCRIPTION
IDX	Index of handsets
IPEI	Handset IPEI. IPEI is unique DECT identification number.
HANDSET STATE	The state of the given handset: Present@RPNxx: The handset is DECT located at the base with RPNxx Detached: The handset is detached from the system (e.g. powered off) Located: The handset is configured to locate on a specific base, but is has not been possible to do so (e.g. if the base is powered off) Removed: The handset has been out of sight for a specified amount of time (~one hour).
HANDSET TYPE FW INFO	Name of the handset type Firmware version of handset
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 "Waiting for charger" (HS) / "Conn. term. wait" (Repeater): All FWU is complete and is now waiting for handset/repeater restart. Complete HS/repeater: FWU complete Error: Not able to fwu e.g. file not found, file not valid etc.
VOIP IDX	Index of the configured SIP extensions. Select/deselect to start SIP registration or delete extension.
EXTENSION	Given extension is displayed
DISPLAY NAME	Given display name is displayed. If no name given this field will be empty
SERVER	Server IP or URL
SERVER ALIAS	Given server alias is displayed. If no alias given this field will be empty.
STATE	SIP registration state – if empty the handset is not SIP registered.

5.3.1.2 Handset and extension list top/sub-menus

The handset extension list menu is used to control paring or deletion of handset to the system (DECT registration/de-registrations) and to control SIP registration/de-registrations to the system. Above and below the list are found commands for making operations on handsets/and extensions. The top menu is general operations, and the sub menu is always operating on selected handsets/extensions.

Screenshot

Add extension
Stop Registration

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)

In the below table, each command is described.

ACTIONS	DESCRIPTION
ADD EXTENSION	Access to the "Add extension" sub menu
STOP REGISTRATION	Manually stop DECT registration mode of the system. This prevents any handset from registering to the system
DELETE HANDSET(S)	Deregister selected handset(s), but do not delete the extension(s).
REGISTER HANDSET(S)	Enable registration mode for the system making it possible to register at a specific extension (selected by checkbox)
DEREGISTER HANDSET(S)	Deregister the selected handset(s) and delete the extension(s).
START SIP REGISTRATION(S)	Manually start SIP registration for selected handset(s).
DELETE SIP EXTENSION(S)	Deregister the selected handset(s) and delete the extension(s).

NOTE: By powering off the handset, the handset will SIP deregister from the PBX.

5.3.2 Edit Extension

To edit an extension simply click the extension number that you want to edit.

Screenshot

Extensions

AC:

[Add extension](#)
[Stop Registration](#)

	Idx	IPEI	Handset State	Handset Type FW Info	FWU Progress		VoIP Idx	Extension	Display Name	Server	Server Alias	State
<input type="checkbox"/>	1	0276A584DA	Present@RPN00	8630 400.2	Off	<input type="checkbox"/>	1	510	510	192.168.11.99	HDJSERVER	SIP Registered@RPN00
<input type="checkbox"/>	2	02788888DB	Present@RPN00	8630 400.2	Off	<input type="checkbox"/>	2	511	511	192.168.11.99	HDJSERVER	SIP Registered@RPN00
<input type="checkbox"/>	3	02779C7F09	Present@RPN00	8630 400.2	Off	<input type="checkbox"/>	3	514	514	192.168.11.99	HDJSERVER	SIP Registered@RPN00
<input type="checkbox"/>	4	027792D0FE	Present@RPN00	8630 400.2	Off	<input type="checkbox"/>	4	513	513	192.168.11.99	HDJSERVER	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\(s\)](#)

Then you will see the Edit extension page

Screenshot

Edit extension

Line name:	<input type="text" value="510"/>
Handset:	<input type="text" value="Handset Idx 1"/>
Push-To-Talk:	<input type="text" value="Disabled"/>
Extension:	<input type="text" value="510"/>
Authentication User Name:	<input type="text" value="510"/>
Authentication Password:	<input type="password" value="....."/>
Display Name:	<input type="text" value="510"/>
XSI Username:	<input type="text"/>
XSI Password:	<input type="password" value="....."/>
Mailbox Name:	<input type="text"/>
Mailbox Number:	<input type="text"/>
Server:	<input type="text" value="Test: 192.168.11.99"/>
Call waiting feature:	<input type="text" value="Enabled"/>
BroadWorks Busy Lamp Field List URI:	<input type="text"/>
BroadWorks Shared Call Appearance:	<input type="text" value="Disabled"/>
BroadWorks Feature Event Package:	<input type="text" value="Disabled"/>
UaCSTA:	<input type="text" value="Disabled"/>
Forwarding Unconditional Number:	<input type="text" value="Disabled"/>
Forwarding No Answer Number:	<input type="text" value="Disabled"/> <input type="text" value="90"/> s
Forwarding on Busy Number:	<input type="text" value="Disabled"/>
Reject anonymous calls:	<input type="text" value="Disabled"/>

Now you can edit the needed information and save the changes.

For detailed description of each field please see section 5.3.1 *Add extension*

5.3.3 Edit Handset

Use the mouse to click the handset IPEI link to open the handset editor window.

Screenshot

Handset (8631)

IPEI:

Paired Terminal:

Push-to-Talk:

AC:

Alarm Line:

Alarm Number:

Beacon Settings:

Receive Mode:

Transmit Interval:

Alarm Profiles:

Profile	Alarm Type	
Profile 0	Not configured	<input type="checkbox"/>
Profile 1	Not configured	<input type="checkbox"/>
Profile 2	Not configured	<input type="checkbox"/>
Profile 3	Not configured	<input type="checkbox"/>
Profile 4	Not configured	<input type="checkbox"/>
Profile 5	Not configured	<input type="checkbox"/>
Profile 6	Not configured	<input type="checkbox"/>
Profile 7	Not configured	<input type="checkbox"/>

Shared Call Appearance Settings:

Idx	Extension
1	<input type="text" value="Not configured"/>
2	<input type="text" value="Not configured"/>
3	<input type="text" value="Not configured"/>
4	<input type="text" value="Not configured"/>
5	<input type="text" value="Not configured"/>
6	<input type="text" value="Not configured"/>
7	<input type="text" value="Not configured"/>
8	<input type="text" value="Not configured"/>

Import Local Phonebook:

Filename: No file chosen

Export Local Phonebook:

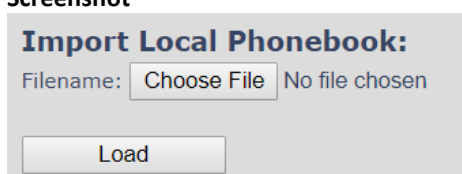
PARAMETER	DEFAULT VALUE(S)	DESCRIPTION
IPEI	Handset IPEI	Shows the handset IPEI. For an already registered handset changing the IPEI will deregister the handset at next handset location update.
PAIRED TERMINAL	No Paired Terminal	You can pair 2 terminals, e.g. Multicell handset with mi-MCH8930 headset For detailed information see mi-MCH8930 user guide
PUSH-TO-TALK (PTT)	Disabled	The feature allows having P2P walkie-talkie, like voice calls between handsets and headsets on the VoIP system. Enable the feature to broadcast a PTT conference call to all portable devices.
AC	Handset AC code	Shows the handset AC code. AC code is used at handset registration. Changing the AC code for an already registered handset will have no effect.
ALARM LINE	No Alarm Line Selected	The line of multiline to be used for alarm call feature

ALARM NUMBER	Empty	Number to be dialed in case of handset alarm key is pressed (Long keypress > 3 seconds on navigation center key)
RECEIVE MODE	Disabled	<p>NOTE: This feature is only shown if handsets have BTLE. When this feature is configured, every time an alarm is triggered, the strongest beacon will be included in the data sent to the message server.</p> <p>Enter Proximity: Leave Proximity: Enter or Leave Proximity:</p>
TRANSMIT INTERVAL	Disabled	NOTE: This feature is only shown if Handset has BTLE.
ALARM PROFILES	Not configured	Check the wanted alarm profiles for the particular handset.
SHARED CALL APPEARANCE SETTINGS	Not configured	<p>Each of the eight rows in the table represents an SCA status LED on the handset Idle screen. For each row it is possible to specify which shared line an LED should display the state of.</p> <ul style="list-style-type: none"> • Only shared lines can be selected, that is, only extensions defined for the handset for which BroadWorks Shared Call Appearance is enabled are included in the selector. • A shared line can be reused for several LEDs. Each LED with the same shared line then corresponds to different appearance-indexes for that line (1 LED = appearance-index 1, 2 LEDs = appearance-indexes 1 and 2, and so on). <p>It is not necessary to select a shared line for all the LEDs. If an LED is not assigned a line, its position on the screen is simply empty.</p>
IMPORT LOCAL PHONEBOOK		Import phonebook from csv file to this specific extension
EXPORT LOCAL PHONEBOOK		Exports this extensions phonebook as csv file NB: Home is not exported as this is considered private data.

5.3.3.1 Import local phonebook

The import local phonebook feature is using a browse file approach. After file selection press the load button to load the file. The system supports only the original *.csv format. Please note that some excel csv formats are not the original csv format.

Screenshot

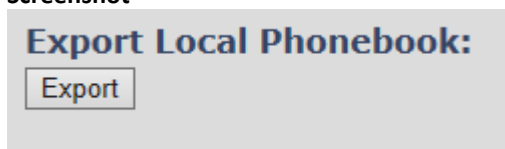


NOTE: The local phonebook can have 100 entries for mi-MCT8633W and mi-MCT385.

5.3.3.2 Export local phonebook

The Export local phonebook feature makes it possible to retrieve all contracts from a specific phone to a .CSV file.

Screenshot



Press the export button and save the .CSV file on you PC or Server.

5.4 Servers

In this section, we describe the different parameters available in the Servers configurations menu. Maximum 10 servers can be configured.

Screenshot

Servers

VoIPServer:
192.168.11.99
[Add Server](#)
[Remove Server](#)

VoIPServer:

Server Alias: VoIPServer

NAT Adaption: Enabled

Registrar: 192.168.11.99

Outbound Proxy:

Conference Server:

Call Log 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:

G711U
G711A
G726

Up Down Reset Codecs Remove

Use ptime: Enabled

RTP Packet Size: 20 ms

RTCP: Enabled

Secure RTP: Disabled

Secure RTP Auth: Disabled

SRTP Crypto Suites:

AES_CM_128_HMAC_SHA1_32
AES_CM_128_HMAC_SHA1_80

Up Down Reset Crypto Suites Remove

Save Cancel

PARAMETER	DEFAULT VALUE	DESCRIPTION
SERVER ALIAS	Empty	Parameter for server alias
NAT ADAPTION	Disabled	To ensure all SIP messages goes directly to the NAT gateway in the SIP aware router. If the system receives a SIP response to a REGISTER request with a "Via" header that includes the "received" parameter (ex: "Via: SIP/2.0/UDP 10.1.1.1:4540;received=68.44.20.1"), the base will adapt its contact information to the IP address from the "received" parameter. Thus, the base will issue another REGISTER request with the updated contact information. If NAT Adaption is disabled, the "received" parameter is ignored.
REGISTRAR	Empty	SIP Server proxy DNS or IP address

		Permitted value(s): AAA.BBB.CCC.DDD:<Port-Number> or <URL>:<Port-Number> Note: Specifying the Port Number is optional.
OUTBOUND PROXY	Empty	This is a Session Border Controller DNS or IP address (OR SIP server outbound proxy address) Set the Outbound proxy to the address and port of private NAT gateway so that SIP messages sent via the NAT gateway. Permitted value(s): AAA.BBB.CCC.DDD or <URL> or <URL>:<Port-Number> Examples: "192.168.0.1", "192.168.0.1:5062", "nat.company.com" and "sip:nat@company.com:5065". If empty call is made via Register.
CONFERENCE SERVER	Empty	Broadsoft conference feature. Set the IP address of the conference server. In case an IP is specified pressing handset, conference will establish a connection to the conference server. If the field is empty, the original 3-party local conference on 8630 is used.
CALL LOG SERVER	Empty	Broadsoft call log feature. Set the IP address of the XSI call log server. In case an IP is specified pressing handset will use the call log server. If the field is empty, the local call log is used
MUSIC ON HOLD SERVER	Empty	Add the address of a server for ensuring music is on when call is on hold
RE-REGISTRATION TIME	600	The "expires" value in SIP REGISTER requests. This value indicates how long the current SIP registration is valid, and hence is specifies the maximum time between SIP registrations for the given SIP account. Permitted value(s): A value below 60 sec is not recommended, Maximum value 65636
SIP SESSION TIMERS:	Disabled	RFC 4028. A "keep-alive" mechanism for calls. The session timer value specifies the maximum time between "keep-alive" or more correctly session refresh signals. If no session refresh is received when the timer expires the call will be terminated. Default value is 1800 s according to the RFC. Min: 90 s. Max: 65636. If disabled session timers will not be used.
SESSION TIMER VALUES (S):	1800	Default value is 1800s according to the RFC. If disabled session timers will not be used. Permitted value(s): Minimum value 90, Maximum 65636
SIP TRANSPORT	UDP	Select UDP, TCP, TLS 1.2
SIGNAL TCP SOURCE PORT	Disabled	When SIP Transport is set to TCP or TLS, a TCP (or TLS) connection will be established for each SIP extension. The source port of the connection will be chosen by the TCP stack, and hence the local SIP port parameter, specified within the SIP/RTP Settings (see 5.5.7) will not be used. The "Signal TCP Source Port" parameter specifies if the used source port shall be signaled explicitly in the SIP messages.
USE ONE TCP CONNECTION	Disabled	When using TCP as SIP transport, choose if a TCL/TLS connection

PER SIP EXTENSION:		shall be established for each SIP extension or if the Base station shall establish one connection which all SIP extensions use. Please note that if TLS is used and SIP server requires client authentication (and requests a client certificate), this setting must be set to disabled. 0: Disabled. (Use one TCP/TLS connection for all SIP extensions) 1: Enabled. (Use one TCP/TLS connection per SIP extensions).
RTP FROM OWN BASE STATION:	Disabled	If disabled RTP stream will be send from the base, where the handset is located. By enable the RTP stream will always be send from the base, where the SIP registration is made.
KEEP ALIVE	Enabled	This directive defines the window period (30 sec.) to keep opening the port of relevant NAT-aware router(s), etc.
SHOW EXTENSION ON HANDSET IDLE SCREEN	Enabled	If enabled extension will be shown on handset idle screen.
HOLD BEHAVIOUR	RFC 3264	Specify the hold behavior by handset hold feature. RFC 3264: Hold is signaled according to RFC 3264, i.e. the connection information part of the SDP contains the IP Address of the endpoint, and the direction attribute is sent only, recvonly or inactive dependent of the context RFC 2543: The "old" way of signaling HOLD. The connection information part of the SDP is set to 0.0.0.0, and the direction attribute is sent only, recvonly or inactive dependent of the context
LOCAL RING BACK TONE	Enabled	In case the server doesn't play local ring back tone the handset will do it.
REMOTE RING TONE CONTROL	Enabled	Sometimes call distinguished ringing. It enables the server to control what ring tone that is used on the handsets.
ATTENDED TRANSFER BEHAVIOUR	Hold 2 nd Call	When we have two calls, and one call is on hold, it is possible to perform attended transfer. When the transfer soft key is pressed in this situation, we have traditionally also put the active call on hold before the SIP REFER request is sent. However, we have experienced that some PBX's do not expect that the 2nd call is put on hold, and therefore attended transfer fails on these PBX's. The "Attended Transfer Behavior" feature defines whether the 2nd call shall be put on hold before the REFER is sent. If "Hold 2nd Call" is selected, the 2nd call will be held before REFER is sent. If "Do Not Hold 2nd Call" is selected, the 2nd call will not be held before the REFER is sent
DIRECT CALL PICKUP	Disabled	This is Part of BroadWorks SCA feature. Enabled a direct call pickup code is sent to the Handsets
DIRECT CALL PICKUP CODE	Empty	Code used to direct call pick up
GROUP CALL PICKUP	Disabled	Enable call group pickup
GROUP CALL PICKUP CODE	Empty	Code used to pick up a group call

USE OWN CODEC PRIORITY	Disabled	Default disabled. By enabling the system codec, priority during incoming call is used instead of the calling party priority. E.g. If base has G722 as top codec and the calling party has a law on top and G722 further down the list, the G722 will be chosen as codec for the call.
DTMF SIGNALLING	RFC 2833	Conversion of decimal digits (and '*' and '#') into sounds that share similar characteristics with voice to easily traverse networks designed for voice SIP INFO: Carries application level data along SIP signaling path (e.g.: Carries DTMF digits generated during SIP session OR sending of DTMF tones via data packets in the <u>same</u> internet layer as the Voice Stream, etc.). RFC 2833: DTMF handling for gateways, end systems and RTP trunks (e.g.: Sending DTMF tones via data packets in <u>different</u> internet layer as the voice stream) Both: Enables SIP INFO and RFC 2833 modes.
DTMF PAYLOAD TYPE	101	This feature enables the user to specify a value for the DTMF payload type / telephone event (RFC2833).
REMOTE CALLER ID SOURCE PRIORITY	FROM	SIP information field used for Caller ID source: PAI - FROM FROM ALERT_INFO - PAI - FROM
CODEC PRIORITY	G.711U G.711A G.726 G.722 G.729 OPUS BV32	Defines the codec priority that Base stations use for audio compression and transmission. Possible Option(s): G.711U, G.711A, G.726, G.722, G.729, OPUS, BV32 Note: Modifications of the codec list must be followed by a "reset codes" and "Reboot chain" on the multipage to change and update handsets. Note: With G.722 as priority, the number of simultaneous calls per Base station will be reduced from 10 (8) to 4 calls. With G.722 in the list, the codec negotiation algorithm is active causing the handset (phone) setup time to be slightly slower than if G.722 is removed from the list. Furthermore, it will reserve audio resources to be able to handle the possible G722 call and thus, the maximum number of possible narrowband calls will be reduced by one extra. Note: To use G.729 and OPUS, add on DSP module must be installed in all Base stations. Contact your local dealer for price information. Note: If BV32 is the only codec used (the only one in the priority list), the user should use handsets that support BV32 (mi-MCT8633W), else a call will not be established.
G729 Annex B		Enable/Disable Annex B of codec G729 Note: Both parts must support it in order to avoid noise and any other kind of voice interruption
USE PTIME	Enabled	Use the RTP Packet size, chosen in the below setting.
RTP PACKET SIZE	20ms	The packet size offered as preferred RTP packet size by 8630 when RTP packet size negotiation. Selections available: 20ms, 40ms, 60ms, 80ms
RTCP	Enabled	Enable/Disable RTCP
SEND SDP CAPABILITIES	Disabled	Enable to support RFC 5939

IN OFFER (RFC5939)		
SECURE RTP	Disabled	With enable RTP will be encrypted (AES-128) using the key negotiated via the SDP protocol at call setup.
SECURE RTP AUTH	Disabled	With enable secure RTP is using authentication of the RTP packages. Note: with enabled SRTP authentication maximum 4 concurrent calls are possible per base in a single or multicell system.
SRTP CRYPTO SUITES	mT	Field list of supported SRTP Crypto Suites. The device is born with two suites.

Note: Within servers or even with multi servers, extensions must always be unique. This means same extension number on server 1 cannot be re-used on server 2.

5.5 Network

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

Screenshot

Network Settings

<p>IP settings</p> <p>DHCP/Static IP: <input type="text" value="DHCP"/></p> <p>IP Address: <input type="text" value="192.168.11.186"/></p> <p>Subnet Mask: <input type="text" value="255.255.255.0"/></p> <p>Default Gateway: <input type="text" value="192.168.11.254"/></p> <p>DNS (Primary): <input type="text" value="10.1.1.10"/></p> <p>DNS (Secondary): <input type="text"/></p> <p>MDNS: <input type="text" value="Disabled"/></p>	<p>NAT Settings</p> <p>Enable STUN: <input type="text" value="Disabled"/></p> <p>STUN Server: <input type="text"/></p> <p>STUN Bindtime Determine: <input type="text" value="Enabled"/></p> <p>STUN Bindtime Guard: <input type="text" value="80"/></p> <p>Enable RPORT: <input type="text" value="Disabled"/></p> <p>Keep alive time: <input type="text" value="90"/></p>
<p>VLAN Settings</p> <p>ID: <input type="text" value="0"/></p> <p>User Priority: <input type="text" value="0"/></p> <p>Synchronization: <input type="text" value="Enabled"/></p>	<p>SIP/RTP Settings</p> <p>Use Different SIP Ports: <input type="text" value="Disabled"/></p> <p>RTP Collision Detection: <input type="text" value="Enabled"/></p> <p>Always reboot on check-sync: <input type="text" value="Disabled"/></p> <p>Outbound Proxy Mode: <input type="text" value="Use Always"/></p> <p>Failover SIP Timer B: <input type="text" value="5"/></p> <p>Failover SIP Timer F: <input type="text" value="5"/></p> <p>Local SIP port: <input type="text" value="5060"/></p> <p>SIP ToS/QoS: <input type="text" value="0x68"/></p> <p>RTP port: <input type="text" value="50004"/></p> <p>RTP port range: <input type="text" value="254"/></p> <p>RTP ToS/QoS: <input type="text" value="0xB8"/></p> <p>Reject anonymous calls: <input type="text" value="Disabled"/></p>
<p>DHCP Options</p> <p>Plug-n-Play: <input type="text" value="Enabled"/></p>	
<p>TCP Options</p> <p>TCP Keep Alive Interval: <input type="text" value="120"/></p>	
<p>Discovery</p> <p>LLDP-MED Send: <input type="text" value="Disabled"/></p> <p>LLDP-MED Send delay: <input type="text" value="30"/></p> <p>VLAN via LLDP-MED: <input type="text" value="Disabled"/></p> <p>CDP Send: <input type="text" value="Disabled"/></p> <p>CDP Send delay: <input type="text" value="60"/></p>	

5.5.1 IP Settings

Screenshot

IP settings

DHCP/Static IP:

IP Address:

Subnet Mask:

Default Gateway:

DNS (Primary):

DNS (Secondary):

MDNS:

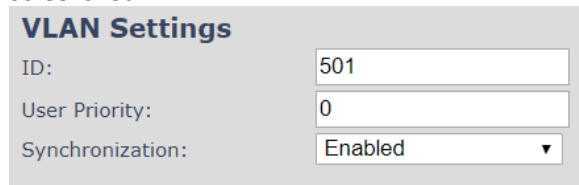
PARAMETER	DEFAULT VALUES	DESCRIPTION
DHCP/STATIC IP	DHCP	<p>If DHCP is enabled, the device automatically obtains TCP/IP parameters. Possible value(s): Static, DHCP</p> <p>DHCP: IP addresses are allocated automatically from a pool of leased address.</p> <p>Static IP: the network administrator manually assigns IP addresses. If the user chooses DHCP option, the other IP settings or options are not available.</p>
IP ADDRESS	NA	<p>32-bit IP address of device (e.g. Base station). 64-bit IP address will be supported in the future. Permitted value(s): AAA.BBB.CCC.DDD</p>
SUBNET MASK	NA	<p>Is device subnet mask. Permitted value(s): AAA.BBB.CCC.DDD</p> <p>This is a 32-bit combination used to describe which portion an IP address refers to the subnet and which part refers to the host. A network mask helps users know which portion of the address identifies the network and which portion of the address identifies the node.</p>
DEFAULT GATEWAY	NA	<p>Device's default network router/gateway (32-bit). Permitted value(s): AAA.BBB.CCC.DDD e.g. 192.168.50.0</p> <p>IP address of network router that acts as entrance to another network. This device provides a default route for TCP/IP hosts to use when communicating with other hosts on hosts networks.</p>
DNS (PRIMARY)	NA	<p>Main server to which a device directs Domain Name System (DNS) queries. Permitted value(s): AAA.BBB.CCC.DDD or <URL></p> <p>This is the IP address of server that contains mappings of DNS domain names to various data, e.g. IP address, etc. The user needs to specify this option when static IP address option is chosen.</p>
DNS (SECONDARY)	NA	<p>This is an alternate DNS server.</p>
MDNS	Disabled	<p>Enable to allow Multicast Domain Name system (MDNS)</p>

5.5.2 VLAN Settings

Enable users to define devices (e.g. Base station, etc.) with different physical connection to communicate as if they are connected on a single network segment.

The VLAN settings can be used on a managed network with separate Virtual LANs (VLANs) for sending voice and data traffic. To work on these networks, the Base stations can tag voice traffic it generates on a specific “voice VLAN” using the IEEE 802.1q specification.

Screenshot

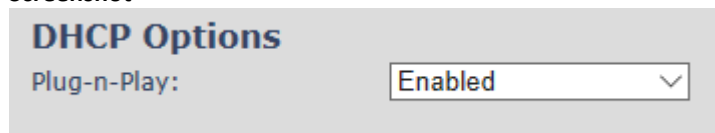


PARAMETER	DEFAULT VALUES	DESCRIPTION
ID	0	Is a 12-bit identification of the 802.1Q VLAN. Permitted value(s): 0 to 4094 (only decimal values are accepted) A VLAN ID of 0 is used to identify priority frames and ID of 4095 (i.e. FFF) is reserved. Null means no VLAN tagging or No VLAN discovery through DHCP.
USER PRIORITY	0	This is a 3-bit value that defines the user priority. Values are from 0 (best effort) to 7 (highest); 1 represents the lowest priority. These values can be used to prioritize different classes of traffic (voice, video, data, etc.). Permitted value(s): 8 priority levels (i.e. 0 to 7)
SYNCHRONIZATION	Disabled	Default disabled. By enabled the VLAN ID is automatic synchronized between the bases in the chain. Bases will be automatic rebooted during the synchronization. Note: If using different VLANs, the synchronization should be disabled. The setting must be changed on each Base station due to non-synchronization between them

For further help on VLAN configuration refer to Appendix.

5.5.3 DHCP Options

Screenshot



PARAMETER	DEFAULT VALUES	DESCRIPTION
PLUG-N-PLAY	Enabled	Enabled: DHCP option 66 to automatically provide PBX IP address to base.

5.5.4 TCP Options

Screenshot

TCP Options

TCP Keep Alive Interval:

PARAMETER	DEFAULT VALUES	DESCRIPTION
TCP KEEP ALIVE INTERVAL	120s	Specifies the interval the client waits before sending a keep-alive message on a TCP connection.

5.5.5 Discovery

Screenshot

Discovery

LLDP-MED Send:

LLDP-MED Send delay:

VLAN via LLDP-MED:

CDP Send:

CDP Send delay:

PARAMETER	DEFAULT VALUES	DESCRIPTION
LLDP-MED SEND	Disabled	If "Enabled", the BS will send 5 LLDP-MED messages when started.
LLDP-MED SEND DELAY	30	Sends messages every 30 seconds to inform the network about its LLDP-MED data Note: This option works only if the first parameter is enabled (LLDP-MED SEND)
VLAN VIA LLDP-MED	Disabled	If "Enabled", the BS will try to retrieve a VLAN ID from the received LLDP-MED from a switch Note: This feature is available only if the first parameter is enabled (LLDP-MED SEND)
CDP SEND	DISABLED	Enable to send CDP messages
CDP SEND DELAY	60	Define the delay between messages in seconds

5.5.6 NAT Settings

We define some options available when NAT aware routers are enabled in the network.

Screenshot

NAT Settings

Enable STUN:

STUN Server:

STUN Bindtime Determine:

STUN Bindtime Guard:

Enable RPORT:

Keep alive time:

PARAMETER	DEFAULT VALUES	DESCRIPTION
ENABLE STUN	Disabled	Enable to use STUN
STUN SERVER	NA	Permitted value(s): AAA.BBB.CCC.DDD (Currently only Ipv4 are supported) or URL (e.g.: firmware.mialert.com).

STUN BINDTIME DETERMINE	Enabled	
STUN BINDTIME GUARD	80	Permitted values: Positive integer default is 90, unit is in seconds
ENABLE RPORT	Disabled	Enable to use RPORT in SIP messages.
KEEP ALIVE TIME	90	This defines the frequency of how keep-alive are sent to maintain NAT bindings. Permitted values: Positive integer default is 90, unit is in seconds

5.5.7 SIP/RTP Settings

These are some definitions of SIP/RTP settings:

Screenshot

PARAMETER	DEFAULT VALUES	DESCRIPTION
USE DIFFERENT SIP PORTS	Disabled	If disabled, the Local SIP port parameter specifies the source port used for SIP signaling in the system. If enabled, the Local SIP Port parameter specifies the source port used for first user agent (UA) instance. Succeeding UA's will get succeeding ports.
RTP COLLISION DETECTION	Enabled	Enable: If two sources with same SSRC, the following RTP is discarded. Disabled: No check – device will accept all sources.
ALWAYS REBOOT ON CHECK-SYNC	Disabled	Reboot Base station when new configuration I loaded.
OUTBOUND PROXY MODE	Use Always	Use Always: All outbound calls are sent to outbound proxy Only Initial request: Only use outbound proxy for initial SIP requests
FAILOVER SIP TIMER B	5	When the time expires and the corresponding SIP transaction fails, failover will be triggered
FAILOVER SIP TIMER F	5	When the time expires and the corresponding SIP transaction fails, failover will be triggered
LOCAL SIP PORT	5060	The source port used for SIP signaling Permitted values: Port number default 5060.

SIP TOS/QOS	0x68	<p>Priority of call control signaling traffic based on both IP Layers of Type of Service (ToS) byte. ToS is referred to as Quality of Service (QoS) in packet-based networks.</p> <p>Permitted values: Positive integer, default is 0x68</p>
RTP PORT	50004	<p>The first RTP port to use for RTP audio streaming.</p> <p>Permitted values: Port number default 50004 (depending on the setup).</p>
RTP PORT RANGE	40	<p>The number of ports that can be used for RTP audio streaming.</p> <p>Permitted values: Positive integers, default is 40</p>
RTP TOS/QOS	0xB8	<p>Priority of RTP traffic based on the IP layer ToS (Type of Service) byte. ToS is referred to as Quality of Service (QoS) in packet-based networks. See RFC 1349 for details. "cost bit" is not supported.</p> <ul style="list-style-type: none"> o Bit 7..5 defines precedence. o Bit 4..2 defines Type of Service. o Bit 1..0 are ignored. <p>Setting all three of bit 4..2 will be ignored.</p> <p>Permitted values: Positive integer, default is 0xB8</p>
REJECT ANONYMOUS CALLS	Disabled	<p>If disabled, all calls will be received.</p> <p>If enabled, calls not registered will be automatically rejected</p>

5.6 Management Settings Definitions

The administrator can configure Base stations to perform some specific functions such as configuration of file transfers, firmware up/downgrades, password management, and SIP/debug logs.

Screenshot

Management Settings

Base Station Name:

Settings

Management Transfer Protocol:

HTTP Management upload script:

HTTP Management username:

HTTP Management password:

Factory reset from button:

Enable Automatic Prefix:

Set Maximum Digits of Internal Numbers:

Set Prefix for Outgoing Calls:

Text Messaging

Text Messaging:

Text Messaging & Alarm Server:

Text Messaging Port:

Text Messaging Keep Alive (m):

Text Messaging Response (s):

Text Messaging TTL:

Configuration

Configuration File Download:

Configuration Server Address:

Base Specific File:

Multi Cell Specific File:

Auto Resync Polling:

Auto Resync Time:

Auto Resync Days:

Auto Resync Periodic (Min):

Auto Resync Max Delay (Min):

DHCP Controlled Config Server:

DHCP Custom Option:

DHCP Custom Option Type:

Terminal

Keep Alive (m):

Auto Stop Alarm:

Auto Stop Alarm Delay (s):

License

Idx	Description
No Entries	

License Key:

Syslog/SIP Log

Upload of SIP Log:

Syslog Level:

TLS security:

Syslog Server IP Address:

Syslog Server Port:

Location Gateway

Location Gateways:

Configuration Server:

Auto Resync Polling:

Auto Resync Time:

Auto Resync Max Delay (Min):

5.6.1 Settings:

PARAMETER	Default value	Description
BASE STATION NAME:	SME VoIP	It indicates the title that appears at the top window of the browser and is used in the multicell page. Maximum characters: 35
MANAGEMENT TRANSFER PROTOCOL	TFTP	The protocol assigned for configuration file and central directory Valid Input(s): TFTP, HTTP, HTTPs

HTTP MANAGEMENT UPLOAD SCRIPT	Empty	The folder location or directory path that contains the configuration files of the Configuration server. The configuration upload script is a file located in e.g. TFTP server or Apache Server which is also the configuration server. Permitted value(s): /<configuration-file-directory> Example: /CfgUpload Note: Must begin with (/) slash character. Either / or \ can be used.
HTTP MANAGEMENT USERNAME	Empty	Username that should be entered in order to have access to the configuration server. Permitted value(s): 8-bit string length
HTTP MANAGEMENT PASSWORD	Empty	Password that should be entered in order to have access to the configuration server. Permitted value(s): 8-bit string length
FACTORY RESET FROM BUTTON	Enabled	If enabled a factory reset will be possible by pressing the button on the BS If disabled, no action will be present by pressing the button on the BS
ENABLE AUTOMATIC PREFIX	Disabled	Disabled: Feature off. Enabled: The base will add the leading digit defined in "Set Prefix for Outgoing Calls". Enabled + fall through on * and #: Will enable detection of * or # at the first digit of a dialed number. In case of detection the base will not complete the dialed number with a leading 0. Examples: 1: dialed number on handset * 1234 -> dialed number to the pabx *1234 2: dialed number on handset #1234 -> dialed number to the pabx #1234 3: dialed number on handset 1234 -> dialed number to the pabx 01234
SET MAXIMUM DIGITS FOR INTERNAL NUMBERS	0	Used to detect internal numbers. In case of internal numbers, no prefix number will be added to the dialed number.
SET PREFIX FOR OUTGOING CALLS	Empty	Set the prefix for outgoing calls. Users need to dial this prefix to get an outside line.

5.6.2 Configuration:

PARAMETER	Default value	Description
CONFIGURATION FILE DOWNLOAD	Disabled	Base Specific file: Used when configuring a single cell base Base and Multicell Specific File: Used on out of factory bases to specify VLAN and settings.
CONFIGURATION SERVER ADDRESS	Empty	Server/device that provides configuration file to Base station. Type: DNS or IP address Permitted value(s): AAA.BBB.CCC.DDD or <URL>
BASE SPECIFIC FILE	Empty	Base configuration file
MULTI CELL SPECIFIC FILE	Empty	The file name must be the chain id of the system. E.g. 00087b0a00b3.cfg Permitted value(s): Format of file is chain ID.cfg
AUTO RESYNC POLLING	Disabled	Enable to have the Base station look for new configuration file, with a predefined time interval
AUTO RESYNC TIME	00:00	Time when the Base station shall load the configuration file 24 hour setting
AUTO RESYNC DAYS	0	Number of days between Auto Resync

AUTO RESYNC PERIODIC (MIN)	0	Number of minutes between Auto Resync
AUTO RESYNC MAX DELAY (MIN)	15	Delay time in sec, to prevent all Base station asking for configuration fin at the same time.
DHCP CONTROLLED CONFIG SERVER	Disabled	Provisioning server options. DHCP Option 66: Look for provision file by TFTP boot up server. DHCP Custom Option: Look for provision file by custom option DHCP Custom Option & Option 66: Look for provision file by first custom option and then option 66. From v460, the Base station supports configuration files of up to 1 MB
DHCP CUSTOM OPTION	Empty	By default, option 160, but custom option can be defined. An option 160 URL defines the protocol and path information by using a fully qualified domain name for clients that can use DNS.
DHCP CUSTOM OPTION TYPE	Empty	URL: URL of server with path. Example of URL: http://myconfigs.com:5060/configs Default configuration file on server must follow the name: MAC.cfg IP Address: IP of server with path.

5.6.3 Text messaging:

PARAMETER	DEFAULT VALUE	DESCRIPTION
TEXT MESSAGING	Disabled	Disable/enable messaging using a Message/Alarm server Enable Without Server. With this setting handset can send messages to other handsets, which support messaging.
TEXT MESSAGING & ALARM SERVER	Empty	Permitted value(s): AAA.BBB.CCC.DDD or <URL> Note: Text messaging server uses UDP and does not support TLS
TEXT MESSAGING PORT	1300	Port number of message server.
TEXT MESSAGING KEEP ALIVE (M)	30	This defines the frequency of how keep-alive are sent Permitted values: Positive integer, unit is in minutes
TEXT MESSAGING RESPONSE (S)	30	This defines the frequency of how response timeout Permitted values: Positive integer, unit is in seconds
TEXT MESSAGING TTL	0	This defines the text messaging time to live Permitted values: Positive integer, unit is in seconds

5.6.4 Terminal:

PARAMETER	DEFAULT VALUE	DESCRIPTION
KEEP ALIVE (M)	0	If different from "0" the handset sends a (emergencyLocationMsg) containing the RSSI measurements with interval "x" that is set. Permitted values: Positive integer, unit is in minutes
AUTO STOP ALARM	Disabled	Enable to activate "AUTO STOP ALARM DELAY"
AUTO STOP ALARM DELAY (S)	30	Handset automatically stops alarm announcement (emergencySms) after "x" sec.

5.6.5 Syslog/SIP Log:

PARAMETER	DEFAULT VALUE	DESCRIPTION
UPLOAD OF SIP LOG	Disabled	Enable this option to save low level SIP debug messages to the server. The SIP logs are saved in the file format: <MAC_Address><Time_Stamp>SIP.log
SYSLOG LEVEL	Normal Operation	Off: No data is saved on syslog server Normal Operation: Normal operation events are logged, incoming call, outgoing calls, handset registration, DECT location, and call lost due to busy, critical system errors, general system information. System Analyze: Handset roaming, handset firmware updates status. The system analyze level also contains the messages from normal operation. Debug: Used by miALERT for debug. Should not be enabled during normal operation.
TLS SECURITY	Disabled	If enabled, it uses encrypted TCP, else - UDP
SYSLOG SERVER IP ADDRESS	Empty	Permitted value(s): AAA.BBB.CCC.DDD or <URL>
SYSLOG SERVER PORT	514	Port number of syslog server.

There are three ways of configuring the system.

1. Manual configuration by use of the Web server in the Base station(s)
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(s) download(s) from a configuration server.

5.6.6 Location Gateway

PARAMETER	DEFAULT VALUE	DESCRIPTION
LOCATION GATEWAYS	Disabled	Enable to allow Location Gateways onto the system. When enabled “Location Gateway” menu will be shown on main menu on the left.
CONFIGURATION SERVER	Empty	Permitted value(s): AAA.BBB.CCC.DDD or <URL>
AUTO RESYNC POLLING	Disabled	The poll enables the configuration server to start the provisioning process for the Location Gateway devices that it chooses. If “Enabled”, it enables an automatic configuration synchronization poll for the Location Gateway(s)
AUTO RESYNC TIME		The time of the day that the automatic synchronization will occur (HH:MM).
AUTO RESYNC MAX DELAY (MIN)		To distribute load such that all bases do not sync at the exact same time, the Auto Resync Max Delay can be set to delay the poll trigger with a given number of minutes. The delay will be a random number between 0 minutes and the value given in this parameter.

5.6.7 License

PARAMETER	DEFAULT VALUE	DESCRIPTION
LICENSE KEY	None	This feature allows administrators to register mi-MCH8930 genetic headsets to the system. License key must be obtained from authorized resellers and only license matching the systems provider code will work.

5.7 Firmware Update Definitions

On this page, the system administrator can configure how Base stations and SIP nodes upgrade/downgrade to the relevant firmware and upload startup/background picture to the handsets. Handset firmware update status can be found in the **Extensions** page and repeater firmware update status in the **Repeaters** page. Base firmware update status is found in the **Multi cell** page. For more details on how to upgrade/downgrade the firmware, or upload an image, please see *8. Appendix – Firmware Upgrade procedure*.

Screenshot

PARAMETER	DEFAULT VALUE(S)	DESCRIPTION
FIRMWARE UPDATE SERVER ADDRESS	Empty	IP address or DNS of firmware update files source Valid Inputs: AAA.BBB.CCC.DDD or <URL> Example: firmware.mialert.com or 10.10.104.41
FIRMWARE PATH	Empty	Location of firmware on server (or firmware update server path where firmware update files are located). Example: Firmware
TERMINAL FILE PATH	Empty	Location of image (folder where background and start up image are located). Example: Images
REQUIRED VERSION	Empty	Version of firmware to be upgraded (or downgraded) on handset, repeater, or Base station. Valid Input(s): 8-bit string length. E.g. 400 Note: Value version 0 will disable firmware upgrade Note: Two handset types will be serial firmware upgraded. First type 8630 then type 8430.
REQUIRED BRANCH	Empty	Branch of firmware to be upgraded (or downgraded) handset, repeater or Base station. Valid Input(s): 8-bit string length. E.g. 01
STARTUP PICTURE	Empty	Name of the startup picture you want on the handsets when they are powered up.

		<p>NOTE: Images have the same resolution as the screen on the handset(s); Resolution info can be found in the handset datasheets If the image does not have the same resolution as the screen, it will be placed in the top left corner. If it is too small, the rest of the screen will be black. If it is too large, only the left portion of the image will be shown.</p> <p>NOTE: Only .BMP is files are supported.</p>
BACKGROUND PICTURE	Empty	<p>Name of the background picture you want on the handsets when they are powered up.</p> <p>NOTE: Images have same resolution as the screen on the handset(s), this can be found in the handset datasheets. If the image does not have the same resolution as the screen, it will be placed in the top left corner. If it is too small, the rest of the screen will be black. If it is too large, only the left portion of the image will be shown</p> <p>NOTE: Only .BMP is files are supported.</p>
VOICE PROMPT	Empty	<p>Name of the voice prompt file Only possible for headsets.</p>

5.7.1 Warning message when firmware upgrading

A warning message will be displayed when starting firmware upgrade.

The parameters are successfully saved
You will be redirected after 3 seconds

DO NOT, power off base stations or remove handsets from charger during firmware update as this can break the unit.

5.8 Location Gateways

This section aims to show the user how to connect the Location Gateway to the system. For more details of the mi-MCG8200 device, please ask for the mi-MCG8200 Location Gateway user manual.

5.8.1 Register Location gateway

STEP 1 Allow Location Gateways on the system by enabling the “Location Gateway” parameter on the management page (Please go to 5.6.6). Press **Save**

Location Gateway

Location Gateways:

Configuration Server:

Auto Resync Polling:

Auto Resync Time:

Auto Resync Max Delay (Min):

STEP 2 Select Add Location Gateway extension

Location Gateways

[Add Location Gateway extension](#)
[Stop Registration](#)

<u>Idx</u>	<u>IPEI</u>	<u>Location Gateway State</u>	<u>Location Gateway Type FW Info</u>	<u>FWU Progress</u>
There are currently no extensions for server				

STEP 3 Press save and leave the IPEI: FFFFFFFF

Location Gateway

IPEI:

STEP 4 Check the box of the Location gateways that you want to add and select Register Location Gateway

Location Gateways

[Add Location Gateway extension](#)
[Stop Registration](#)

<u>Idx</u>	<u>IPEI</u>	<u>Location Gateway State</u>	<u>Location Gateway Type FW Info</u>	<u>FWU Progress</u>
<input checked="" type="checkbox"/>	1	FFFFFFFF		

Check All /Uncheck All

With selected: [Delete Location Gateway](#) [Register Location Gateway\(s\)](#) [Deregister Location Gateway\(s\)](#)

STEP 5 Power on the Location Gateway and after a few seconds the device will be registered

Location Gateways

[Add Location Gateway extension](#)
[Stop Registration](#)

<u>Idx</u>	<u>IPEI</u>	<u>Location Gateway State</u>	<u>Location Gateway Type FW Info</u>	<u>FWU Progress</u>
<input type="checkbox"/>	1	0328D3C941	Present@RPN00	8200 625.836 Off

Check All /Uncheck All

With selected: [Delete Location Gateway](#) [Register Location Gateway\(s\)](#) [Deregister Location Gateway\(s\)](#)

5.9 Country/Time Settings

In this section, we describe the different parameters available in the Time Server menu.

The country setting controls the in-band tones used by the system.

The Time server supplies the time used for data synchronisation in a multi-cell configuration. As such it is mandatory for a multi-cell configuration. The system will not work without a time server configured.

As well the time server is used in the debug logs and for SIP traces information pages and used to determine when to check for new configuration and firmware files.

NOTE: It is not necessary to set the time server for standalone Base stations (optional).

Press the “Time PC” button to grab the current PC time and use in the time server fields.

NOTE: When time server parameters are modified/changed synchronisation between Base stations can take up to 15 minutes before all Base stations are synchronised, depending on the number of Base stations in the system. Changing time settings will require a reboot of system.

Country/Time Settings

Select country:

State / Region:

Notes:

Select Language:

Time Server:

Allow broadcast NTP:

Refresh time (h):

Set timezone by country/region:

Timezone:

Set DST by country/region:

Daylight Saving Time (DST):

DST Fixed By Day:

DST Start Month:

DST Start Date:

DST Start Time:

DST Start Day of Week:

DST Start Day of Week Last in Month:

DST Stop Month:

DST Stop Date:

DST Stop Time:

DST Stop Day of Week:

DST Stop Day of Week Last in Month:

PARAMETER	DEFAULT VALUES	DESCRIPTION
SELECT COUNTRY	US/Canada	Supported countries: Australia, Belgium, Brazil, Denmark, Germany, Spain, France, Ireland, Italia, Luxembourg, Nederland, New Zealand, Norway, Portugal, Swiss, Finland, Sweden, Turkey, United Kingdom, US/Canada, Austria
STATE / REGION	NA	Only shown by country selection US/Canada, Australia, Brazil
SELECT LANGUAGE	English	Web interface language. Number of available languages: English, Dansk, Italiano, Trike, Deutsch, Portuguese, Hrvatski, Srpski, Slovenian, Nederland's, Francaise, Espanyol, Russian, Polski.
TIME SERVER	Empty	DNS name or IP address of NTP server. Enter the IP/DNS address of the server that distributes reference clock information to its clients including Base stations, Handsets, etc. Valid Input(s): AAA.BBB.CCC.DDD or URL (e.g. time.server.com) Currently only Ipv4 address (32-bit) nomenclature is supported.
ALLOW BROADCAST NTP	Checked	By checked time server is used.
REFRESH TIME (H)	24	The window time in hours within which time server refreshes. Valid Inputs: positive integer
SET TIME ZONE BY COUNTRY/REGION	Checked	By checked country setting is used (refer to country web page).
TIME ZONE	0	Refers to local time in GMT or UTC format. Min: -12:00 Max: +13:00
SET DST BY COUNTRY/REGION	Checked	By checked country setting is used (refer to country web page).
DAYLIGHT SAVING TIME (DST)	Disabled	The system administrator can Enable or Disable DST manually. Automatic: Enter the start and stop dates if you select Automatic.
DST FIXED BY DAY	Use Month and Day of week	You determine when DST actually changes. Choose the relevant date or day of the week, etc. from the drop-down menu.
DST START MONTH	March	Month that DST begins Valid Input(s): Gregorian months (e.g. January, February, etc.)
DST START DATE	0	Numerical day of month DST comes to effect when DST is fixed to a specific date Valid Inputs: positive integer
DST START TIME	2	DST start time in the day Valid Inputs: positive integer
DST START DAY OF WEEK	Sunday	Day within the week DST begins
DST START DAY OF WEEK, LAST IN MONTH	Second First In Month	Specify the week that DST will actually start.
DST STOP MONTH	October	The month that DST actually stops.
DST STOP DATE	0	The numerical day of month that DST turns off. Valid Inputs: positive integer (1 to 12)
DST STOP TIME	2	The time of day DST stops Valid Inputs: positive integer (1 to 12)
DST STOP DAY OF WEEK	Sunday	The day of week DST stops
DST STOP DAY OF WEEK LAST IN MONTH	First in Month	The week within the month that DST will turn off.

NOTE: By checked time zone and DST the parameters in web page Time will be discarded.

The following types of in-band tones are supported:

- Dial tone
- Busy tone
- Ring Back tone
- Call Waiting tone
- Re-order tone

5.10 Security

The security section is used for loading certificates, changing web authentication, and configuring a secure web server. To setup secure fwu and configuration file download, go to the **Management** menu and select HTTPs for the “Management Transfer Protocol”.

SIP and RTP security are server dependent, therefore the user must use the menu option **Servers** in order to configure them.

The Identity and Trusted certificates are preserved during upgrade. However, during a factory default, all certificates that have been installed via the web server, will be deleted. The base does not include any default trusted certificates. Please note that, there is no expiration notification for the certificates.

Security

Device Identity

Idx	Issued To	Issued By	Valid Until
No certificates installed:			

Import Device Certificate and Key Pair:

Filename: No file chosen

Trusted Server Certificates

Idx	Issued To	Issued By	Valid Until
No certificates installed:			

Import Trusted Certificates:

Filename: No file chosen

Trusted Root Certificates

Idx	Issued To	Issued By	Valid Until
No certificates installed:			

Import Root Certificate:

Filename: No file chosen

Use Only Trusted Certificates:

Password:

Username:

Current Password:

New Password:

Confirm Password:

Secure Web Server:

HTTPS:

5.10.1 Device identity

The certificate and personal key used by the base when acting as a server or when the server requires client authentication in the SSL handshake procedure.

Screenshot:

5.10.2 Trusted Server Certificates

Intermediate certificates (non-root certificates) trusted by the base. Used to validate a received certificate chain (or a chain of trust) in scenarios where only the root certificate is sent by the server during the SSL handshake procedure.

Screenshot:

5.10.3 Trusted Root Certificates

Root certificates (self-signed) trusted by the base. Used to validate received root certificates sent by the server during the SSL handshake procedure.

Screenshot:

By enabling “Use Only Trusted Certificates”, the certificate validity period is checked. Therefore, the certificates which the base will receive from the server, must be valid and loaded into the system. If no valid matching certificate is found during the TLS connection establishment, the connection will fail. When “Use Only Trusted Certificates” is disabled, all certificates received from the server will be accepted.

NOTE: It is important to use correct date and time of the system when using trusted certificates. In case of undefined time/date, the certificate validation can fail.

5.10.4 Password

In the below the authentication parameters are defined.

Password:

Username:

Current Password:

New Password:

Confirm Password:

PARAMETER	Default Values	Description
USERNAME	Admin	Can be modified to any supported character and number Maximum characters: 15
CURRENT PASSWORD	Admin	Can be modified to any supported character and number
NEW PASSWORD	Empty	Change to new password Maximum characters: 15
CONFIRM PASSWORD	Empty	Confirm password to reduce accidentally wrong changes of passwords

Password valid special signs: @/|<>_-.!?*+
 Password valid numbers: 0-9
 Password valid letters: a-z and A-Z

5.10.5 Secure Web Server

This setting allows all communication with the Web Server to be encrypted.

Screenshot

Secure Web Server:

HTTPS:

PARAMETER	DEFAULT VALUES	DESCRIPTION
HTTPS	Disabled	Enable to use HTTPS for Web Server Communication.

5.11 Central Directory and LDAP

The SME VOIP system supports three types of central directories - local central directory, LDAP and XML directory. For all directories' caller id look up is made with match for 6 digits of the phone number.

5.11.1 Local Central Directory

Select “Local” and save for local central directory.

Screenshot

PARAMETER	DEFAULT VALUES	DESCRIPTION
LOCATION	Local	Drop down menu to select between local central directory, LDAP based central directory and XML server
SERVER	Empty	The parameter is used if directory file is located on a server Valid inputs: aaa.bbb.ccc.ddd or <url> Refer to appendix for further details.
FILENAME	Empty	The parameter is used if directory file is located on server. Refer to appendix for further details
PHONEBOOK RELOAD INTERVAL (S)	0	The parameter is controlling the reload interface of phonebook in seconds. The feature is for automatic reload the base phonebook file from the server with intervals. It is recommended to specify a conservative value to avoid overload of the Base station. With default value setting 0 the reload feature is disabled.

5.11.2 Import Central Directory

The import central directory feature is using a browse file approach. After file selection press the load button to load the file. The system supports only the original *.csv format. Please note that some excel csv formats are not the original csv format. The central directory feature can handle up to 3000 contacts (Max file size 100kb). For further details of the central directory feature refer to appendix.

5.11.3 LDAP

Select “LDAP Server” from the “Location” parameter and wait a few seconds for the new configuration menu. Fill in the empty fields with the needed data and press **Save**.

LDAP Central Directory

Central Directory Location:

Server:

TLS security:

Port:

Sbase:

LDAP Filter:

Bind:

Password:

Virtual List:

Handset Identity:

Name:

Work:

Home:

Mobile:

PARAMETER	DEFAULT VALUES	DESCRIPTION
CENTRAL DIRECTORY LOCATION	LDAP Server	Drop down menu to select between local central directory and LDAP based central directory. LDAP Server is displayed when LDAP server is selected.
SERVER	Empty	IP address of the LDAP server. Valid Inputs: AAA.BBB.CCC.DDD or <URL>
TLS SECURITY	Disable	If enabled, it uses encrypted TCP, else – UDP Note: In most cases LDAP over TLS is running on port 636
PORT	Empty	The server port number that is open for LDAP connections Note: In most cases LDAP over TLS is running on port 636
SBASE	Empty	Search Base. The criteria depend on the configuration of the LDAP server. Example of the setting is CN=Users, DC=umber, DC=loc
LDAP FILTER	Empty	LDAP Filter is used to as a search filter, e.g. setting LDAP filter to ((givenName=%*)(sn=%*)) the IP-DECT will use this filter when requesting entries from the LDAP server. % will be replaced with the entered prefix e.g. searching on J will give the filter ((givenName=J*)(sn=J*)) resulting in a search for given name starting with a J or surname starting with J.
BIND	Empty	Bind is the username that will be used when the IP-DECT phone connects to the server
PASSWORD	Empty	Password is the password for the LDAP Server
VIRTUAL LIST	Disabled	By enable, virtual list searching is possible
NAME	Empty	The name can be used to specify if sn+givenName or cn (common name) is return in the LDAP search results
WORK NUMBER	Empty	Work number is used to specify that LDAP attribute that will be mapped to the handset work number
HOME NUMBER	Empty	Home number is used to specify that LDAP attribute that will be mapped to the handset home number
MOBILE NUMBER	Empty	Mobile number is used to specify that LDAP attribute that will be mapped to the handset mobile number

5.11.4 Characters supported

The below table shows which characters are supported in the communication between mi-MCT8663 and handset.

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0			0	@	P	`	p	€	i	°	À	Ð	à	ð		
1		!	1	A	Q	a	q	ı	'	ı	±	Á	Ñ	á	ñ	
2		"	2	B	R	b	r	,	'	¢	Č	Ā	Ò	â	ò	
3		#	3	C	S	c	s	f	"	£	č	Ā	Ó	ă	ó	
4		\$	4	D	T	d	t	„	"	¤	’	Ā	Ô	ã	ô	
5		%	5	E	U	e	u	...	•	¥	µ	Ā	Õ	ä	õ	
6		&	6	F	V	f	v	†	-	ı	¶	Æ	Ö	æ	ö	
7		'	7	G	W	g	w	‡	—	§	·	Ç	×	ç	÷	
8		(8	H	X	h	x	^	~	¨	˘	È	Ø	è	ø	
9)	9	I	Y	i	y	Ř	ř	Ů	Đ	É	Ù	é	ù	
A		*	:	J	Z	j	z	Š	š	Ú	đ	Ê	Ú	ê	ú	
B		+	;	K	[k	{	<	>	«	»	Ë	Û	ë	û	
C		,	<	L	\	l		Œ	œ	Ě	ř	İ	Ü	i	ü	
D		-	=	M]	m	}	Š	š	ě	ř	Í	Ý	í	ý	
E		.	>	N	^	n	~	Ž	ž	Ň	ň	İ	ß	ı	ß	
F		/	?	O	_	o	Ğ	ğ	Ÿ	ı	ı	İ	ß	ı	ÿ	

5.11.5 XML Server

Select “XML Server” server from the drop-down menu and fill in the empty fields. All types of directories are supported. Please note that only directories that are enabled are shown on the handset. If one directory is enabled, then the handset will only enter the chosen directory. If multiple directories are enabled, the option “All Search” is shown.

PARAMETER	DEFAULT VALUES	DESCRIPTION
CENTRAL DIRECTORY LOCATION	XML Server	Drop down menu to select between local central directory, LDAP based central directory and XML server. XML Server configuration is displayed when the “XML server” parameter is chosen.
SERVER	Empty	IP address of the LDAP server. Valid Inputs: AAA.BBB.CCC.DDD or <URL>
ENTERPRISE	Enabled	Type of tag for the group/directory
ENTERPRISE COMMON	Enabled	Type of tag for the group/directory
GROUP	Enabled	Type of tag for the group/directory
GROUP COMMON	Enabled	Type of tag for the group/directory
PERSONAL	Disabled	Type of tag for the group/directory

5.12 Multi-cell Parameter Definitions

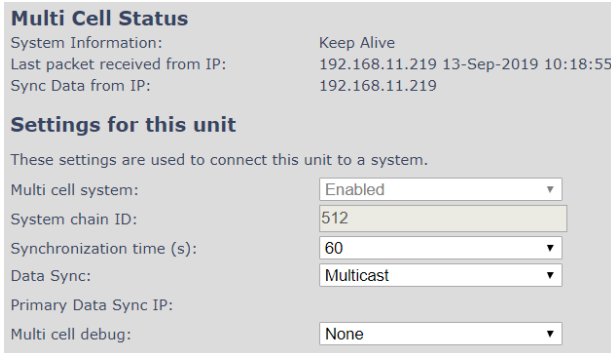
NOTE: To join 2 or more Base stations in a Multi Cell system, you need to have one handset added to the system. For further details and Step-by-Step guide to a Multi Cell setup, please see *6 Appendix How-To setup a Multi cell System*.

In this section, we describe the different parameters available in the Multi-cell configurations menu.

5.12.1 Settings for this unit

Description of Settings for specific base units is as follows:

Screenshot



Multicell status covers status of data synchronization. The status “Keep-alive” means normal operation.

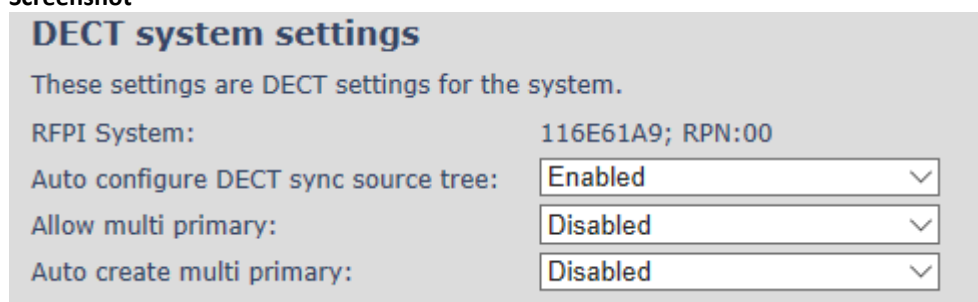
PARAMETER	DEFAULT VALUES	DESCRIPTION
MULTI CELL SYSTEM	Disabled	Enable this option to allow the Base unit to be set in multi-cell mode Valid Inputs: Enable, Disable Must Save and Reboot after change from disabled to enable.
SYSTEM CHAIN ID	Empty	This is an identifier (in string format e.g. 2275) that is unique for a specific multi-cell system. The Chain ID value MUST NOT be equal to a used SIP account. NOTE: Chain ID is used as SIP account for check Sync. Default value is 512, which means extension 512 must not be used – unless the chain ID is modified. When there is a Multi-cell system up and running, the Chain ID can be modified by provisioning only. Note: There can be several multi-cell systems in SME network. Up to 24 levels of Base stations chains are permitted in a setup. Valid Input: The Web site allow max 5 digits in this field.
SYNCHRONIZATION TIME (S)	60 sec	This specifies the period in seconds when elements/nodes (e.g. Base units) in a specific Multi-cell will synchronize to each other. If no keep-alive packets are received within a period of $2 * NETWORK_SYNC_TIME$, the base will be indicated as lost in the multi cell configuration. The parameter is also used with “Auto create multi primary” feature from the next section DECT system settings .
DATA SYNC:	Multicast	Select between “Multicast” or “Peer to Peer” data synchronization mode. The multicast port range and IP addresses used is calculated from the chain id. NOTE: Please note that if there are over 150 base stations in a multicell, the “Multicast” data sync should be used The multicast feature uses the port range: 49200 – 49999 The multicast feature IP range: 224.1.0.0 – 225.1.0.0 Multicast uses UDP. For multi-cast operation make sure that Multicast/IGMP is enabled on your switch(es), else use Peer-to-peer mode.
PRIMARY DATA SYNC IP	Empty	IP of Base station data sync source – the base handling the data synchronization. Using multicast this base IP is selected automatically.

		<p>The data sync feature uses the port range: 49200 – 49999</p> <p>NOTE: When using Peer to Peer mode the IP of the base used for data sync. source MUST be defined.</p> <p>NOTE: Using Peer to Peer mode with version below V306 limits the system’s automatic recovery feature – as there is no automatic recovery of the data sync. source in Peer to Peer mode.</p>
MULTI CELL DEBUG	None	<p>Enable this feature, if you want the system to catalogue low level multi-cell debug information or traces.</p> <p>Options:</p> <p>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.</p> <p>Auto Tree: Writes states and data related to the Auto Tree Configuration feature.</p> <p>Both: Both Data Sync and Auto Tree are enabled.</p> <p>NOTE: Must only be used for debug purpose and not enabled on a normal running system</p>

5.12.2 DECT System Settings

Description of DECT Settings for Specific Base units is as follows:

Screenshot



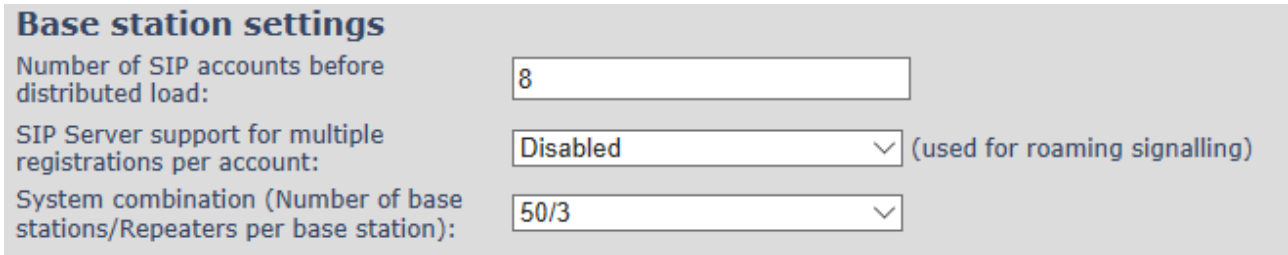
PARAMETER	DEFAULT VALUES	DESCRIPTION
DECT SYSTEM RFPI	May vary	This is a radio network identity accessed by all Base units in a specific multi-cell system. It is composed of 5 octets and has 5 different variables combined. RFPI Format: XX XX XX XX XX (where XX are HEX values)
AUTO CONFIGURE DECT SYNC SOURCE TREE	Enabled	Enable this to allow the system to automatically synchronize the multi-cell chain/tree. NOTE: Must be enabled in order to allow a new primary to recover in case the original primary goes into faulty mode.
ALLOW MULTI PRIMARY	Disabled	This feature is used for multi-location setups. Allows two or more primary in the same system. The two cells will be unsynchronized, and handover will not be possible. “Auto Configure DECT sync source tree” must be enabled for this feature to also be enabled
AUTO CREATE MULTI PRIMARY:	Disabled	When enabled, the system will generate cells in case a base goes into faulty mode. Two cells will only be generated in case no radio connection between the two cells is present. In order to recover the full system after establishing of the faulty base, the system must be rebooted. “Allow multi primary” must also be enabled for this feature to work.

NOTE: To run a system with two separate primaries in two locations “Allow multi primary” and “Auto configure DECT sync source tree” must be enabled. To add the second primary, the slave must manually be configured as primary. Alternatively, the “Auto create multi primary” must be enabled.

5.12.3 Base station settings

Description of SIP Settings for specific Base units is as follows:

Screenshot



PARAMETER	DEFAULT VALUES	DESCRIPTION
NUMBER OF SIP ACCOUNTS BEFORE DISTRIBUTED LOAD	8	The maximum number of handsets or SIP end nodes, that are permitted to perform location registration on a specific Base unit, before load is distributed to other base units. The parameter can be used to optimize the handset distribution among visible Base stations. Note: A maximum of 8 simultaneous calls can be routed through each Base unit in a multi-cell setup. Permitted Input: Positive Integers (e.g. 6)
SIP SERVER SUPPORT FOR MULTIPLE REGISTRATIONS PER ACCOUNT	Disabled	Disable this option so it is possible to use the same extension (i.e. SIP Account) on multiple phones (SIP end nodes). These phones will ring simultaneously for all incoming calls. When a phone (from a SIP account group) initiates a handover from Base X to Base Y, this phone will de-register from Base X, and register to Base Y after a call. Permitted Input: Disabled: No SIP de-registration will be made when a handset roams to another Base station Enabled: The old SIP registration will be deleted with a SIP Deregistration, when a handset roams to another base station
SYSTEM COMBINATION (NUMBER OF BASE STATIONS/REPEATERS PER BASE STATION):	50/3	Select between basic base configurations. 50/3 : 50 bases and 3 repeaters 127/1 : 127 bases and 1 repeater 254/0 : 254 bases and 0 repeater The configuration cannot be modified after a system is established. The configuration must be set during first multicell configuration.

5.12.4 Base station Group

The Base station group list various parameter settings for Base stations including chain level information.

Screenshot:

Base Station Group									
ID	RPN	Version	MAC-Address	IP-Address	IP Status	DECT sync source	DECT property	Base Station Name	
<input type="checkbox"/>	0	00	280	00087B0A00B3	192.168.11.159	This Unit	Select as primary	Primary	1
<input type="checkbox"/>	1	04	280	00087B09FECA	192.168.11.116	Connected	Primary:RPN00 (-24dBm)	Locked	2
<input type="checkbox"/>	2	08	280	00087B09FE45	192.168.11.113	Connected	Level 1:RPN04 (-24dBm)	Locked	3
<input type="checkbox"/>	3	0C	280	00087B09FF08	192.168.11.109	Connected	Level 2:RPN08 (-24dBm)	Locked	4
<input type="checkbox"/>	4	10	280	00087B09FE4A	192.168.11.166	Connected	Level 3:RPN0C (-24dBm)	Locked	5
<input type="checkbox"/>	5	14	280	00087B079205	192.168.11.133	Connected	Level 4:RPN10 (-24dBm)	Locked	6

Check All / Uncheck All
With selected: [Remove from chain](#)

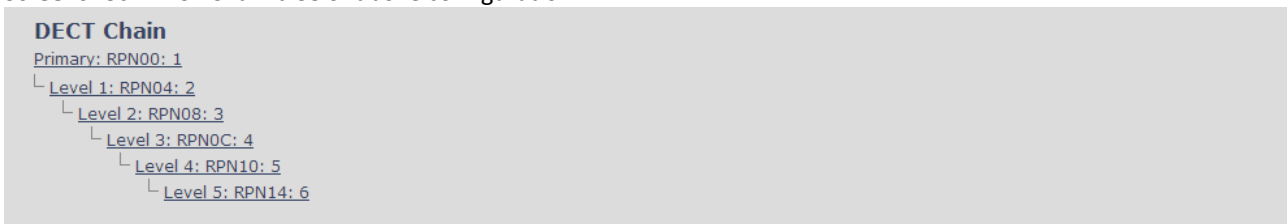
PARAMETERS	DESCRIPTION
ID	Base unit identity in the chained network. Permitted Output: Positive Integers
RPN	The Radio Fixed Part Number is an 8-bit DECT cell identity allocated by the installer. The allocated RPN within the SME must be geographically unique. Permitted Output: 0 to 255 (DEC) OR 0x00 to 0xFF (HEX)
VERSION	Base station's current firmware version. Permitted Output: positive Integers with dot (e.g. 480.1)
MAC ADDRESS	Contains the hardware Ethernet MAC address of the Base station. It varies from Base station to Base station.
IP ADDRESS	Base station's current IP address
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
DECT SYNC SOURCE	With setting "Auto configure DECT sync source tree" set to "Enable", this tree will automatically be generated. If manually configured, the administrator should choose the relevant "multi cell chain" level he wants and organize the Base units. Maximum number of "multi-cell chain" levels is 24. Format of the selection: "AAAAxx: RPNyy (-zz dBm)" AAAAA: indication of sync. source for the base. Can be "Primary" or "Level xx" xx: Sync. source base sync. level yy: Sync. source base RPN zz: RSSI level of sync. source base seen from the actual base "(Any) RPN": When a base is not synchronized to another base. State after reboot of chain.
DECT PROPERTY	Base station characteristics in connection to the current multi cell network. Possible Output(s) Primary: Main Base station to which all other nodes in the chain synchronizes to. Locked: The Base unit is currently synchronized and locked to the master Base unit. Searching: Base unit in the process of locating to a Master/slave as specified in DECT sync source

	<p>Free Running: A locked Base unit that suddenly lost synchronization to the Master.</p> <p>Unknown: No current connection information from specific Base unit</p> <p>Assisted lock: Base has lost DECT sync. source and Ethernet is used for synchronization</p> <p>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.</p>
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.

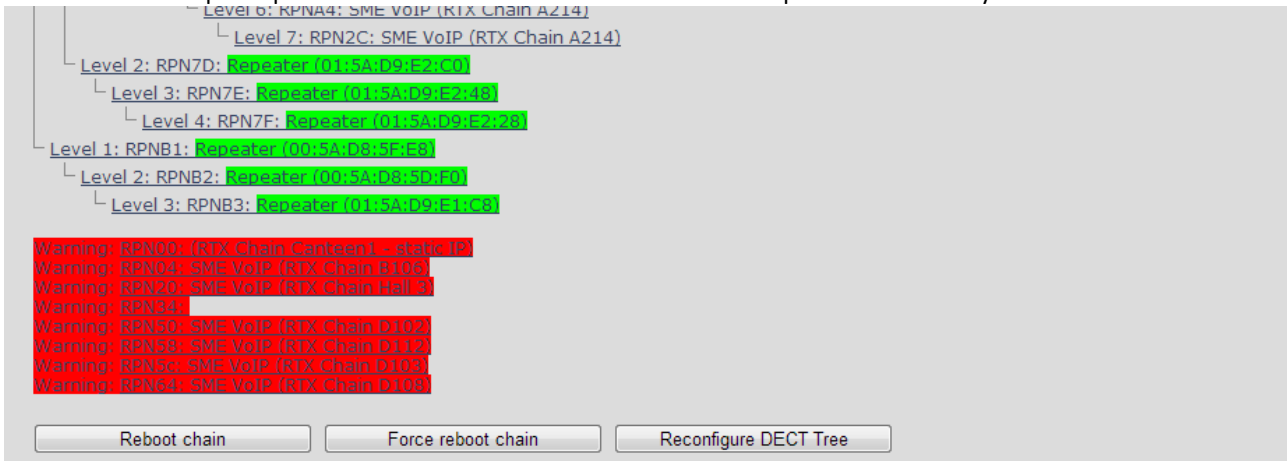
Screenshot: DECT Chain tree of above configuration



Screenshot: Example of part of DECT Chain tree with repeaters



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



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

5.12.6 mi-MCB0158 -mi-MCB8663 Mixed mode

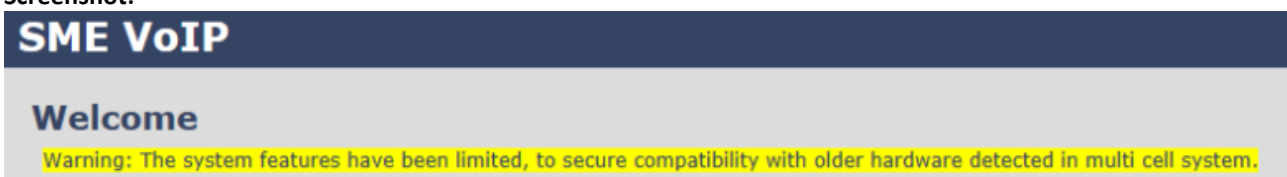
mi-MCB8663 Base station can be added to existing systems using mi-MCB0158 Base station. Even though the two base stations will be able to co-exist in the same Multi cell setup, the system will be set to some limitations. This means that the Multi cell will disable the features of mi-MCB8663, that are not supported by mi-MCB0158, and run on mixed mode but with limited to mi-MCB0158 features.

NOTE: LAN SYNC will not work in mixed mode.

NOTE: mi-MCB0158 cannot be added to an existing mi-MCB8663 Multi-cell. Only mi-MCB8663 can join an mi-MCB0158 system.

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

Screenshot:



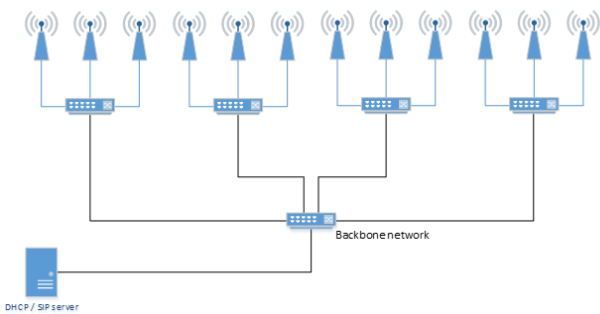
5.13 LAN SYNC

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.

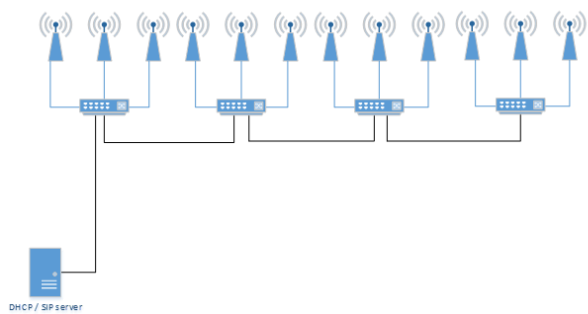
NOTE: To join 2 or more Base stations in a Multi Cell system you need to have one handset added to the system. For details and Step-by-Step guide to Multi Cell setup, please see Appendix.

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

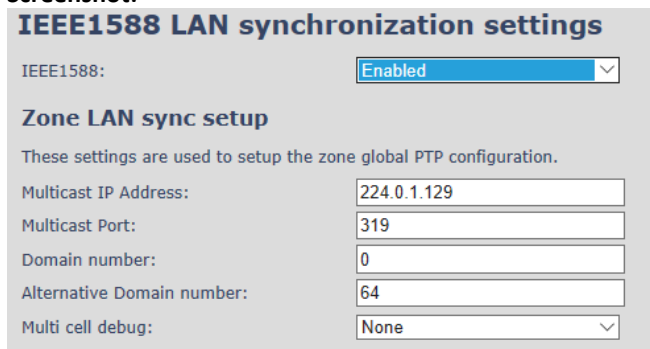
IEEE1588:

PARAMETERS	DEFAULT VALUES	DESCRIPTION
IEEE1588	Disabled	The initial part 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:



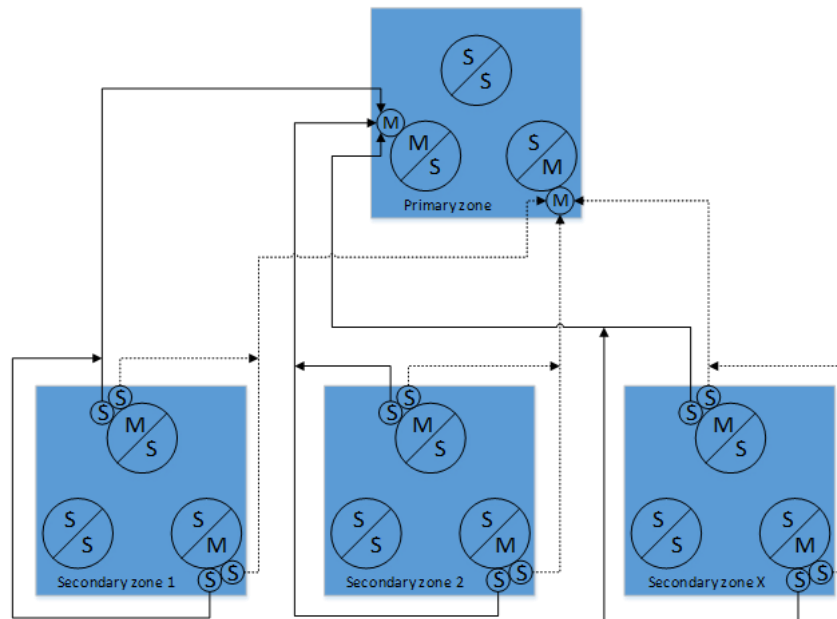
PARAMETERS	DEFAULT VALUES	DESCRIPTION
MULTICAST IP ADDRESS	224.0.1.129	This setting defines the IP address where to listen for IEEE1588 PTP packages IP address of the multicast group. The IP address must start with 224.0.xx.xx and this cannot be changed. To be compliant with IEEE1588, this port must 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:

ID	Status	Preferred 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-6
1	Locked	Automatic	Secondary	LAN:ID:0	LAN:ID:3	(190/193/215)	(10678/10692/10702)	Connected	ATI-13
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
PREFERRED 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 sampels used 25/32 of 31/35
Status	Offset -26 5/8/14 ns, Delay 10678/10699/10702 ns, Jitter 178/211/225 ns, Sync time 1 d 03:40:24
DECTtoIEEE1588	13532/6/0/0
Rejects by outlier	Average 6/0 %, Total 7/0 of 1127/1195
Messages	Sync and follow up received 1195/1195, Delay req send and received 1129/1127
Dect	Time diff 387 -825/0/974 ns
Frequency trim	Reg 0x320, Factory default 0x2d7, FrequencyTarget 0x321
Secondary instance, Inactive, PTP SLAVE	
Outlier	Filters ready 1/1, Init runtime 67 s, Init restarts 0, Ready count 1, Init sampels used 26/43 of 58/66
Status	Offset 103 -14/16/25 ns, Delay 10696/10719/10728 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 miALERT to debug IEEE1588 network issues.

In case debug is needed, send this information to miALERT 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

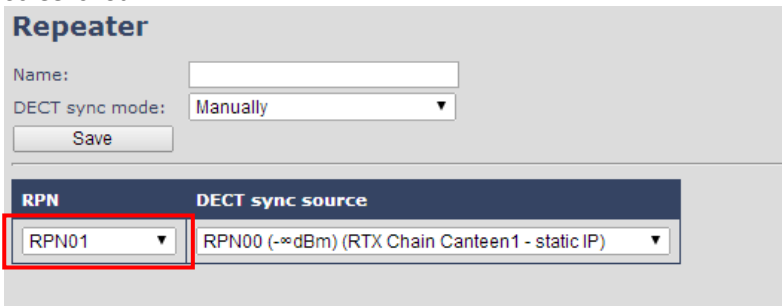


PARAMETERS	DESCRIPTION
NAME	Repeater name. If no name specified, the field will be empty
DECT SYNC MODE	<p>Manually: User controlled by manually assign “Repeater RPN” and “DECT sync source RPN”</p> <p>Local Automatic: Repeater controlled by auto detects best base signal and auto assign RPN.</p>

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



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
<input type="checkbox"/>	<u>1</u>	RPN01	RPN1/ FFFFFFFF		Manually	Enabled		

[Check All](#) / [Uncheck All](#)

With selected: [Delete Repeater\(s\)](#), [Register Repeater\(s\)](#) [Deregister Repeater\(s\)](#)

Good practice when adding repeaters to a Dual Cell system is to use manually registration, because then you can control what base station the repeater(s) connects to. In this way, the repeater will also have a static RPN whereas if the repeater is set to automatic, the RPN may vary from one registration to another. This is dependent on the repeater which will register to the base first, after for example a base reboot. If at least 1 repeater is set to manually, it is therefore strongly recommended to have all repeaters in the setup configured to manually, in order to make sure that the repeaters connect to the desired RPN.

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:

DECT sync mode:

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
<input type="checkbox"/>	<u>2</u>		RPN2/ FFFFFFFF		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
<input type="checkbox"/>	<u>1</u>	RPN02	RPN1/ 015AD85E80	RPN00 (-26dBm)	Local Automatical	Present@RPN00	41.1	Off
<input type="checkbox"/>	<u>2</u>	RPN01	RPN2/ 005AD85D90	RPN00 (-26dBm)	Local Automatical	Present@RPN00	41.1	Off
<input type="checkbox"/>	<u>3</u>	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”

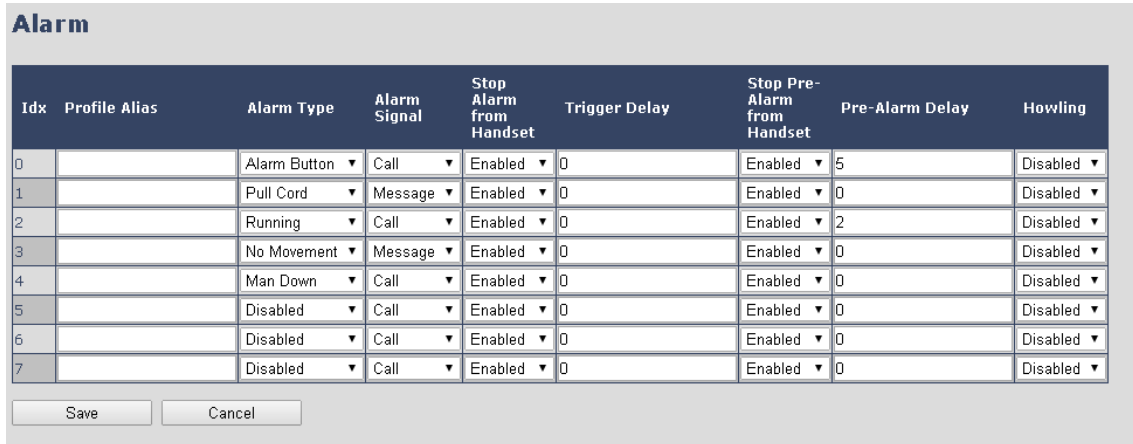
	<p>Local Automatical: Repeater controlled by auto detects best base signal and auto assign RPN.</p> <p>Chaining Automatical: Base controlled by auto detects best base or repeater signal and auto assign RPN. This feature will be supported in a future version</p>
STATE	Present@unit means connected to unit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

For detailed description on how to operate repeaters please ask miALERT 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



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 *Edit 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	<p>The type of alarm is dependent of what kind of event that has triggered the alarm on the handset.</p> <p>The type of alarms supported is handset related.</p> <p>mi-MCT8633:</p>

	Alarm button mi-MCT385: Alarm button Man Down No Movement Running Pull Cord Emergency Button Disabled
ALARM SIGNAL	The way the alarm is signaled when received on the handset. Message: A text message to an alarm server. Note: If a handset supports Bluetooth and Receiver mode is enabled, the beacon data will be included in the message. For more details, please go to <i>5.3.3 Edit Handset</i> 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. mi-MCT8633 and mi-MCT385) 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 have 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

The screenshot shows the 'Statistics' page with 'Export' and 'Clear' buttons. Below the buttons are navigation links: **System** / Calls / Repeater / DECT / Call quality. The main table displays the following data:

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 triggered, 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 stable 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

Statistics

Export Clear

[System](#) / [Calls](#) / [Repeater](#) / [DECT](#) / [Call quality](#)

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 COUNT	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.
DROPPED	Counts number of calls on a base. 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 ACTIVE	Call duration is total time that calls are active on the base. 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

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	Total operation time for the repeater since last reboot or reset

D-H:M:S	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

Statistics

Export

System / Calls / Repeater / DECT / Call quality

	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

Export

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	

PARAMETERS	DESCRIPTION																								
BASE STATION NAME	Base IP address and base station name from management settings																								
TYPE	Call Relay conn																								
CALL COUNT	Count the number of calls																								
LOCAL/REMOTE SIDE	Local: Remote:																								
JITTER[MS]	Measures how the RTP packets are received, the lower the Jitter is the better																								
ROUND TRIP LATENCY [MS]	Measures the time it takes for RTP packets to reach it destination.																								
PACKET LOSS [%]	Percentages of packets lost.																								
R-VALUE	A way to measure call quality, from 0-120 <table border="1" style="margin-left: 20px;"> <thead> <tr> <th>USER SATISFACTION LEVEL</th> <th>MOS</th> <th>R-Factor</th> </tr> </thead> <tbody> <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> </tbody> </table>	USER SATISFACTION LEVEL	MOS	R-Factor	MAXIMUM USING G.711	4.4	93	VERY SATISFIED	4.3-5.0	90-100	SATISFIED	4.0-4.3	80-90	SOME USERS SATISFIED	3.6-4.0	70-80	MANY USERS DISSATISFIED	3.1-3.6	60-70	NEARLY ALL USERS DISSATISFIED	2.6-3.1	50-60	NOT RECOMMENDED	1.0-2.6	Less than 50
USER SATISFACTION LEVEL	MOS	R-Factor																							
MAXIMUM USING G.711	4.4	93																							
VERY SATISFIED	4.3-5.0	90-100																							
SATISFIED	4.0-4.3	80-90																							
SOME USERS SATISFIED	3.6-4.0	70-80																							
MANY USERS DISSATISFIED	3.1-3.6	60-70																							
NEARLY ALL USERS DISSATISFIED	2.6-3.1	50-60																							
NOT RECOMMENDED	1.0-2.6	Less than 50																							
MOS-VALUE	MOS 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.																								

5.17 Generic Statistics

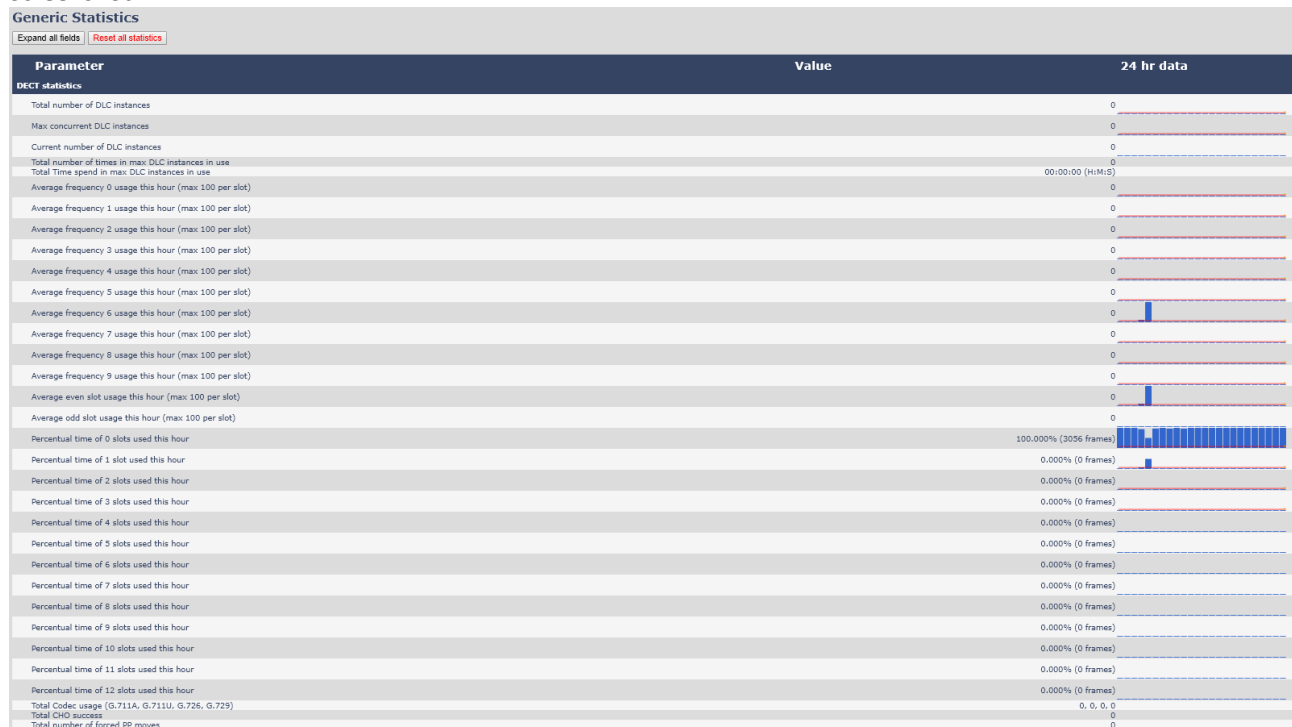
The statistic feature is divided into five sections, which can be access from any base.

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:



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 synchronisation chain changes	2
Total time in sync state: Master	2 days 01:23:05 (H:M:S)
Total time in sync state: Locked	00:00:00 (H:M:S)
Total time in sync state: Free Running	00:00:00 (H:M:S)
Total time in sync state: Locked Assisted	00:00:00 (H:M:S)
Total time in sync state: Sync Lost	00:00:00 (H:M:S)
Total time in sync state: Searching	00:00:40 (H:M:S)
Total time in sync state: Unknown	00:00:38 (H:M:S)
Last reported sync information from this base	20/Mar/2019 08:08:08

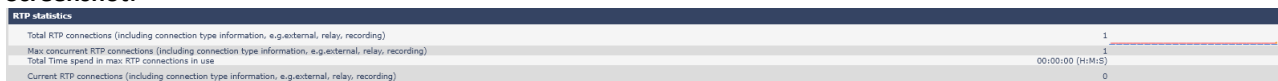
PARAMETERS	DESCRIPTION
CURRENT SYNCHRONISATION STATE	The current DECT sync state (e.g. Master, Searching, Free Running, etc).
CURRENT SYNCHRONISATION CHAIN	The current DECT sync source Fp Id of this base.
TIMESTAMP FOR LAST CHANGED SYNCHRONISATION CHAIN	Timestamp of the last time this base changed DECT 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:



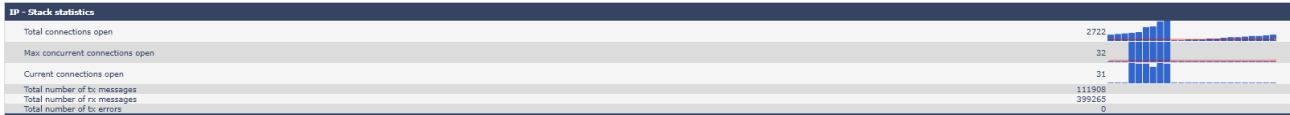
PARAMETERS	DESCRIPTION
TOTAL RTP CONNECTIONS (INCLUDING CONNECTION TYPE INFORMATION, E.G. EXTERNAL, RELAY, RECORDING)	The life time total count of instantiated RTP streams.
MAX CONCURRENT RTP CONNECTIONS (INCLUDING CONNECTION TYPE INFORMATION, E.G. EXTERNAL, RELAY, RECORDING)	The life time highest concurrent 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:

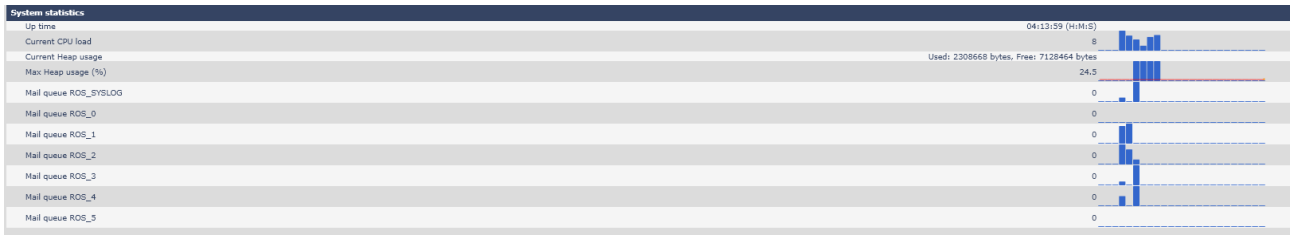


PARAMETERS	DESCRIPTION
TOTAL CONNECTIONS OPEN	The life time total count of used sockets.
MAX CONCURRENT CONNECTIONS OPEN	The life time highest concurrent count of used sockets.
CURRENT CONNECTIONS OPEN	The current count of used sockets.
TOTAL NUMBER OF TX MESSAGES	The life time total count of transmitted 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:



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):
- Trace received Ethertype
- Trace received IPv4 protocol
- Trace received TCP/UDP port

	to		to		to		to		to	

Info

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

Save
Cancel
Reset traces

Download traces from: All Basestations Current Basestation

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 miALERT 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 miALERT 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.zrfff66.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 mi-MCB0158 and mi-MCB8663 in the same chain, but the features of the system will be reduced to mi-MCB0158. This means that if a user has a multi cell system with 50x mi-MCB0158 and adds 1x mi-MCB8663, the system will run on the mi-MCB0158 features and exclude the extra ones from mi-MCB8663.

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



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:

State / Region:

Notes:

Select Language:

Time Server:

Allow broadcast NTP:

Refresh time (h):

Set timezone by country/region:

Timezone:

Set DST by country/region:

Daylight Saving Time (DST):

DST Fixed By Day:

DST Start Month:

DST Start Date:

DST Start Time:

DST Start Day of Week:

DST Start Day of Week Last in Month:

DST Stop Month:

DST Stop Date:

DST Stop Time:

DST Stop Day of Week:

DST Stop Day of Week 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.
- 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
 - Next, from the Server page, click on the **Add Server** URL and enter the relevant SIP server information (an example is shown below).
 - 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

Servers

Test:
192.168.11.99

[Add Server](#)

[Remove Server](#)

Test:

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

6.1.3 Add an extension

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

Screenshot

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

Screenshot

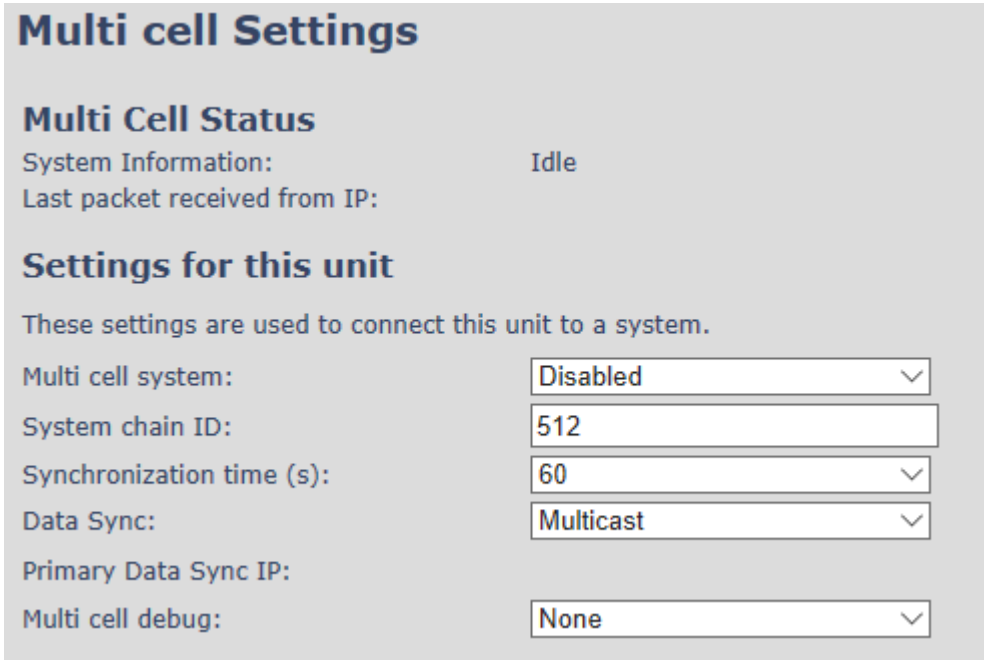
Idx	IPFI	Handset State	Handset Type FW Info	FWU Progress	VoIP Idx	Extension	Display Name	Server	Server Alias	State
<input type="checkbox"/>	4	EEEEEEEEEE			<input type="checkbox"/>	4	521	521	192.168.11.99	Test

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)

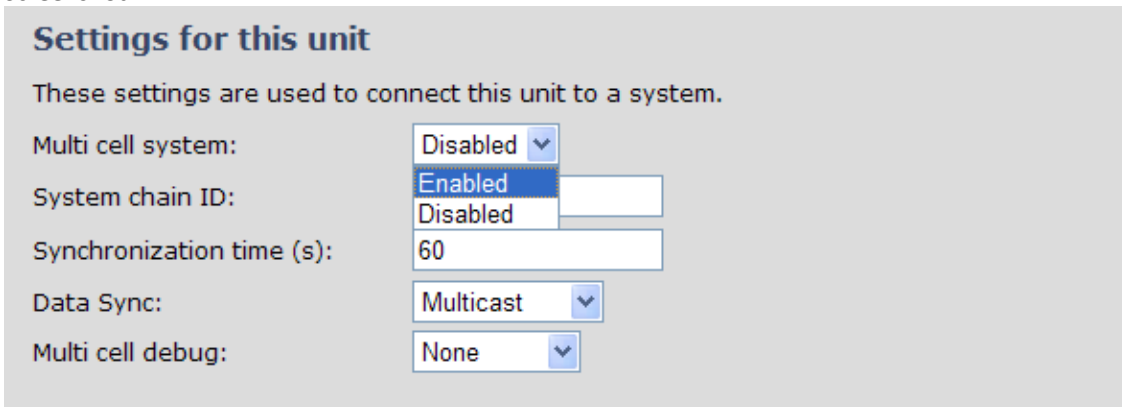
STEP 8 Click on **Multi Cell** URL link from the left-handed menu to view the current Multi cell settings status of the current Base station. Brand new Base stations have **Multi cell system** feature disabled by default

Screenshot



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.

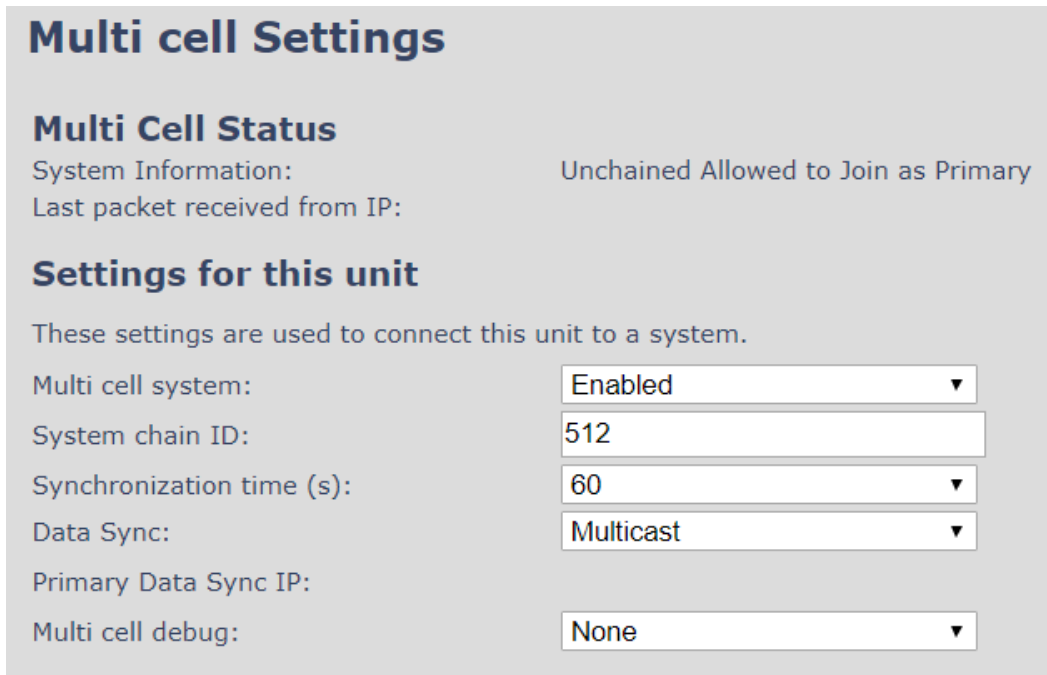
Screenshot



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 ▼

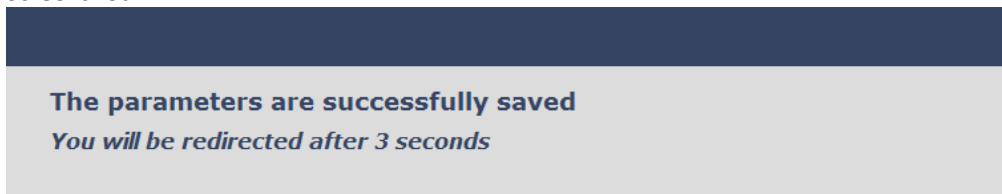
Data Sync: Multicast ▼

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



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

Save and Reboot Save Cancel

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
<input type="checkbox"/>	0	00	911.1858 00087B174649	192.168.11.186	This Unit	Primary:RPN04 (-24dBm)	Locked	SME VoIP
<input type="checkbox"/>	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

Reboot chain Force reboot chain Reconfigure DECT Tree

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

Push-To-Talk: Disabled

Extension: 510

Authentication User Name: 510

Authentication Password:

Display Name: 510

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

Save Cancel

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](#)

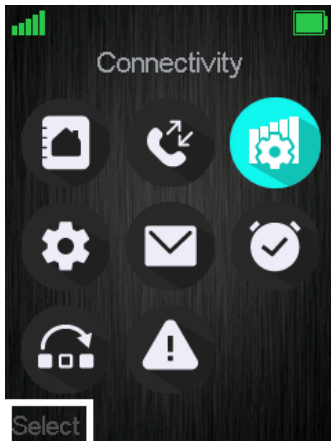
	Idx	IPEI	Handset State	Handset Type FW Info	FWU Progress		VoIP Idx	Extension	Display Name	Server	Server Alias	State
<input type="checkbox"/>	1	FFFFFFFF				<input type="checkbox"/>	1	510	510	192.168.11.99	HDJSERVER	

[Check All / Uncheck All](#) [Check All Extensions / Uncheck All Extensions](#)

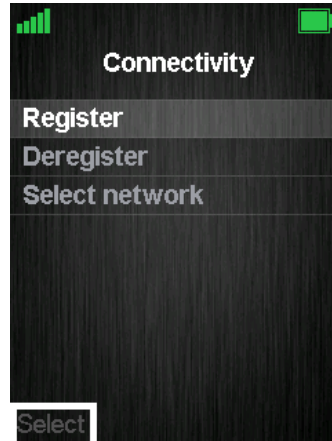
With selected: [Delete Handset\(s\)](#) **[Register Handset\(s\)](#)** [Deregister Handset\(s\)](#) [Start SIP Registration\(s\)](#) [SIP Delete Extension\(s\)](#)

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

a) Select main menu “Connectivity”



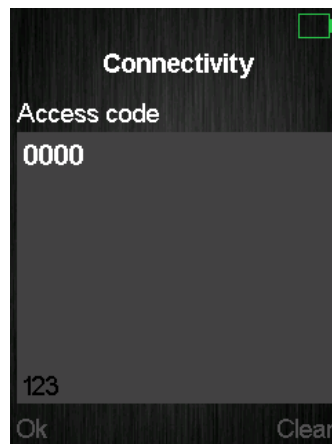
b) Select the menu “Register”



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:

[Add extension](#)
[Stop Registration](#)

	Idx	IPEI	Handset State	Handset Type FW Info	FWU Progress	VoIP Idx	Extension	Display Name	Server	Server Alias	State
<input type="checkbox"/>	1	02788888DB	Present@RPN04	8630 400.1	Off	<input type="checkbox"/> 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

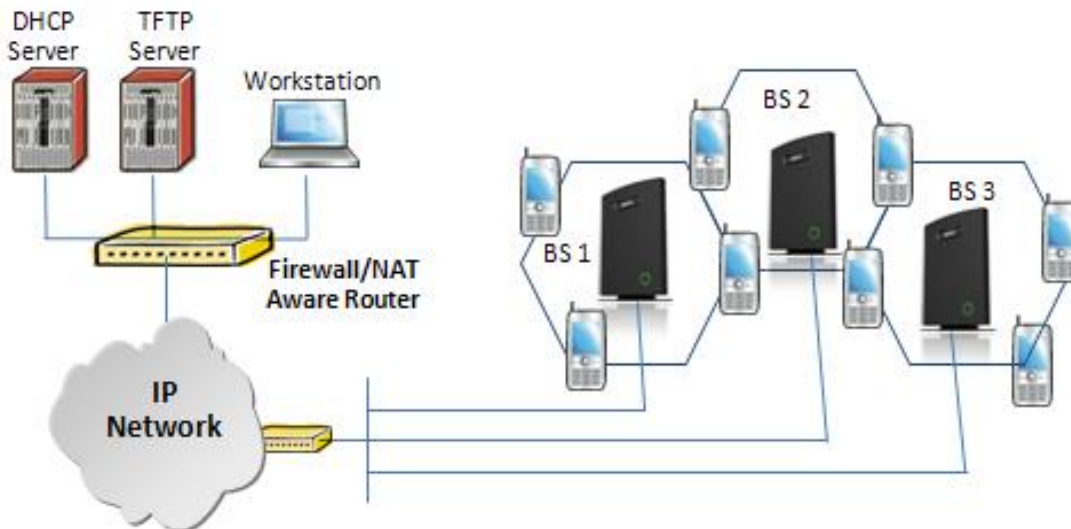
This step-by-step chapter describes how to upgrade or downgrade Base station(s) and/or handset(s) / repeater (s) to the relevant firmware provided by miALERT (NSI Distribution).

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.

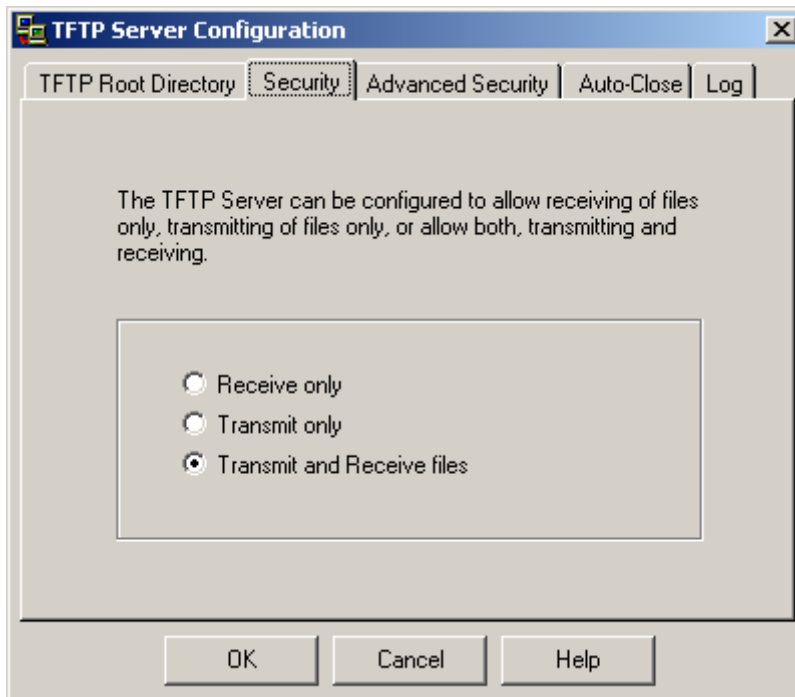
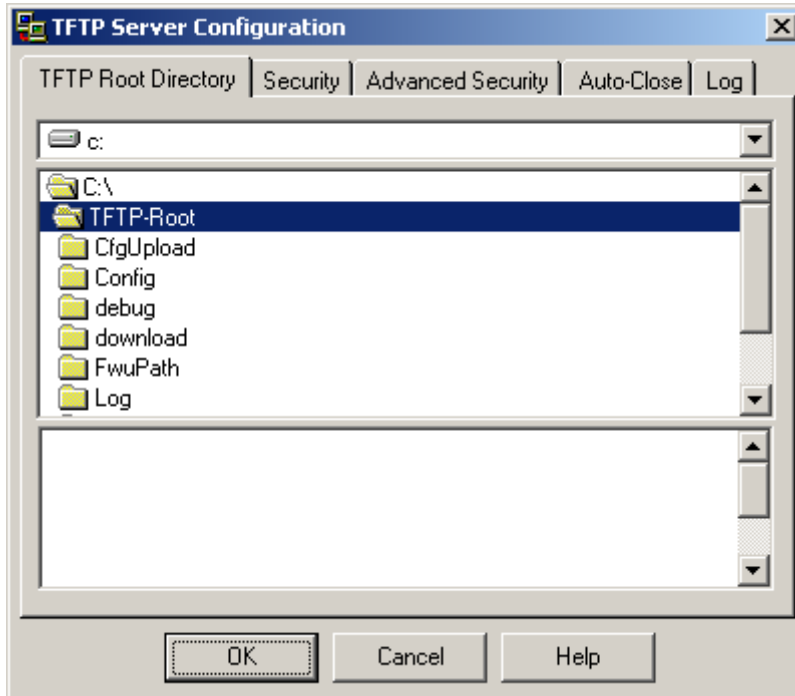
The minimum hardware and software components that are required to be able update via TFTP include the following (but not limited to):

- 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.



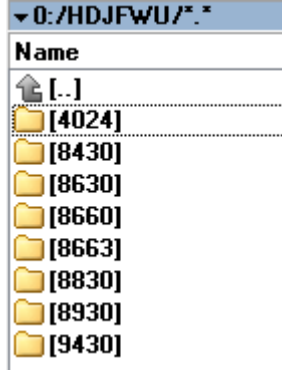
NOTE: If TFTP server timeout settings are too short firmware upgrade might not complete. Recommended time out setting is more than 3 seconds.

8.3 Create Firmware Directories

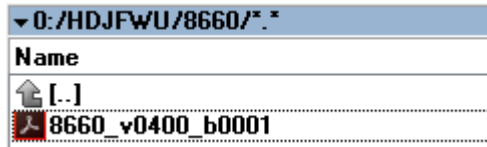
The admin from the service provider’s side must create the relevant firmware directory in the server where both old and new firmware(s) can be placed in it. (See the STEP above)

8.3.1 Base:

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



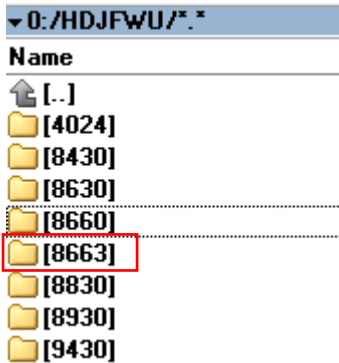
Copy Base station firmware to the named directory.



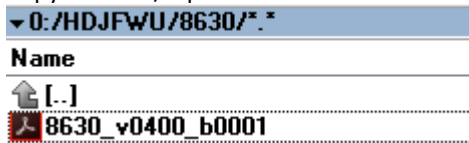
IMPORTANT: The **8663** directory name cannot be changed.

8.3.2 Handsets/Repeaters:

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



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



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:

Firmware path:

Terminal file path:

Type	Required version	Required branch	Startup picture	Background picture
Update Base Stations	<input type="text" value="0"/>	<input type="text" value="0"/>		
8630	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text"/>	<input type="text"/>
8830	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text"/>	<input type="text"/>
8430	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text"/>	<input type="text"/>

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:

Firmware path:

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:

Firmware path:

Terminal file path:

Type	Required version	Required branch	Startup picture	Background picture
Update Base Stations	<input type="text" value="480"/>	<input type="text" value="1"/>		
8631	<input type="text" value="480"/>	<input type="text" value="3"/>		
8430	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text"/>	<input type="text"/>

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

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		
<input type="checkbox"/>	1	0328D1990E	Present@RPN00	8631 480.2	Off	<input type="checkbox"/>	1	529	529	192.168.11.99	Test	SIP Registered@RPN00
<input checked="" type="checkbox"/>	2	027888187C	Present@RPN00	8430 440.4	1%	<input checked="" type="checkbox"/>	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

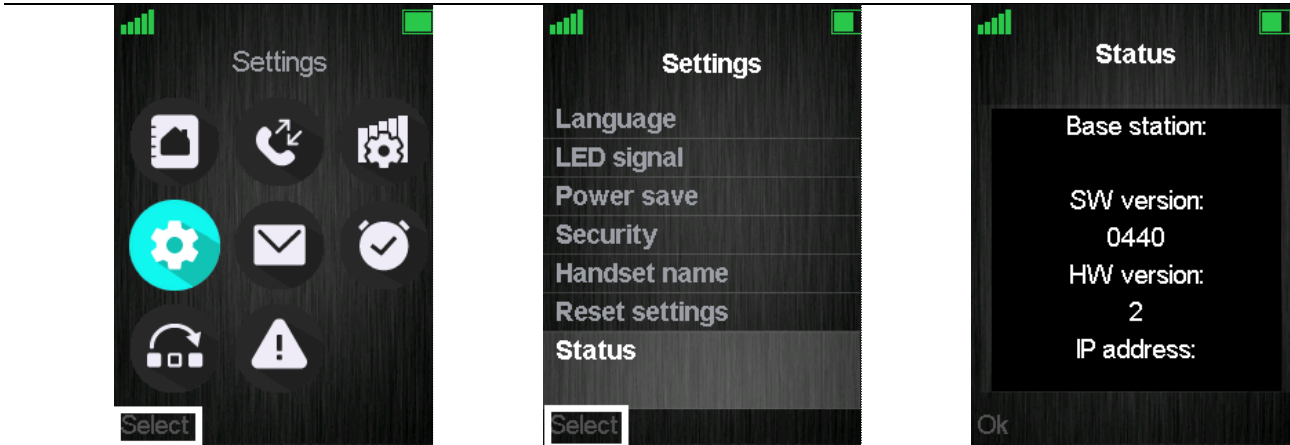
Repeater firmware upgrade status is monitored on the **Repeaters** page, under “FWU Progress”.

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.



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
<input type="checkbox"/>	0	00	400.1	00087B079207	192.168.11.106	This Unit	Select as primary	Primary	SME VoIP
<input type="checkbox"/>	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:

Firmware path:

Terminal file path:

Type	Required version	Required branch	Startup picture	Background picture
Update Base Stations	423	1904		
8631	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="DECT1.bmp"/>	<input type="text" value="DECT2.bmp"/>
8830	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text"/>	<input type="text"/>
8632	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="img123.bmp"/>	<input type="text"/>

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:

Add extension
Stop Registration

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

/ /

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).

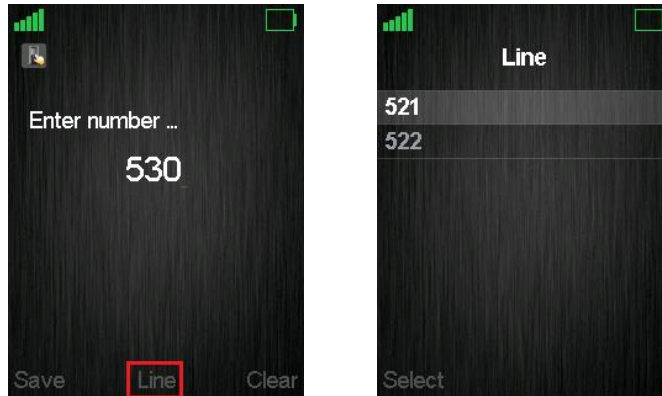
STEP 3 The extension will now show in the extension list with the same Idx and IPEI as the handset selected.

Note: The handset must be rebooted for the changes to take effect.

<input type="checkbox"/>	5	02788DD16D	Present@RPN04	8630 430.1	Off	<input type="checkbox"/>	5	6005	6005	192.168.11.99	HDJSERVER	SIP Registered@RPN04
<input type="checkbox"/>	5	02788DD16D	Present@RPN04	8630 430.1	Off	<input type="checkbox"/>	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.



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 handedover between Base-stations using connection handover procedures.
- **Security:** The Multicell SME VOIP system also supports robust security functionalities for Base-stations. Most security² 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:	<ul style="list-style-type: none"> • 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
MULTICELL SYSTEM GUIDE 5.3
Proprietary and Confidential

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
TLS_RSA_WITH_AES_128_GCM_SHA256
TLS_ECDHE_ECDSA_AES256_GCM_SHA256

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 webservice.

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	The Session Initiation Protocol UPDATE Method
RFC3325	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	
SRTT	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

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.

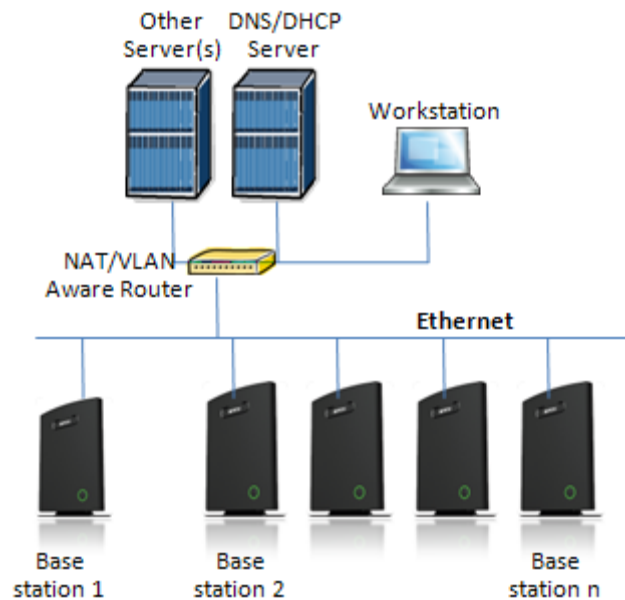
11.3.1.1 Hints on how to Configure DNS behind a Firewall/NAT

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.

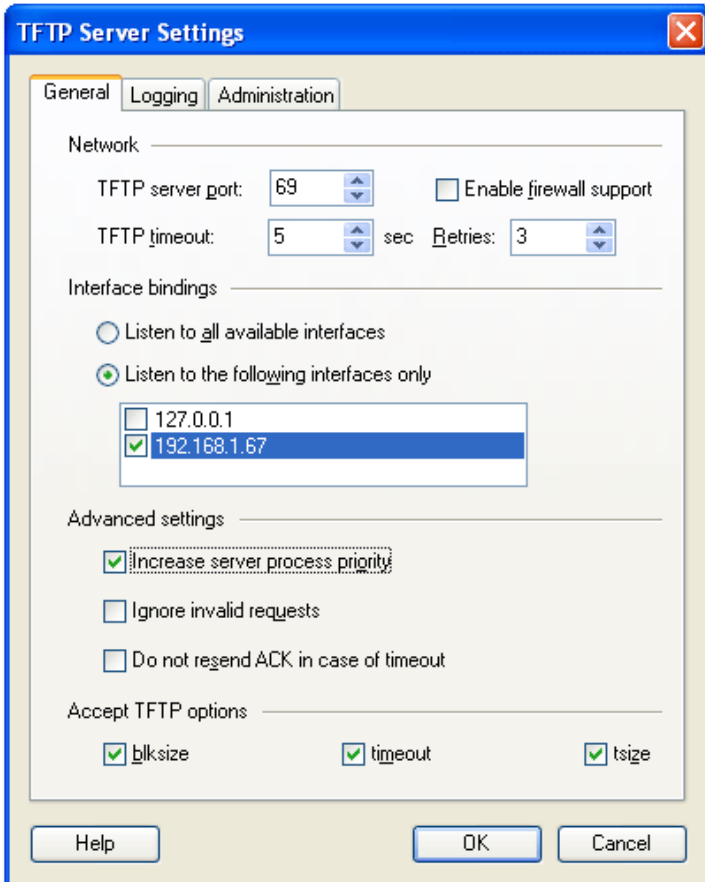
11.5.1 TFTP Server Settings

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).

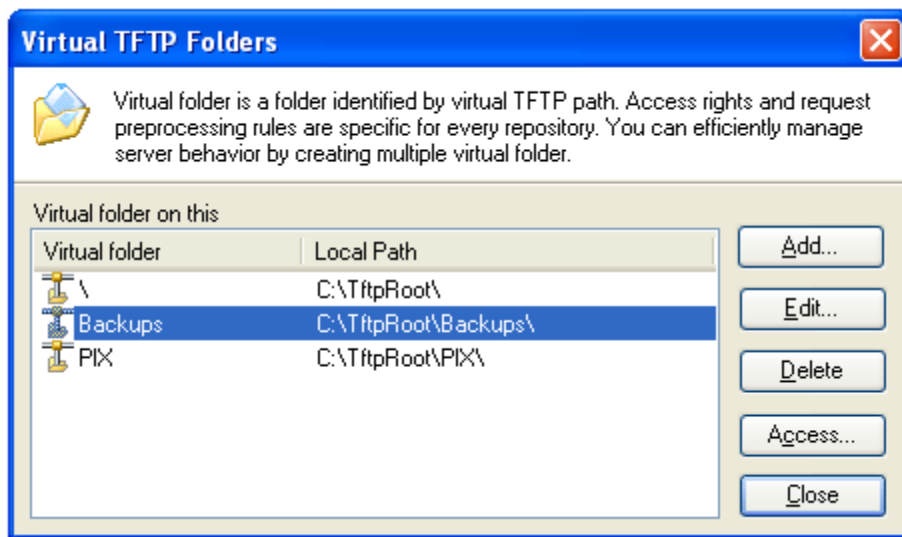
Specify the interface bindings, TFTP root directory, port which the TFTP Server will listen, timeout and number of retries, and TFTP options supported by the server.

Screenshot



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



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

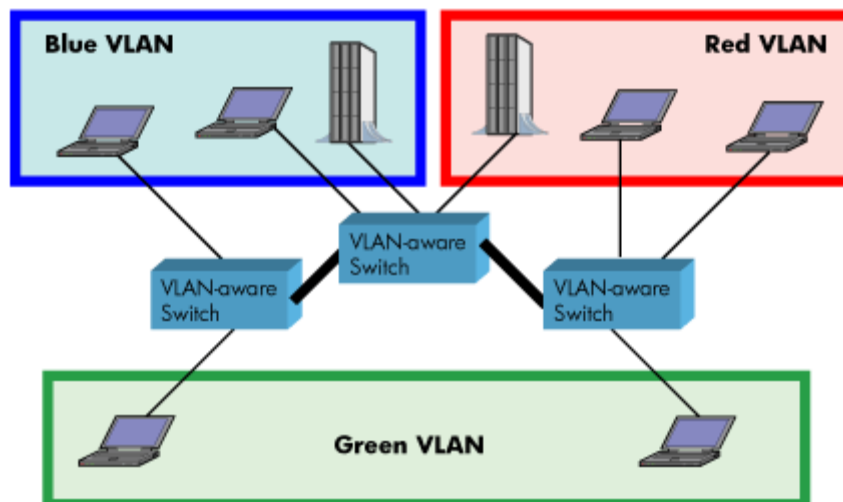
In this chapter, we describe how to setup VLAN to typical network. There are three main stages involved in this procedure:

- 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:

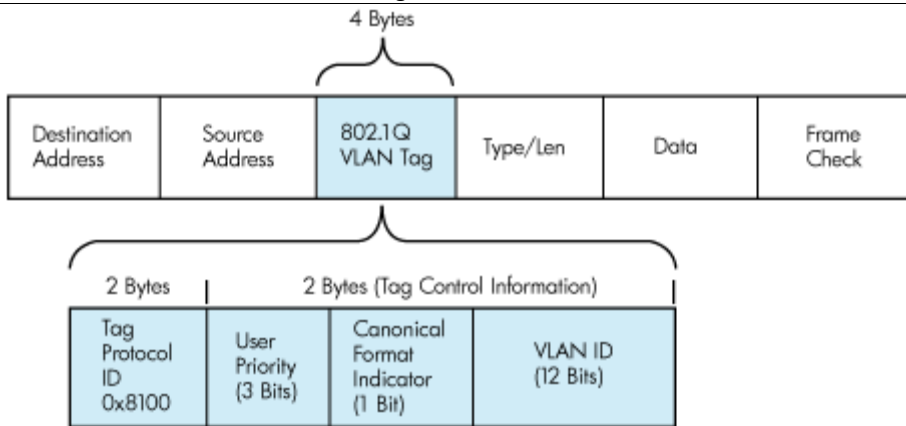
1. When the switch receives a broadcast or multicast frame from a port, it floods the frame to only those ports that belong to the same VLAN as the frame.
2. When a switch receives a unicast frame, it forwards it to the port to which it is addressed, only if the port belongs to the same VLAN as the frame.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

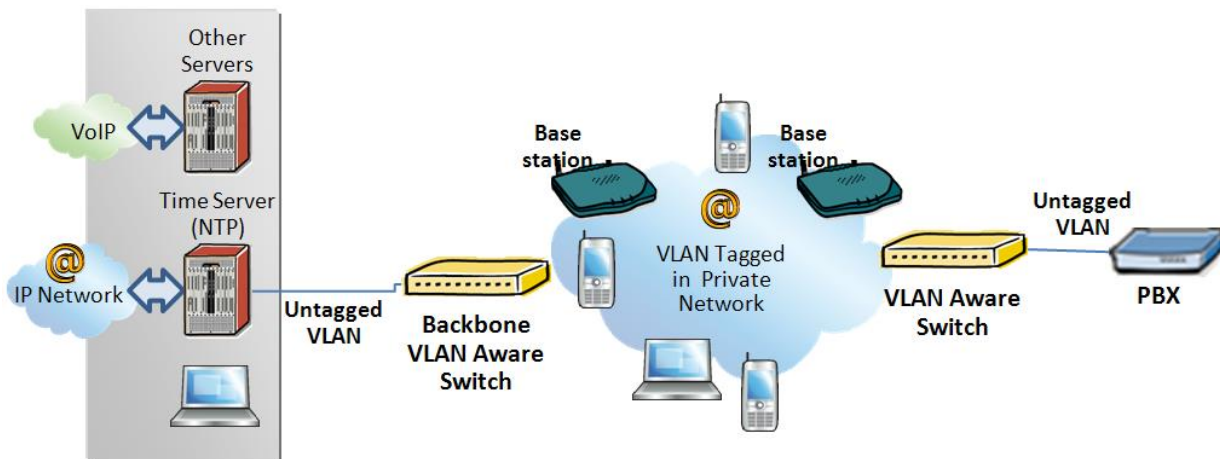
12.4 Implementation Cases

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 PC

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

Save and Reboot Save Cancel

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

The screenshot shows the 'SME VoIP' configuration interface. The 'Network Settings' page is active, with a sidebar on the left containing various menu items. The 'Network' menu item is highlighted. The main content area is divided into several sections: 'IP settings', 'NAT Settings', 'SIP/RTP Settings', 'DHCP Options', and 'VLAN Settings'. The 'VLAN Settings' section is highlighted with a red box and contains the following fields: ID (501) and User Priority (0). The 'DHCP Options' section shows 'Plug-n-Play' set to 'Enabled'. The 'NAT Settings' section includes 'Enable STUN' (Disabled), 'STUN Server', 'STUN Bindtime Determine' (Enabled), 'STUN Bindtime Guard' (80), 'Enable RPORT' (Disabled), and 'Keep alive time' (90). The 'SIP/RTP Settings' section includes '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), and 'RTP ToS/QoS' (0xB8). At the bottom, there are three buttons: 'Save and Reboot', 'Save', and 'Cancel'.

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

```

File Edit Format View Help
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

```
File Edit Format View Help
<IPPhoneDirectory>
<DirectoryEntry>
<Name>Mark Ross</Name>
<Telephone>100</Telephone>
<Office>+4 501234 56789</Office>
<Mobile>+4 511234 56789</Mobile>
<Fax>+4 521234 56789</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

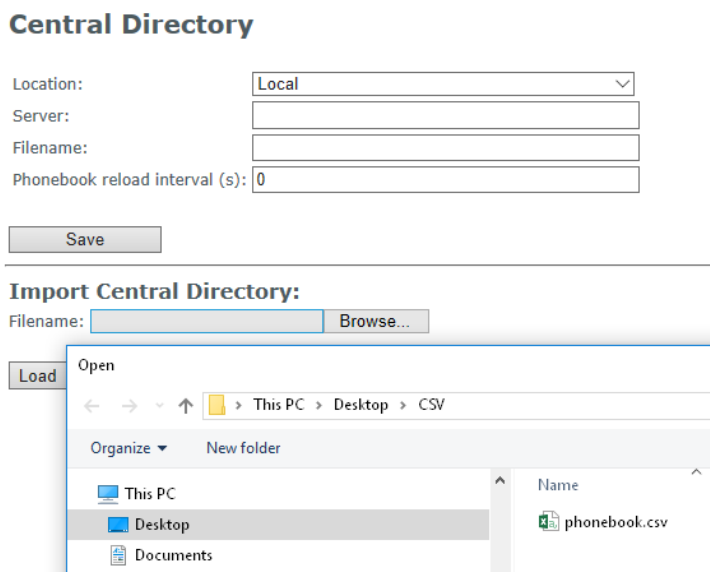
The Contact list is saved as file format: **.txt .csv or .xml**

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



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:

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:
 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:
 Server:
 Filename:
 Phonebook reload interval (s):

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 mi-MCB8663 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.

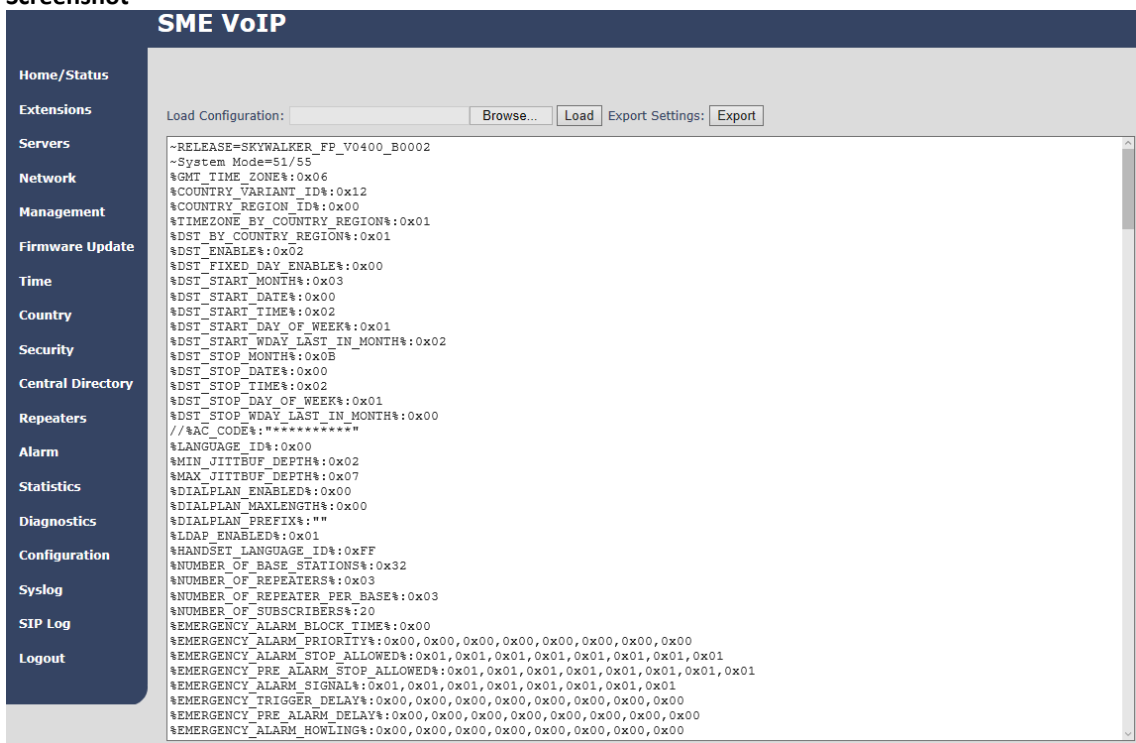
14.2 Manual Configuration by use of Web Server.

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



STEP 1 Chose configuration file

STEP 2 Press Load to load the file.

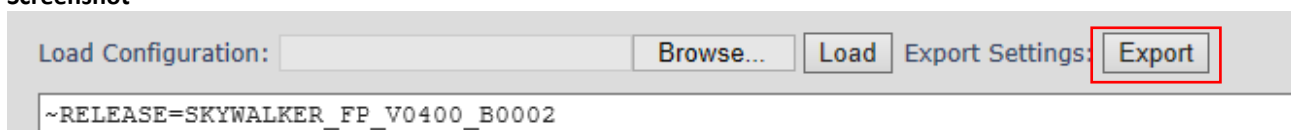
The base station will now load the file and the settings will be as in the configuration file.

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



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.

NOTE: If the base fails to download the configuration file, it will retry accessing the configuration server again after 1h.

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

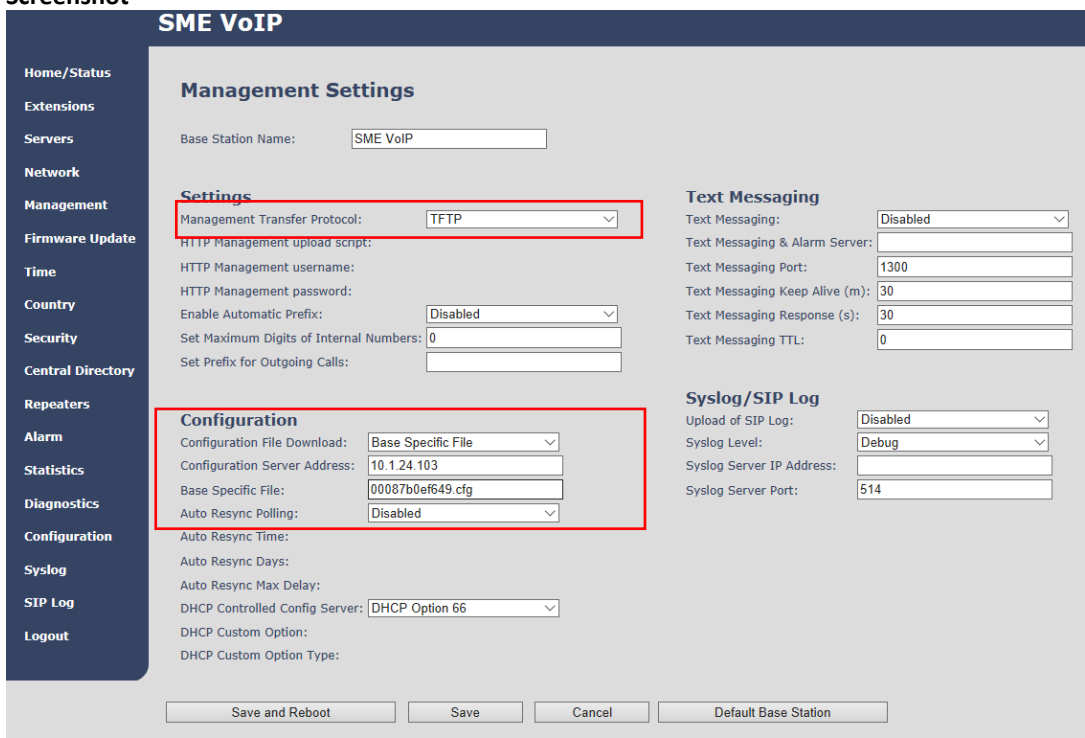
14.5.2 Configuration for web server:

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



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