

SME VoIP System Guide

*Installation & Configuration
Network Deployment
Operation & Management*

Technical Reference Document
Version 1.5
© Dec-2010 RTX Telecom A/S, Denmark

Trademarks

RTX and the combinations of its logo thereof are trademarks of RTX Telecom A/S, Denmark. Other product names used in this publication are for identification purposes and maybe the trademarks of their respective companies.

Disclaimer

The contents of this document are provided in connection with RTX products. RTX makes no representations with respect to completeness or accuracy of the contents of this publication and reserves the right to make changes to product descriptions, usage, etc., at any time without notice. No license, whether express, implied, to any intellectual property rights are granted by this publication

Confidentiality

This document should be regarded as confidential, unauthorized copying is not allowed

© Dec-2010 RTX Telecom A/S, Denmark, All rights reserved
<http://www.rtx.dk>

Contents

SME VoIP System Guide	1
Contents	3
1 About This Document.....	8
1.1 Audience	8
1.2 When Should I Read This Guide	8
1.3 Important Assumptions	8
1.4 What's Inside This Guide	8
1.5 What's Not in This guide.....	9
1.6 Abbreviations.....	10
1.7 References/Related Documentation	10
1.8 Document History.....	10
1.9 Documentation Feedback	10
2 Introduction – System Overview	11
2.1 Hardware Setup.....	11
2.2 Components of SME VoIP System	12
2.2.1 RTX Base Stations	12
2.2.2 SME VoIP Administration Server/Software	12
2.2.3 RTX Wireless Handset.....	13
2.3 Wireless Bands	13
2.4 System Capacity (in Summary)	13
2.5 Advantages of SME VoIP System	14
3 SME System Deployment Scenarios	15
3.1 Multi-cell System	15
3.2 Multi-cell Setup	15
3.3 Case Studies.....	16
3.3.1 Case ##1: Isolated Buildings	16
3.3.2 Case ##2: Location with co-located partners	17
3.3.3 Case ##3: Large to Medium Sized Enterprises	18
3.3.4 Case ##4: Large Enterprises at Different Locations.....	18
4 SME VoIP Network Planning/Optimization	20
4.1 Network Requirements	20
4.2 Deployment Considerations	20
4.3 Site Planning	20
4.3.1 Deployment kit	20
4.3.2 Location Probability	20
4.3.3 Handover Mechanics/Planning	21
4.4 Cell Coverage / Capacity Planning	21
4.4.1 Cell Coverage	21
4.4.2 Capacity Planning	22
4.5 Network Dimensioning.....	23
4.6 Environmental Considerations	23

4.7 Recommended Base station/Repeater Placement	24
4.8 Network Assessment/Optimisation	25
5 Deployment Mechanics – Multi-cell SME Network.....	26
6 Installation of Base Stations/Repeater.....	29
6.1 Package - Contents/Damage Inspection.....	29
6.2 RTX Base station Mechanics	30
6.3 RTX Base Unit - Reset feature.....	31
6.4 Installing the Base Station	31
7 Making Handset Ready.....	33
7.1 Package - Contents/Damage Inspection.....	33
7.2 Before Using the Phone.....	34
7.3 Using the Handset	35
8 Core Network Server(s) Configuration	36
8.1 Server setup.....	36
8.2 Requirements	36
8.3 DNS Server Installation/Setup	36
8.4 DHCP Server Setup	36
8.4.1 Hint: Getting DHCP Server to Work.....	37
8.5 TFTP Server Setup.....	38
8.5.1 TFTP Server Settings	38
8.6 SIP Server Setup.....	39
8.6.1 FreePBX SIP Server.....	39
9 SME VoIP Administration Interface.....	42
9.1 Home/Status.....	42
9.2 Extensions.....	43
9.3 Servers	45
9.4 Network	46
9.4.1 IP Settings	46
9.4.2 VLAN Settings	47
9.4.3 Boot Server Options	48
9.4.4 NAT Settings	49
9.4.5 SIP/RTP Settings.....	49
9.5 Management Settings Definitions	50
9.6 Firmware Update Definitions	51
9.7 Time Server.....	52
9.8 Multi-cell Parameter Definitions	53
9.8.1 Settings for Base Unit	53
9.8.2 DECT System Settings	54
9.8.3 SIP System Settings.....	55
9.8.4 MAC-units in Chain	55
9.9 Settings – Configuration File Setup	56
9.10 Debug Logs	57
9.11 SIP Logs	58
10 Firmware Upgrade Management.....	59
10.1 Network Dimensioning.....	59
10.2 TFTP Configuration	60

10.3 Create Firmware Directories	61
10.4 Login to Base SME Configuration Interface	61
10.5 Firmware Update Settings	63
10.6 Base Station(s) Firmware Upgrade	65
10.7 Handset (s) Firmware Upgrade	66
10.8 Verification of Firmware Upgrade	66
10.9 Reboot the Base station(s)	68
11 Registration Management - Handset	70
11.1 Hardware required	70
11.2 Software required equipment	71
11.3 Add server	71
11.4 Register handset to base	73
12 VLAN Setup Management	77
12.1 Introduction	77
12.2 Backbone/ VLAN Aware Switches	78
12.3 How VLAN Switch Work: VLAN Tagging	79
12.4 Implementation Cases	79
12.5 Base station Setup	80
12.6 Configure Time Server	81
12.7 VLAN Setup: Base station	82
13 Multi-cell Setup & Management	83
13.1 SME Configuration Interface	83
13.2 Adding Base stations via SME Configuration Interface	83
13.2.1 Time Server Setup	85
13.2.2 SIP Server (or PBX Server) Setup	86
13.2.3 Multi-cell Setup	87
13.3 Synchronizing the Base stations	90
13.4 Summary of Procedure – Creating a Chain	92
13.5 Stage 1	92
13.6 Stage 2	92
13.7 Stage 3	93
13.8 Stage 4	94
13.9 Practical Configuration of Multi-cell System	95
13.9.1 Case ##1: Isolated Buildings	95
13.9.2 Case ##2: Location with co-located partners	96
13.9.3 Case ##3: Large to Medium Sized Enterprises	97
13.9.4 Case ##4: Large Enterprises at Different Locations	98
14 Functionality Overview	100
14.1 System Feature List	100
14.2 Detail Feature Description	101
15 Network Operations	104
15.1 Introduction	104
15.2 System Start Up	104
15.3 Terminal Attachment	104
15.4 Outgoing Calls	104
15.5 Incoming Calls	104

15.6 Handover	105
15.6.1 RTP Stream Remains at Initial Base Station.....	105
15.7 Roaming.....	106
16 Operation Setup – Bases/Handsets/SIP Sever	108
16.1 Power Up	108
16.2 Power Down	108
16.3 Call Operations	109
16.3.1 Initiating Calls	109
16.3.2 Call Holding	110
16.3.3 Call Transfer (Blind)	111
16.3.4 Call Bridging (Attended Transfer)	111
16.3.5 Call Conference (Conference).....	112
17 Handset - Service Menu Management.....	113
17.1 Service Menu – Site Survey Mode.....	113
17.2 Service Menu Parameter Definitions	114
17.2.1 Master Reset.....	114
17.2.2 Site Survey Mode.....	114
17.2.3 HS Logs.....	115
17.2.4 Status	116
17.2.5 IPEI	116
17.2.6 Demo mode	117
Appendix.....	118
18 Appendix A.....	119
Handset.....	119
Base Station	120
Web interface	120
Charge unit	121

Reviewed

1 About This Document

This document describes the configuration, customization, management, operation, maintenance and trouble shooting of the SME VoIP System. It also describes effective practices that should be done to deploy an optimal SME System.

1.1 Audience

Who should read this guide? First, this guide is intended for networking professionals responsible for designing and implementing RTX based 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 UMBER 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 also deploy a fully functionally VoIP SME System.

1.3 Important Assumptions

This document was written with the following assumptions in mind:

- 1) You have understanding of 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	Description of System Deployment Scenarios	Provides the reader an idea of different possibilities available to the user in deploying the system.
Chapter 4	SME VoIP Network Planning/Optimization	To learn radio network planning techniques including dimensioning, detailed capacity, coverage planning and network optimisation
Chapter 5	Deployment Mechanics – Multi-cell	Examine practical cases of how Multi-cell SME VoIP network can be deployed

	SME Network	
Chapter 6	Installation of Base station/Repeater	Considerations to remember before unwrapping and installing base units and repeaters
Chapter 7	Making Handsets Ready	To determine precautions to take in preparing handsets for use in the system
Chapter 8	Core Network Servers Configuration	To learn about operating the handset and base stations including detail description of handset MMI.
Chapter 9	SME VoIP Administration Interface	To learn about the Configuration Interface and define full meaning of various parameters needed to be setup in the system.
Chapter 11	Firmware Upgrade/Downgrade Management	Provides a procedure of how to upgrade firmware to base stations and/or handsets
Chapter 12	Registration Management - Handsets	Learn how to add servers via the Configuration Interface and how to register handset to base stations
Chapter 13	VLAN Setup Management	Examines how to setup VLAN in the SME network
Chapter 14	Multi-Cell Setup & Management	Learn how to setup multiple bases into a multi-cell network
Chapter 15	System Functionality Overview	To gain detail knowledge about the system features.
Chapter 16	Network Operations	To study the operation of network elements during system start up, location registration, etc.
Chapter 17	Operations Setup – Handset/Base/SIP Server	To study the operation of handset and base stations/SIP server.
Chapter 18	Handset – Service Menu Management	To learn how to enable and use the hidden menu's in the handset

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 documentation.

1.6 Abbreviations

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

DHCP:	Dynamic Host Configuration Protocol
DNS:	Domain Name Server
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

1.7 References/Related Documentation

[1]:	Deployment Kit Guide Version 2.5
[2]:	Hosted PBX Solution - Deployment Kit Version 0.5
[3]:	Handset operation Manual V0.1
[4]:	

1.8 Document History

Revision	Author	Issue Date	Comments
1.5	MYA	17-Dec-2010	Complete review and modifications of all sections
1.4	MYA	12-Nov-2010	New Input: 17.3 Call Operations, Operations Setup – Handset/Base/SIP Server.
1.1	MYA	27-Oct-2010	Total re-write of overall of manual
1.0	MYA	05-Oct-2010	First version, SIP version, EU DECT
0.1	MYA	23-Sep-2010	Initial Version

1.9 Documentation Feedback

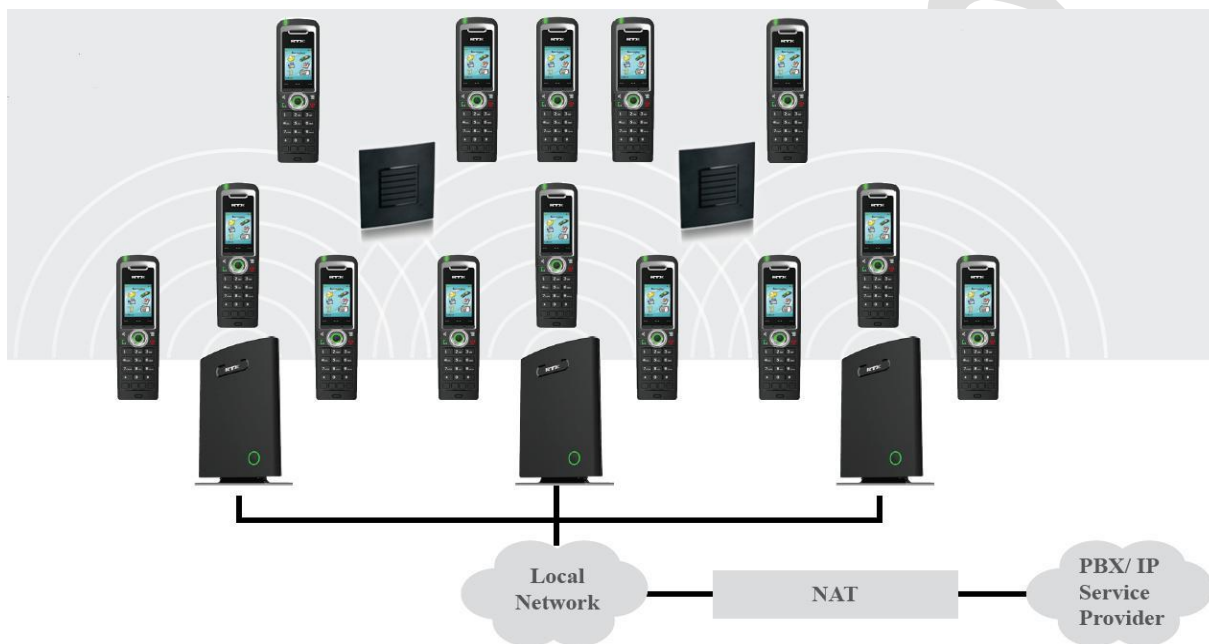
We always strive to produce the best and we also value your comments and suggestions about our documentation. If you have any comments about this guide, please enter them through the Feedback link on the RTX Telecom website. We will use your feedback to improve the documentation.

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 back-bone 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 40 bases in the same network. Further it is able to support up to 200 registered handsets. 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 next generation IP DECT CAT-IQ repeater with support up to 5 channels simultaneous call sessions.

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



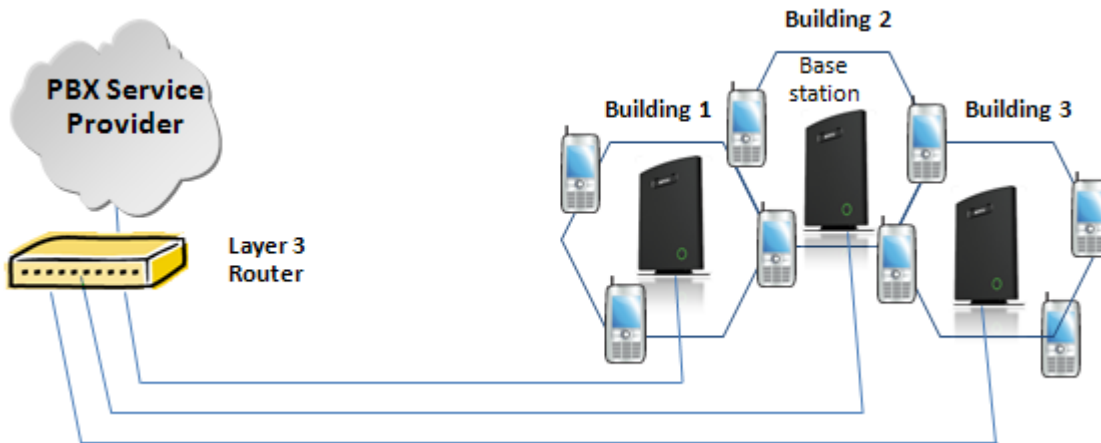
2.1 Hardware Setup

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 indoor (300m outdoor). Radio coverage can be extended to 400m using repeaters that are installed up to 300m from the base-station(s).

The base-station antenna mechanism is based on space diversity feature which improves coverage. The base-stations use complete DECT MAC protocol layer and IP media stream audio encoding feature to provide up to 10 simultaneous calls.



2.2 Components of SME VoIP System

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

- At least one RTX Base Station is connected over an IP network and using DECT as air-core interface.
- RTX IP DECT wireless Handset.
- RTX 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.
- Other 3rd party vendor products which will be described in details in Chapter 8

2.2.1 RTX 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 signalling 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 signalling 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

administrator. These logs can be used to troubleshoot the system when the system faces unforeseen operational issues.

2.2.3 RTX Wireless Handset

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

The handset includes Colour 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 manual for full details handset features.

2.3 Wireless Bands

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

Frequency band:	1880 – 1930 MHz (DECT)
	1880 – 1900 MHz (10 carriers) Europe/ETSI
	1910 – 1930 MHz (10 carriers) LATAM
	1920 – 1930 MHz (5 carriers) US

Other frequency bands can be customized via Base station low-level debug programming.

2.4 System Capacity (in Summary)

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

Description	Capacity
Min ## of Bases Single Cell Setup	1
Max ## of Bases in Multi-cell Setup	40
Single Cell Setup: Max ## of Repeaters	3 per Base station
Multi-cell Setup: Max ## of Repeaters	3x40=120
Max ## of Users per Base	30
Max ## of Users per SME VoIP System	30x40=1200 (limited to 200)
Multi-cell Setup: Max ## of Synchronisation levels	6
Multi-cell Setup: Max ## of Users	8
Max ## Simultaneous Calls (Single Cell)	10 per Base station
Max ## Simultaneous Calls (Multi-cell Setup)	8x40=320 call sessions

Quick Definitions-

Single Cell Setup:	SME telephony network composed of one base station
Multi-cell Setup:	Telephony network that consists of more than one base stations
Synchronisation Level:	Is the air core interface between two base stations.

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 SME System Deployment Scenarios

In principle, there is no one best solution for deployment of SME Telephony network. Different solutions (i.e. deployments scenarios) exist depending on the customer requirements.

Before describing commonly used cases in SME System deployment, we first describe a multi-cell system and its configuration.

3.1 Multi-cell System

A multi-cell system has a coordinated installation of intra-system synchronized base stations, which enables seamless inter-cell handover for moving handsets.

It provides, besides the increased mobility, higher total capacity and higher quality than a corresponding number of standalone base stations. This is due to a combination of the inter-cell synchronization and the seamless handover features of a multi-cell system.

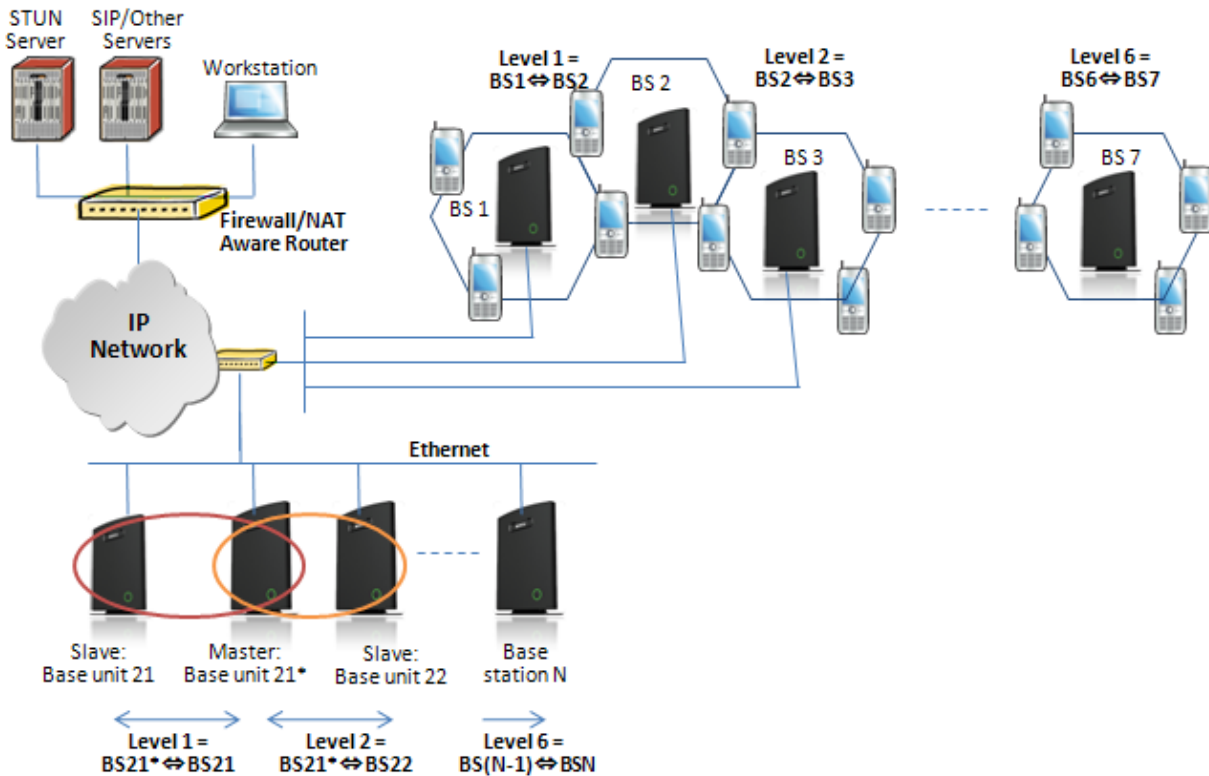
All handsets subscribed to a multi-cell system will benefit from high voice quality, full coverage and full mobility over the whole multi-cell system coverage area.

3.2 Multi-cell Setup

A total of 40 Base stations can be hosted in a typical SME multi-cell system. At each time, a maximum of 6 levels can be formed in a multi-cell chain. Synchronisation Level is the air core interface between two base stations.

Using the figure below, synchronisation level 1 is when Base unit 1 synchronizes to Master Base unit, and Level 2 is when Base unit 2 uses Base unit 1 as its synchronization source, in that order.

The relevant synchronisation levels can be defined by specifying the hierarchy of bases in multi-cell systems. The hierarchy of bases can be specified using the “DECT sync source” parameter in the SME VoIP Configuration Server (Refer to Chapter 13 for detail procedure of Multi-cell setup).



3.3 Case Studies

The following requirements must be considered when deploying SME Telephony Network:

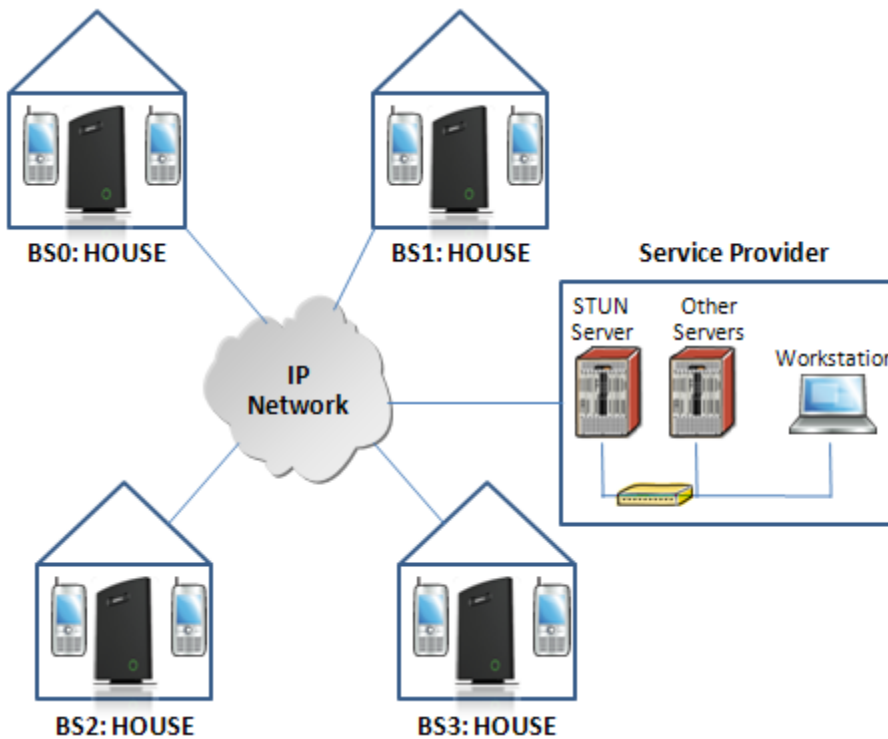
- The type of end users (e.g. Business type, Educational Campus, etc.)
- Distances end users require
- Vendor's Business Situation

In this section we describe common cases or situations where SME Telephony solutions can be implemented. Typical case studies includes (but not limited to):

3.3.1 Case ##1: Isolated Buildings

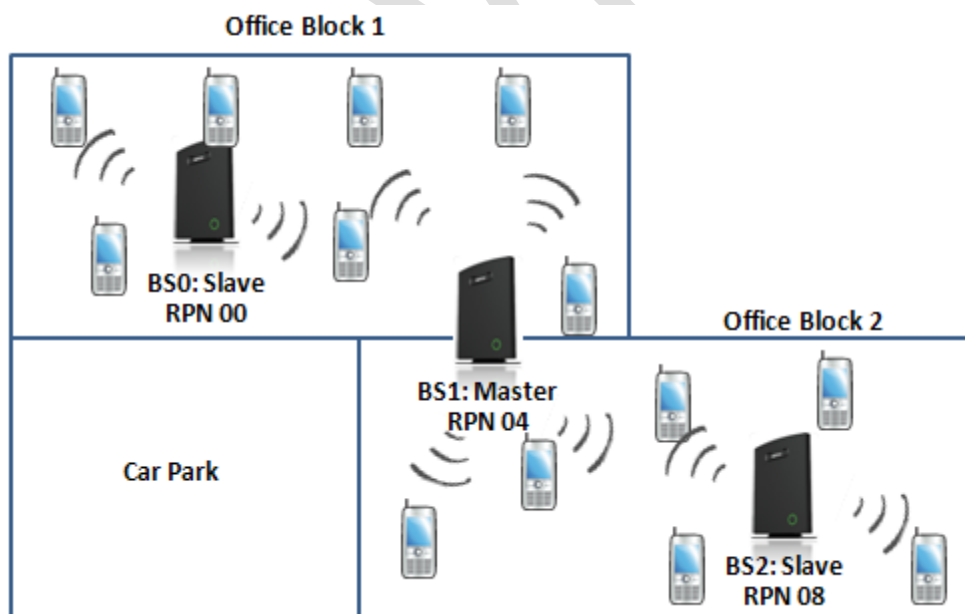
This is the simplest scenario a SME VoIP System can be deployed in e.g. branch or small office, Retail outlet or store. It consists of a standalone base station and a number of handsets registered to it.

This setup is optimal for isolated buildings. A typical illustration is shown in the figure below. From this illustration, it is not possible to roam or handover to other bases in this setup.



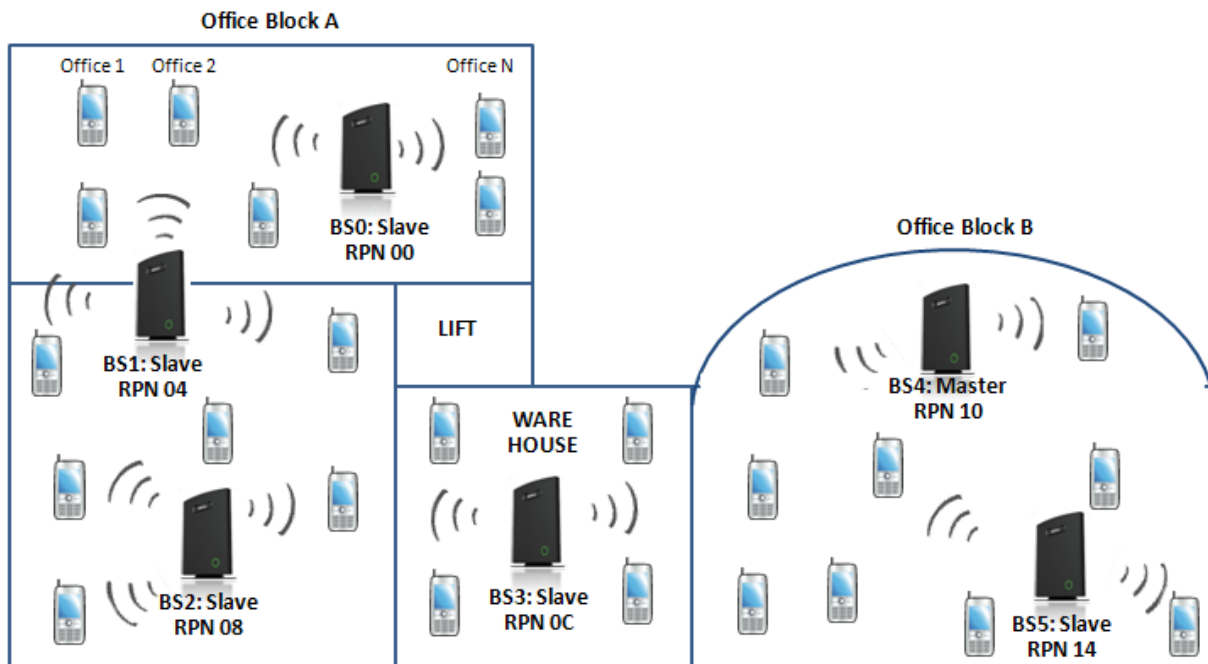
3.3.2 Case #2: Location with co-located partners

This scenario can be deployed in e.g. Department shops, Retail location with co-located photo kiosk or pharmacy and huge apartment complexes. This setup consists of more than one base station and each handset is registered to a specific base. Roaming and handovers are permitted in this setup. Here is diagram to illustrate Case #2. In this illustration, two slave bases synchronises to a Master DECT source.



3.3.3 Case ##3: Large to Medium Sized Enterprises

This scenario is a multi-cell setup can be deployed in e.g. Corporate headquarters, Harbour areas, High School Campus. In the illustration shown below, handsets can roam and handover to other bases.



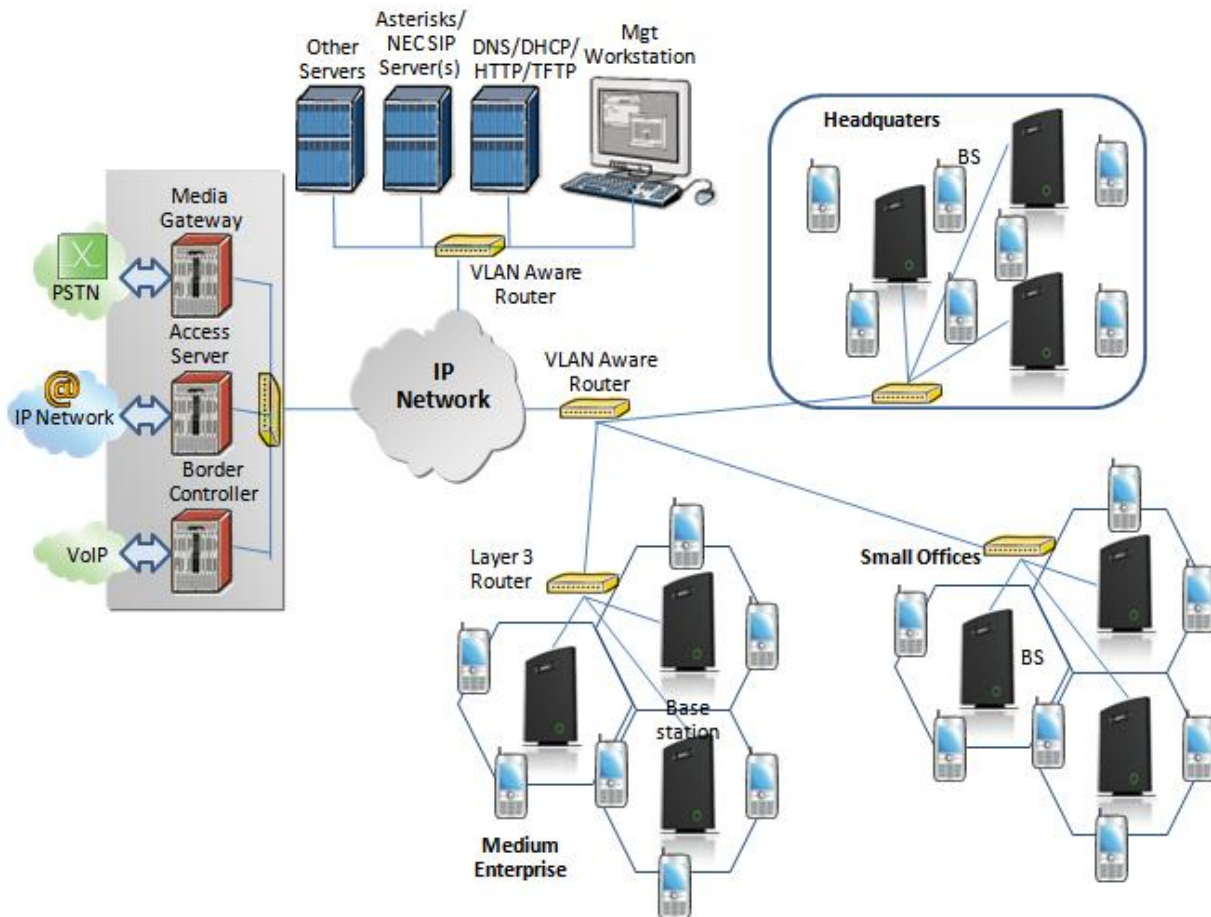
3.3.4 Case ##4: Large Enterprises at Different Locations

In this scenario, multi-cell systems are deployed at different locations; geographically separated from each other. An example of this setup includes Government departments/agencies geographically separated from each other; University campuses or Hospital(s) in different regions.

Roaming and handovers are permitted in this setup even though the each multi-cell system is geographically separated from each other.

Each base station has a unique identifier. Handsets registered to one multi-cell setup can be used in other geographically separated setups because visited base stations retrieves the base station identifier which the visiting handset is originally registered to.

In addition, the relevant SIP server functions must be enabled to so roaming and handover can be allowed at different geographies.



4 SME VoIP Network Planning/Optimization

In this chapter, we describe SME VoIP radio network planning techniques including dimensioning, detailed capacity and coverage planning, and network optimisation.

4.1 Network Requirements

Network requirement is essential to determine elements necessary to achieve the overall expectations of the customer. Typical network requirements includes (but not limited to):

- The geographical area to be covered
- The type or architecture of building and/or topology, etc.
- The estimated traffic on each zone or region or building
- The blocking criteria in each traffic area.
- The relevant quality targets expected to be achieved

4.2 Deployment Considerations

The following radio considerations must be examined before deploying a SME VoIP System. These includes (but not limited to):

Building Penetration:

When a signal strikes a building it is diffracted or absorbed; therefore to some extent the signal is reduced. The amount of absorption is dependent of the kind of building and its environment, the amount of solid structure. This is an important consideration in coverage planning.

Interference Sources:

Signals to receiving antenna can be weakened by virtue of interference from other signals. These signals may be from the same network or other man-made objects. Interference sources must be identified and avoided or minimized.

4.3 Site Planning

4.3.1 Deployment kit

Based on propagation models, the coverage of areas is done with the use of radio planning tools. In the RTX SME VoIP Network, the radio planning tool available is called Deployment Kit. Detail description and use of this document is available in a separate document(s) [1][2].

4.3.2 Location Probability

The quality of coverage is determined by location probability. For practical purposes, the location probability of 50% is equal to the sensitivity of receiver in a specific region. This is also measured by the Deployment Kit [1][2].

4.3.3 Handover Mechanics/Planning

Handsets should seamlessly move between coverage areas. In other words, handset should be able to move in a multi-cell setup of base stations and/or repeaters from one base station to another without terminating or causing hindrance while receiving continuous service and maintaining call-sessions in progress.

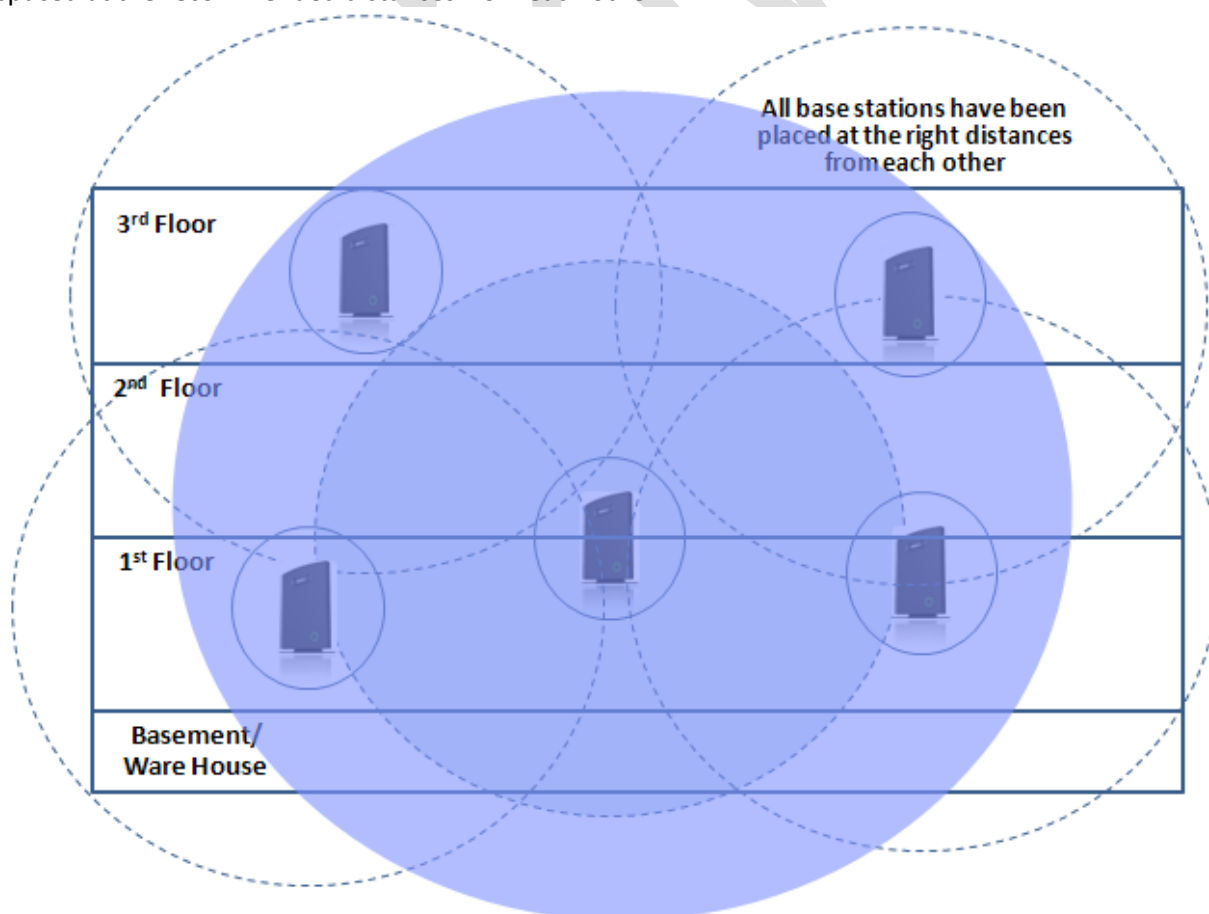
For efficient handover of conversations between Base stations in multi-cell setup, deploy Base stations with wide overlap between them (i.e., plan for some areas to be covered by more than one Base station). Overlaps are necessary to maintain seamless handover and to establish synchronization chains. A good example may be a cafeteria during lunch hour where temporary concentrations of handsets may occur. The overlap carries the excess call load to adjacent Base stations to provide uninterrupted services to subscribers.

4.4 Cell Coverage / Capacity Planning

4.4.1 Cell Coverage

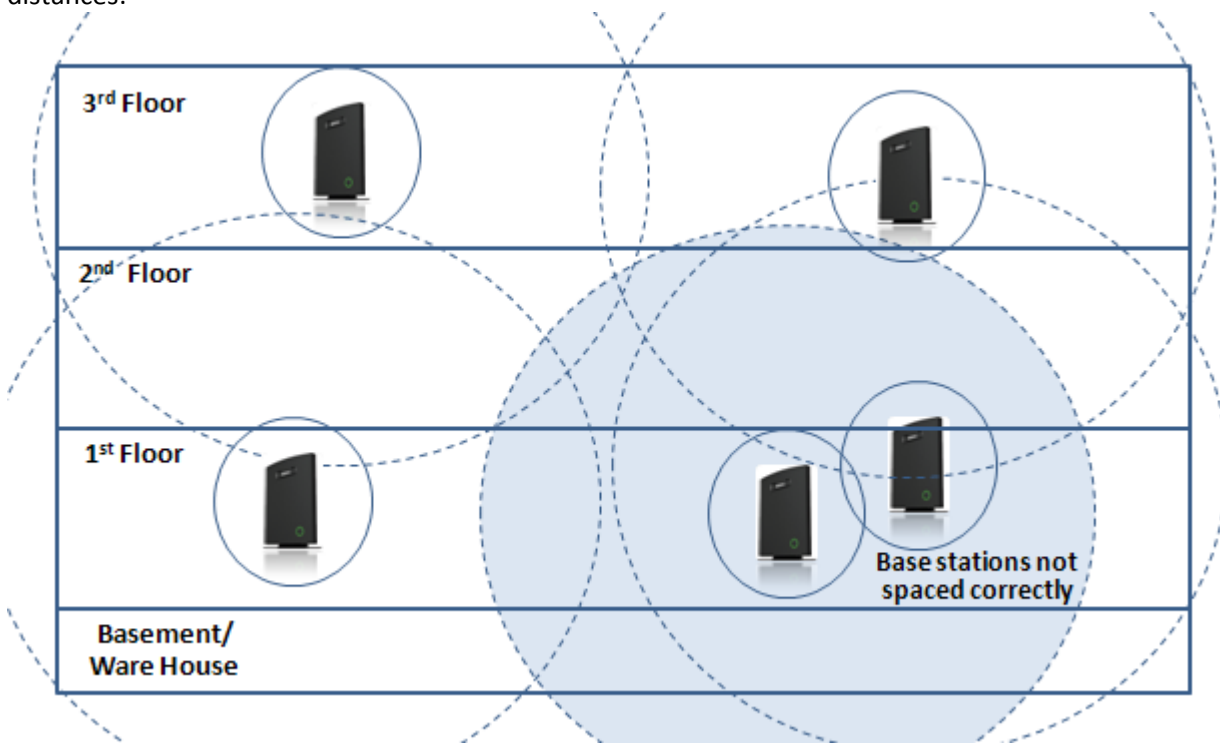
Due to the unexpected nature of RF propagation in an indoor environment, an actual on-site test must be performed before the deploying and/or installing core network elements. An extensive guide to effective RF coverage planning is outside the scope of this document. This should be noted:

The Base stations provides typical RF coverage of up to 50 meters/164 feet in a typical indoor office environment and up to 300 meters/984 feet in an open area (line-of-sight-LOS), extending in all directions from the Base stations (i.e. Omni directional). The exact coverage range depends on the building architecture, wall material and surroundings. The figure below show the correct installation of base stations spaced at the recommended distances from each other:



Typically, installations such as office buildings, hotels and hospitals should be equipped with both base stations and repeaters on several floors to create uniform and complete radio coverage. Open areas can be covered with a sparse network of base stations. In such deployments, the base stations and/or repeaters cover an extended range due to the extended line-of-sight radio propagation capability

The figure below shows an example of an installation where base stations are not spaced at the right distances:



4.4.2 Capacity Planning

This is where the Network provider estimates how many calls will be initiated in a typical window/time frame and how many users will be initiating them.

Another aspect of capacity planning should address the user growth pattern of a typical SME VoIP network. How many users will be using this network in for example two years window, etc. Based on these estimations, the network dimensioning can be planned orderly bearing in mind the SME capacity.

The capacity of the SME VoIP System is summarised as follows (this should guide the network planner):

Description	Capacity
Min ## of Bases Single Cell Setup	1
Max ## of Bases in Multi-cell Setup	40
Single Cell Setup: Max ## of Repeaters	3 per Base station
Multi-cell Setup: Max ## of Repeaters	$3 \times 40 = 120$
Max ## of Users per Base	30
Max ## of Users per SME VoIP System	$30 \times 40 = 1200$
Multi-cell Setup: Max ## of Synchronisation levels	6

Multi-cell Setup: Max ## of Users	8
Max ## Simultaneous Calls (Single Cell)	10 per Base station
Max ## Simultaneous Calls (Multi-cell Setup)	8x40=320 call sessions

4.5 Network Dimensioning

After the network requirements are clearly defined, the number of users that are expected to use the network must be estimated. Based on that, you should estimate and identify the number and type of equipments required in order to cater for the capacity, coverage and quality requirements. The more accurate the dimensioning, the more efficient the network rollout.

Handsets/SIP End-Nodes:

In a typical setup, the system can support up to 200 handsets depending on the configuration.

Base stations/Repeaters:

The system can easily scale up to 40 base stations. Depending on the network setup, coverage can be extended by up to 5 repeaters. The planner should bear in mind that base stations can support 10 simultaneously call sessions while repeaters can support 5 call sessions.

Core Network Equipments:

These equipments are at the premises of the service operator or data center. Depending on the network requirements the following devices should be available:

VLAN/NAT aware router(s), Session Border Controller, DHCP/TFTP/FTP Servers, STUN Server, Media Server, Access Gateway, SIP Server, etc.

4.6 Environmental Considerations

In this section, we enumerate some environmental conditions that need to be considered prior to planning, deployment and optimisation of the SME network. The considerations are as follows:

- Ensure that the installation area is clean, dry, and protected from weather extremes.
- Ensure that the floor of the installation area is finished with linoleum, vinyl, ceramic, wooden flooring, computer floor tiles, or polished sealed concrete.
- Ensure that the ceiling of the installation area is finished or treated to prevent particle discharge.
- Ensure that the installation area is well lit, and that the light source is uniformly diffused without shadows. Adequate lighting should provide a comfortable reading level and allow the identification of wire insulator colours without undue eye fatigue. Lighting should be comparable to an office work environment, with a minimum level of 21 meter/68.9 feet at each work surface. As a rule of thumb, in a room with a 2.5 meters/8.2 feet ceiling, one 1.2 meters/4 feet fluorescent tube provides sufficient illumination for 1.9-2.4 square meters/20.5-25.9 square feet.
- Ensure that ventilation of the installation area is capable of maintaining an ambient temperature of 0-40°C/32-104°F, and a relative humidity of 20-80% non-condensing, while the system is operating. The maximum power rating of a base station under full load should not exceed 315W/1070 BTU/Hr. These figures are for each cabinet only, and do not take into account heat generated by other equipment. In particular, charging fully-discharged batteries may generate a considerable amount of heat, depending on battery capacity and rate of charge. Refer to the equipment manufacturer data for more information.

- Ensure that the installation area is free of caustic or corrosive liquids, substances, or materials. If batteries will be installed as part of the system, ensure that adequate precautions are taken (such as special ventilation) to prevent corrosive emissions from the batteries. Check local building codes for additional requirements.

4.7 Recommended Base station/Repeater Placement

There is no one strategy for deploying base stations. These are some recommended Base station and/or Repeater placement strategies:

Around Corridors:

Base stations/repeater should be deployed vertically preferably at corridor intersections where propagation patterns follow the corridor patterns. The base station/repeater should point towards the corridor and preferably in the middle height between the floor and the actual ceiling. In case there are high objects in the area, the base station/repeater should be installed above those objects but still kept distant from the ceiling.

Multi-Storey Buildings:

Base stations and repeaters can be installed on opposite sides of the floors to take advantage of the floor-to-floor coverage. The coverage design cannot rely entirely on floor-to-floor propagation; each case must be verified due to variations in local attenuation patterns.

Open Areas/ Large Halls:

Base stations and repeaters can be deployed in open areas for buildings that contain a central open space area with windows to the other areas. This provides a good coverage for the rooms in the inner circle on all floors (e.g. hotels).

In large halls, Base stations/repeater should be installed vertically in the middle of the space below the drop ceiling.

Mounting Positions:

When Base stations and repeaters are mounted vertically on a wall, the radio coverage in front of these devices is twice as large as the coverage at the rear.

Repeaters should be installed in the middle of corridors and small rooms.

Metallic Structures/Objects:

Base stations and repeaters should not be deployed near large metallic objects.

Reinforced Concrete Structures:

These structures have a high attenuation factor inside the building. They reduce the radio coverage range of the Base stations and repeaters and therefore require a higher number of base stations or repeaters in the building. Lighter types of construction materials require fewer base stations since attenuation figures are considerably lower.

Others Recommendations:

- Maximum distance between two base stations varies depending on material and construction of buildings, but there must always be synchronization chains and radio coverage overlap between the two base stations or handover between radio units. The time it takes a person to cross the common coverage area must be 10 seconds or more, as the handset needs time to scan for an alternative base stations.
- Ensure that the installation area is located no closer than 6.1meters/20.0 feet from electric devices that produce large electro-magnetic fields (EMF) or high levels of radio frequency energy. Possible EMF

sources are radio transmitters, electric arc welding machines, copying machines, electric motors, refrigeration units, power transformers, electric load centers, and main circuit breaker panels.

- Ensure that the electrical service is sufficient and located in close proximity to the Base stations.

4.8 Network Assessment/Optimisation

This involves monitoring, verifying and improving the performance of the SME VoIP network. Depending on the network setup and varying deployment conditions and network usage some requirements have to be monitored and corrected.

The main focus of network optimisation should be telephony quality, handovers, network traffic and other related measurements.

The quality of the network is ultimately determined by the satisfaction of users of the network. Therefore before SME VoIP Networks are handed over to customers, Network providers must perform walk or drive testing using the appropriate measurement kits.

The walk or drive testing kit includes 2 or 3 test phones, a walk/drive testing software (deployment kit software) and a suggested walk path, etc.

Collect statistics of the network an example is illustrated in the table below:

Parameters	Value	Comments
## Call Setup failures		
## Dropped calls		
## HO successes		
## HO failures		
Traffic Blocking Rate (%)		
Traffic Blocking (Erl)		
Receiver level (dBm)		
Receiver Quality (%)		

After collecting the necessary information, you should fine tune signalling and radio resource sharing parameters. Network optimisation is a continuous process during and after the launch of the network.

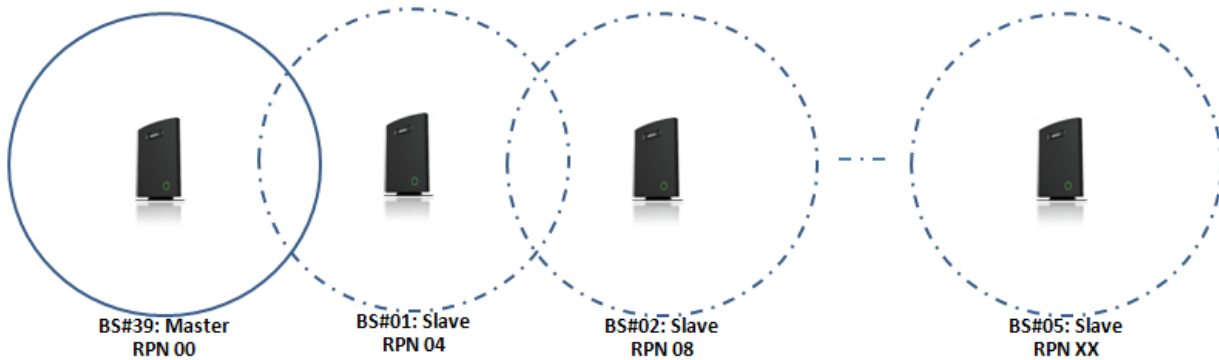
For example, if it is found that an area within a building has low signal level. There should be an immediate scrutiny of base station and/or repeater locations, heights and tilts. The problem is sorted out by moving the relevant devices and altering the tilts of these devices.

For buildings/halls constructed with high signal attenuation materials, deploying additional base stations will be one of the solutions.

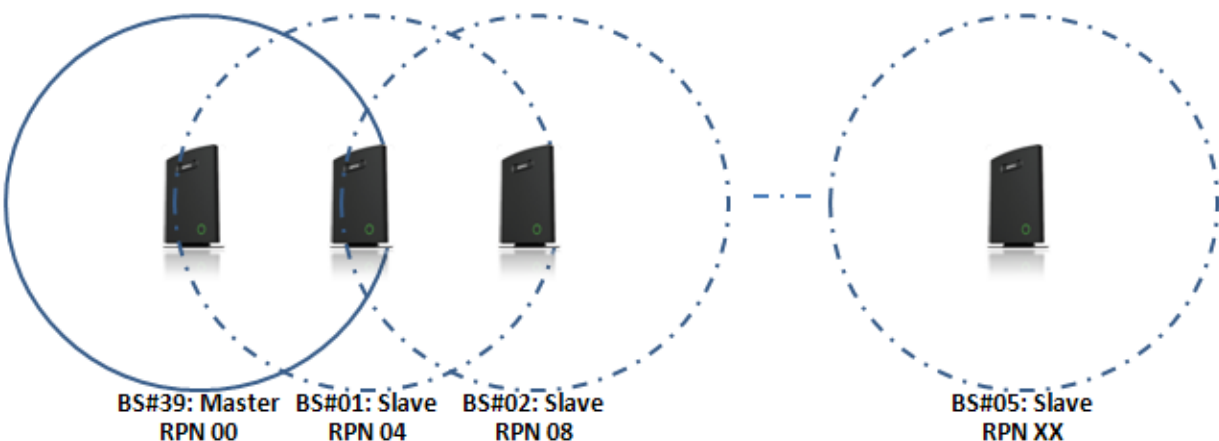
5 Deployment Mechanics – Multi-cell SME Network

In this chapter we provide short description of practical cases of how Multi-cell SME VoIP network can be deployed – unfold synchronisation details of how master bases latches to one or more slaves.

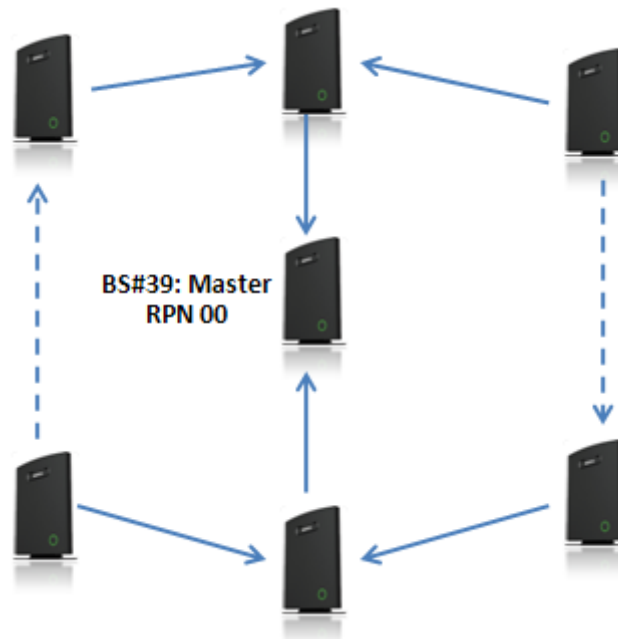
Case ##1: Synchronisation Chain with One Master Sync.



- The Synchronisation chain must always overlap with other Base stations in order to latch each other in Sync.
- In this illustration Base station ##39 is the Sync Master
- A maximum of 7 devices (Including the master bases) can be chained at a time
- The other slave base stations or repeaters are connected to the Sync Master through the synchronisation chain
- If one of the base or repeater units in the sync chain is broken or not working, then the units that follows non-working device are cut off from the sync chain. Therefore handover is not possible between the non working units and working ones.
- However, handover is possible in the deployment figure below, because e.g. both BS#01 and BS#02 overlaps with BS#39. Therefore when BS#01 is not active, handover between BS#39 and the rest of the slaves is still permitted.



Case ##2: Synchronisation Chain without Alternative Sync Paths



- Assuming Master Sync source is Base station ##39. A maximum of 40 base stations can be deployed in one setup (depending on the network requirement not all base stations should be chained).
- A maximum of 7 devices can be chained at one time.
- Depending on the system setup, it is recommended to place the Sync source Master in the middle of the building and to assign numbers/addresses, radio ID (RPN), etc., to each base station or repeater for easy identification.
 - Continuous line:** Shows the primary sync paths, with the relevant bases chained in the multi-cell network.
 - Dotted line:** Alternative sync paths, but cannot be used because the relevant base stations have not been chained.

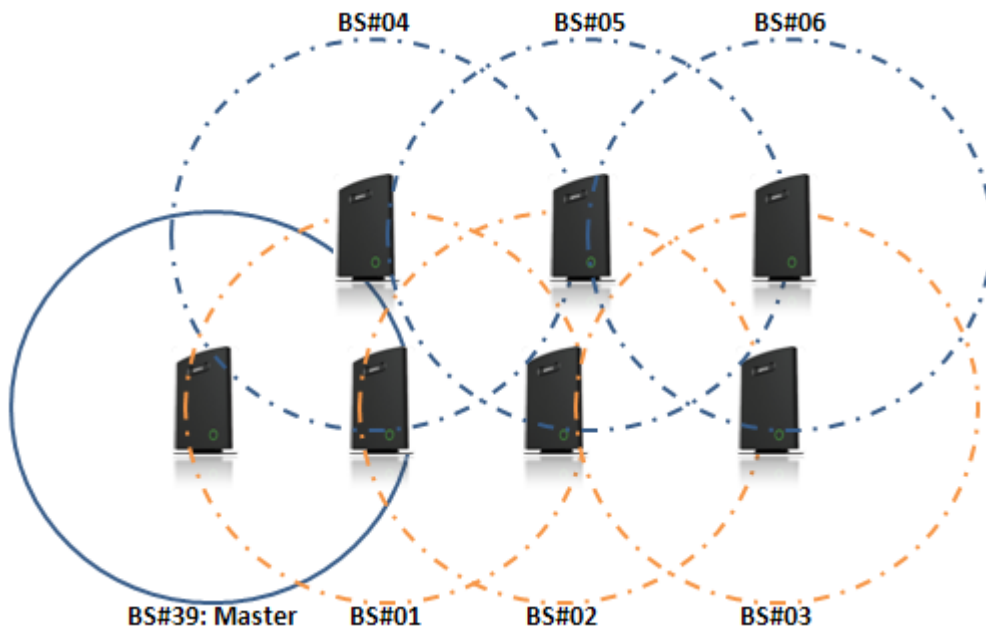
Case ##3: Synchronisation Chain with Alternative Sync Paths

The illustration below shows a multi-cell network with alternative Synchronisation paths. A failure of one base unit does not mean handset or users cannot perform handovers to other active cells.

BS#39 is the SYNC Master, if BS#05 is down, most user handovers can be formed via 3 other alternative cells (i.e. BS#06, BS#02 and BS#04) without any problems at all.

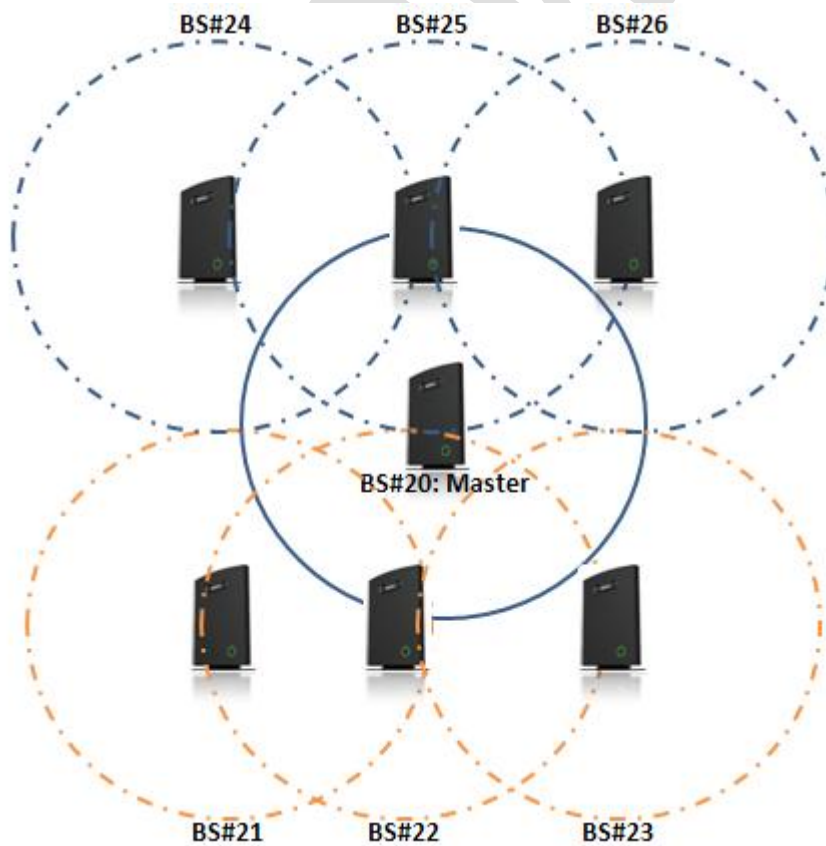
Furthermore observe the following:

- BS#04 and BS#01 are Primary with alternative sync to BS#39.
- BS#05 is primary sync to BS#04 while alternative sync is BS#01 or BS#02
- BS#03 is primary sync to BS#02 while alternative sync is BS#05 or BS#06.



In the illustration below:

- BS#24 is primary sync to BS#25 while alternative sync is BS#20
- BS#22 is primary sync to BS#20 while alternative sync is BS#21 or BS#23.



6 Installation of Base Stations/Repeater

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

6.1 Package - Contents/Damage Inspection

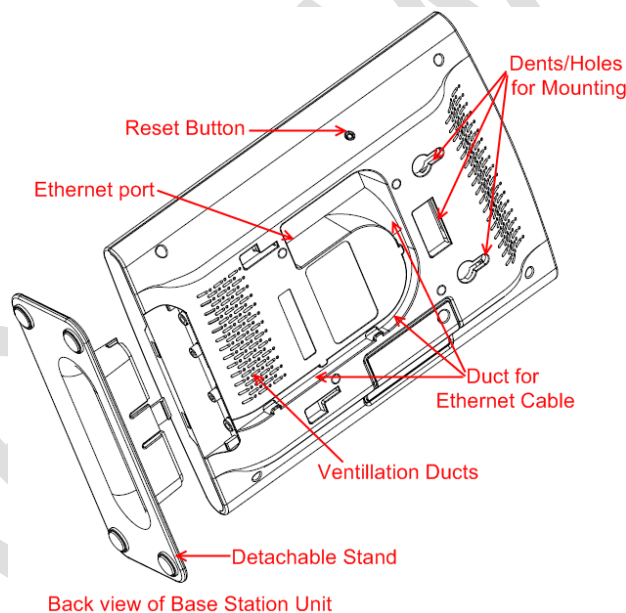
Before Package Is Opened:

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 Metal plate(s)
- 1 x Plastic stand
- 1 x Cat. 5 cable (Ethernet cable)
- Base unit



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 it has been examined by the operator. 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.

RTX Base station Provides RF Channels to Handsets

The base station supports 12 RF channels simultaneously for all DECT bands, summarised below:

The RF communication is provided according to the band standard at the site:

Frequency band: 1880 MHz – 1930 MHz (DECT)
 1880 – 1900 MHz (10 carriers) Europe/ETSI
 1910 – 1930 MHz (10 carriers) LATAM
 1920 – 1930 MHz (5 carriers) US

Other frequency bands can be customized via Base station low-level debug programming.

6.2 RTX 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 summarises the various LED states:

LED State	State
Unlit	No power in unit
Unlit/Solid red	Error condition
Blinking green	Initialisation
Solid red	Factory reset warning or long press in BS reset button
Blinking red	Factory setting in progress
Solid green	Ethernet connection available (Normal operation)
Blinking red	Ethernet connect not available OR handset de/registration failed
Solid red	Critical error (can only be identified by RTX Engineers). Symptoms include no system/SIP debug logs are logged, etc.
Orange	Press reset button of base station.

6.3 RTX 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.

6.4 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.

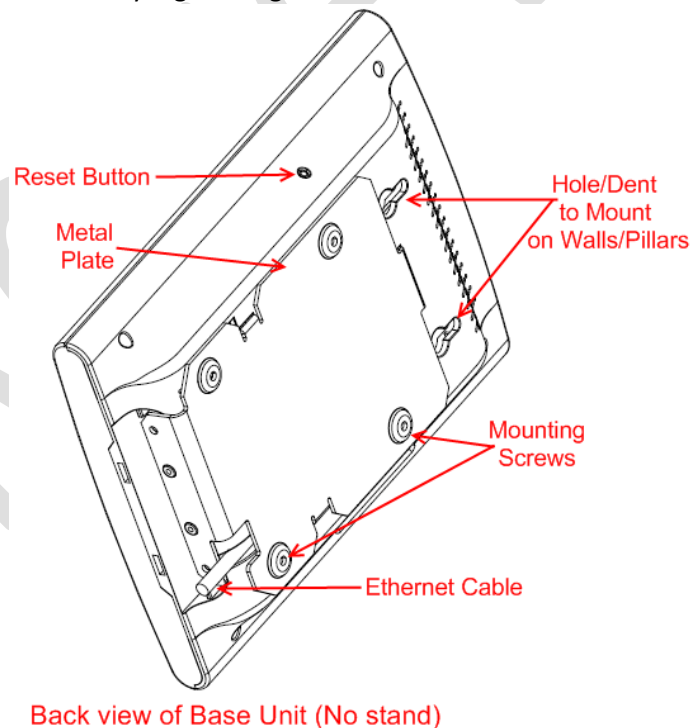
Next, mount the Base Station on a wall to cover range between 50 - 300 meters (i.e. 164 to 984 feet), depending whether it's an indoor or outdoor installation. Please refer to chapter 4 for important information regarding network requirements, deployment considerations, site planning, cell coverage/capacity planning, environmental considerations and recommended Base station placement.

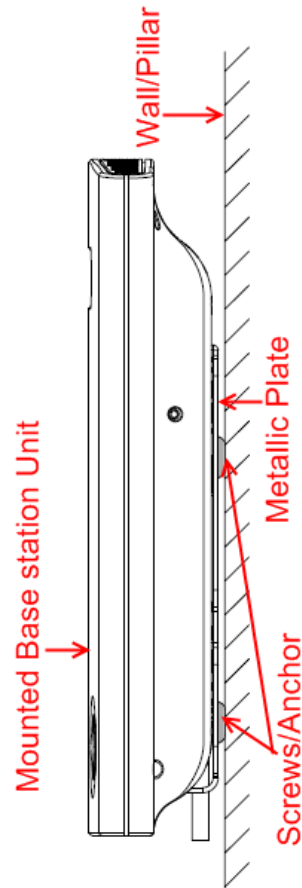
Mounting the Base Stations/Repeaters:

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 units 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.





Documentation of Installation:

It is highly recommended to document the deployment of Multi-cell network; writing the locations or relevant geographical addresses each base unit has been installed.

This is useful for maintenance purposes, so installed base units can be located easily on the field.

7 Making 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.

7.1 Package - Contents/Damage Inspection

Before Package Is Opened:

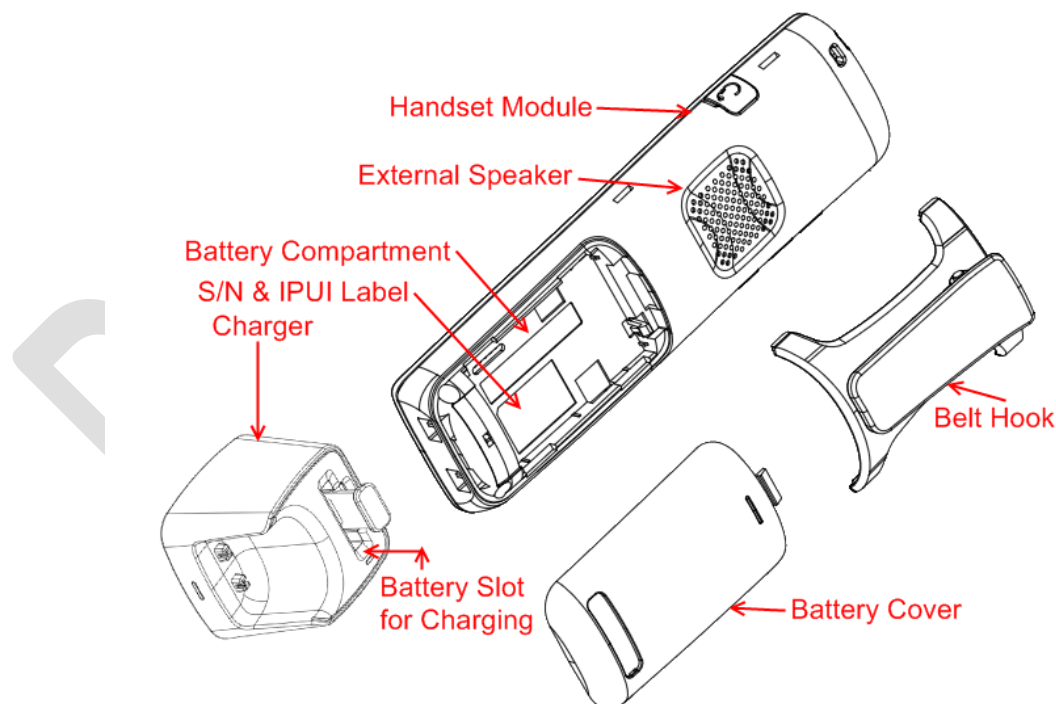
Examine the shipping package for evidence of physical damage or mishandling prior to opening. If there is a proof of mishandling prior to opening, you must report it to the relevant support center of the regional representative or operator.

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 it has been examined by the operator. 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.

7.2 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, customise or short circuit the battery

Using the Charger

Each handset is charged through the use of 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

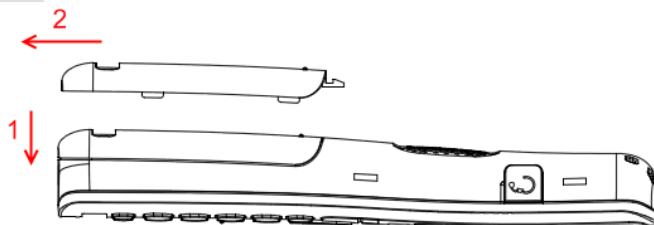
For correct charging, ensure that the room temperature is between 0°C and 25°C/32°F and 77°F. Do not place the handset in direct sunlight. The battery has a built-in heat sensor which will stop charging if the battery temperature is too high.

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

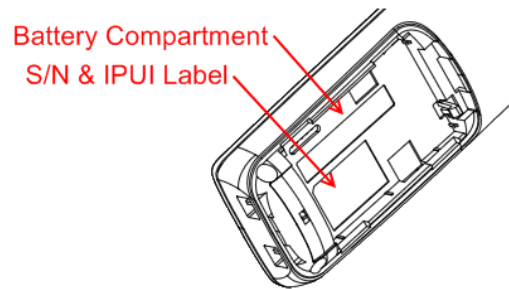
1. Press down the back cover and slide it towards the bottom of the handset.
2. Remove Back Cover from Handset



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.

7.3 Using the Handset

Please refer to chapter 16 for detail description of how to use the handset.

8 Core Network Server(s) Configuration

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

8.1 Server setup

In the SME 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 Repeater and 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.

8.2 Requirements

Regardless of whether or not 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.

8.3 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.

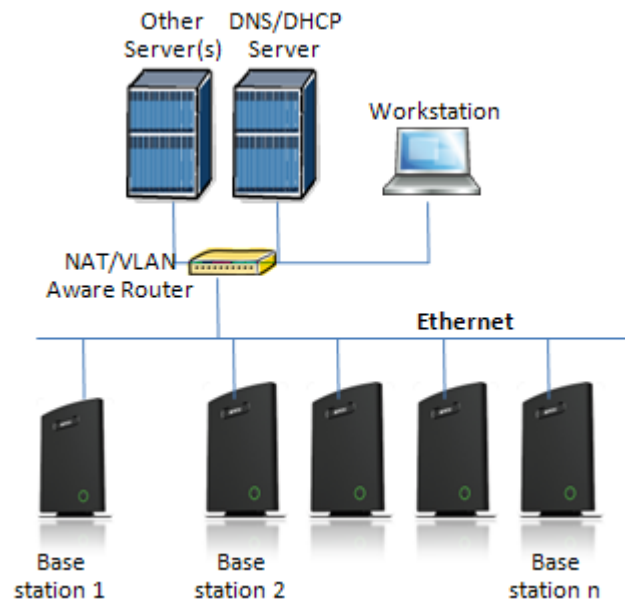
8.3.1.1 Hints on how to Configure DNS behind a Firewall/NAT

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.

8.4 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.

8.4.1 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

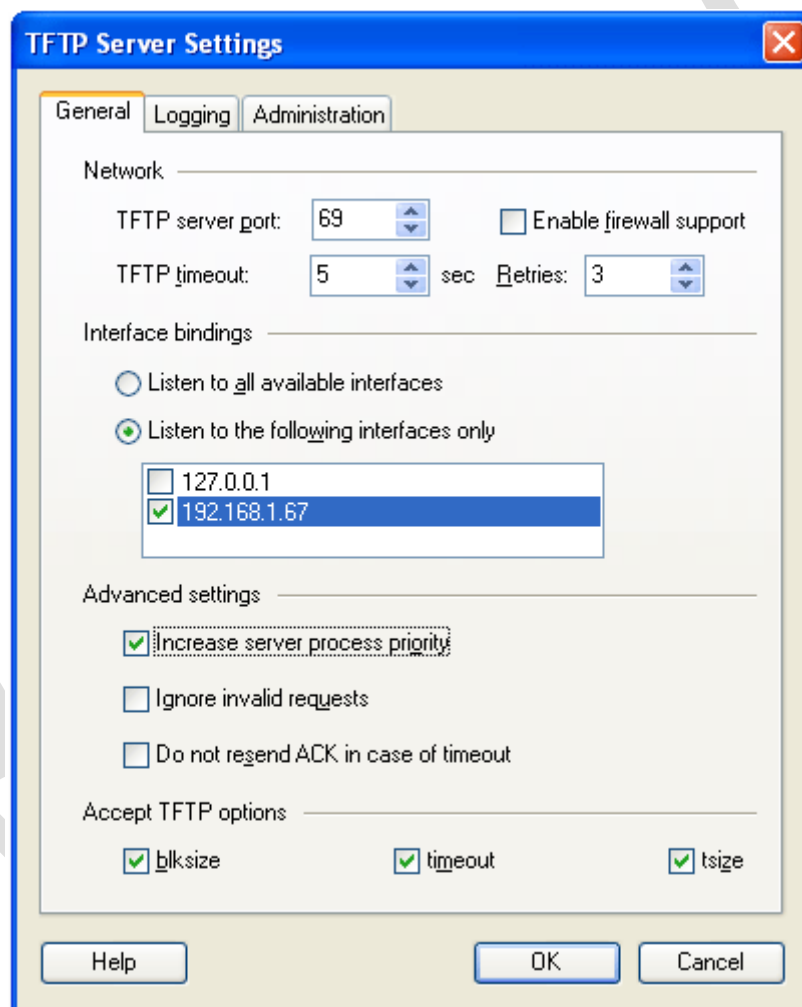
8.5 TFTP Server Setup

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

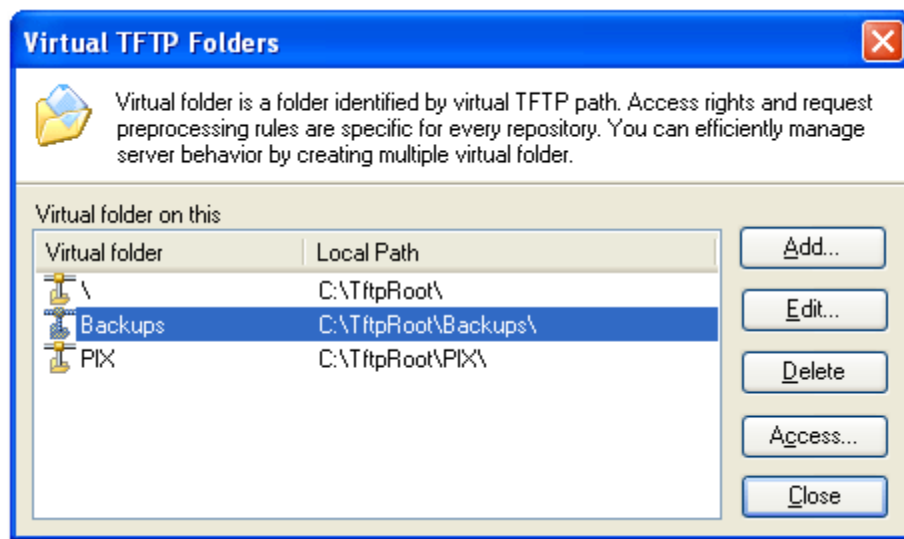
8.5.1 TFTP Server Settings

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.



- 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.



8.6 SIP Server Setup

SIP server is one of the main components of an SME 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.

The RTX SME family of network phones are fully interoperable with the most of SIP Server applications. There are many off-the-shelf vendor and open source SIP servers. In this section, we will briefly explain settings required to take full advantage of FreePBX SIP Server feature set. The settings are similar for other SIP servers.

8.6.1 FreePBX SIP Server

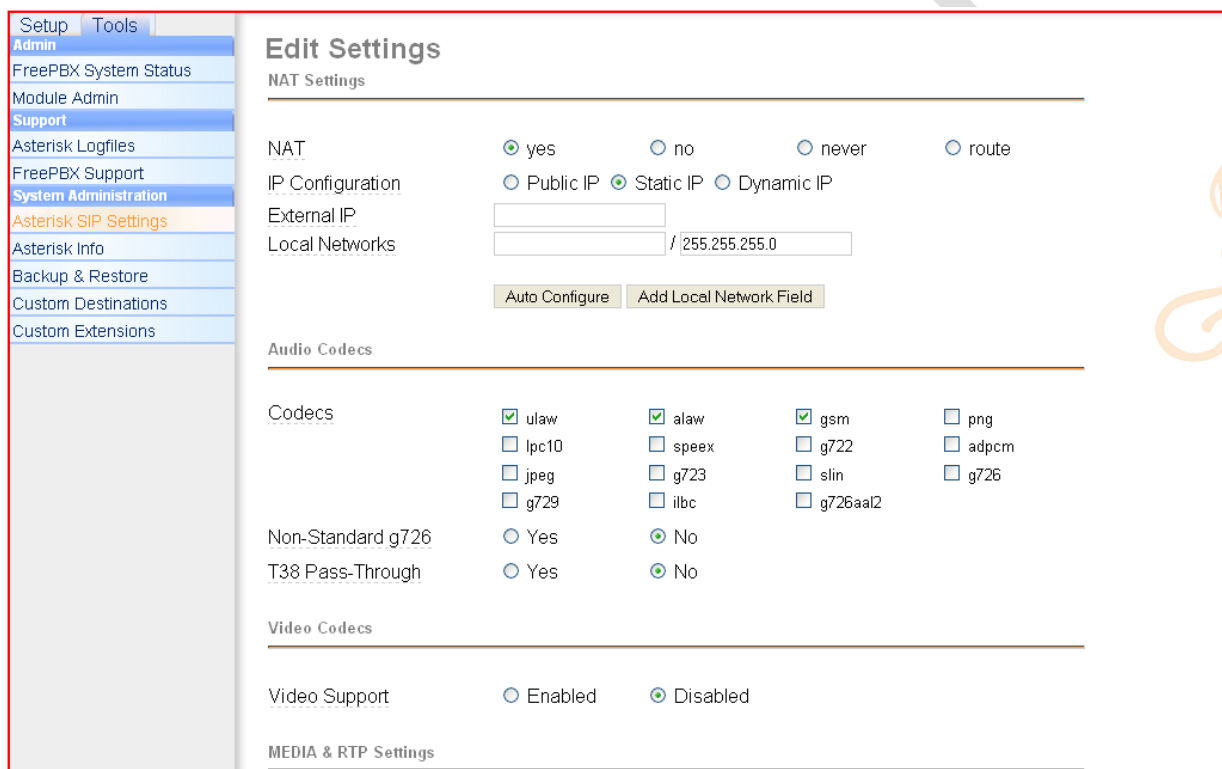
FreePBX is an easy to use GUI (graphical user interface) that controls and manages Asterisk, which the most popular open source telephony engine software.

The administrator should refer to the relevant detail step-by-step procedure of how to install FreePBX SIP server. This section briefly describes SIP Server setup parameters.

1) SIP Server Setup

Settings	Description
NAT	This option determines the settings for users connecting to an asterisk server. Possible values: Yes, No, Never, Route NAT=route Asterisk will send the audio to the port and IP where its receiving the audio from. Instead of relying on the addresses in the SIP and SDP messages. This will only work if the phone behind NAT send and receive audio on the same port and if they send and receive the signalling on the same port. (The signalling port does not have to be the same as the RTP audio port). NAT=No Asterisk will add an RPORT to the via header of the SIP messages NAT=never This will cause asterisk not to add an RPORT in the VIA line of the sip invite

	header
Other NAT Settings	Choose the relevant option or enter the settings in IP configuration, External IP, Local Network.
Codecs	Some SIP Servers supports dynamic codec support. Codecs are algorithm used to compress or decompress speech or audio signals. The user should select the relevant Codecs and other speech compression techniques whose traffic will be routed to the SME network.
Video Codecs	The user should enable this option if SME network supports video telephony.
Media & RTP Settings	This option should be enabled to provide for deliver media streams (e.g., audio and video) or out-of-band events signaling (DTMF in separate payload type).



2) Extensions

This feature allows administrators create handset profiles in the SME network. In other words, Extensions describes the Dial plan for the PBX SIP system. Enter the relevant parameters



Admin
Reports
Panel
Recordings
Help

FreePBX 2.7.0.2 on 192.168.50.77

Apply Configuration Changes

Logged in: admin (Logout)

Setup
Tools

Admin
FreePBX System Status
Module Admin
Basic
SIPSTATION
Extensions
Feature Codes
General Settings
Outbound Routes
Trunks
Administrators
Inbound Call Control
Inbound Routes
Zap Channel DIDs
Internal Options & Configuration
Music on Hold
System Recordings

Add SIP Extension

Add Extension

User Extension
Display Name
CID Num Alias
SIP Alias

Extension Options

Outbound CID
Ring Time
Call Waiting
Call Screening
Pinless Dialing
Emergency CID

Default

Enable

Disable

Disable

Assigned DID/CID

DID Description
Add Inbound DID
Add Inbound CID

Add Extension

117 <117>
118 <118>
119 <119>
201 <201>
400 <400>
1234 <1234>
MYA <2275>
MYA1 <2276>
3000 <3000>
3001 <3001>
3002 <3002>
3003 <3003>
3004 <3004>
3005 <3005>
3006 <3006>
3007 <3007>
3008 <3008>
3009 <3009>

Review

Chapter: Core Network Server(s) Configuration

SME VoIP System Guide, Version 1.5
Proprietary and Confidential

41

VoIPon www.voipon.co.uk sales@voipon.co.uk Tel: +44 (0)1245 808195 Fax: +44 (0)1245 808299

9 SME VoIP Administration Interface

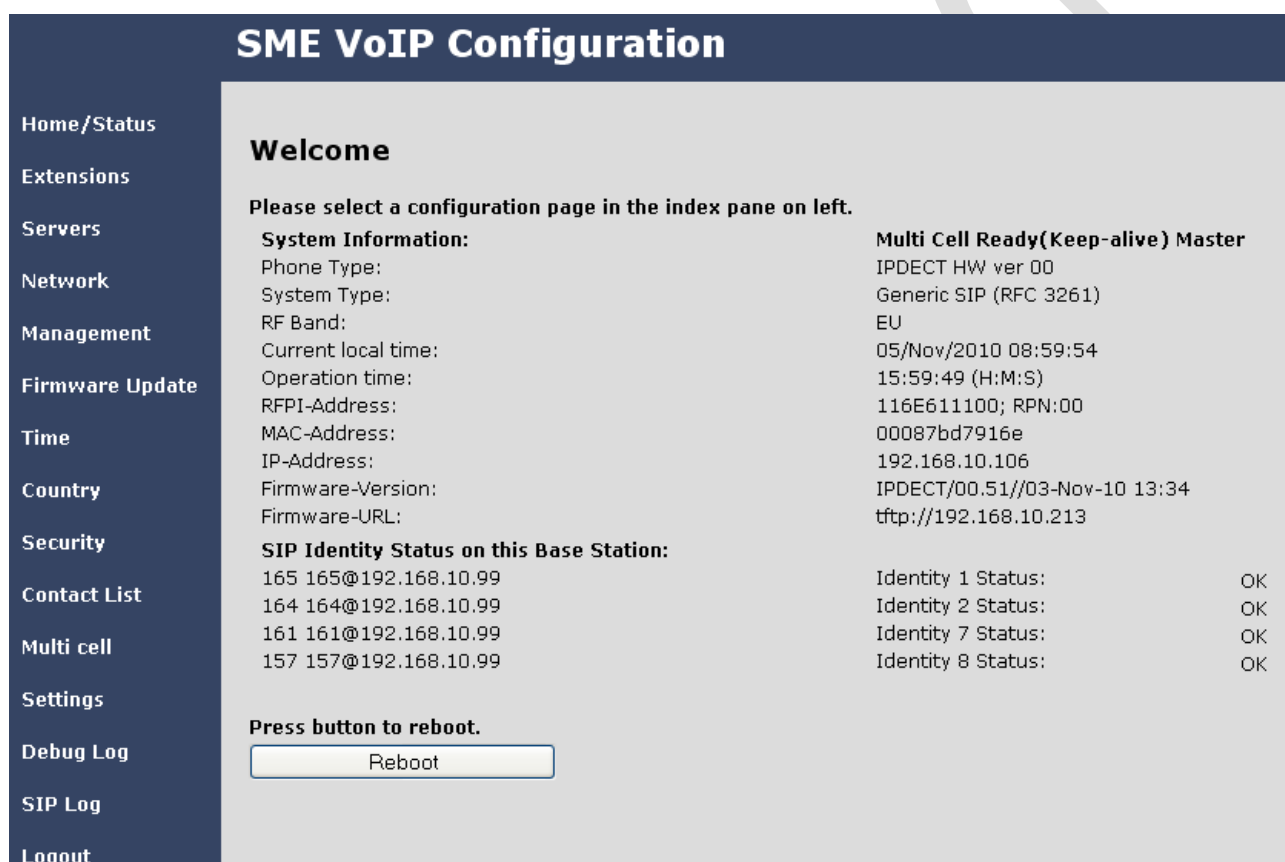
The SME VoIP Administration Interface is also known as SME VoIP Configuration. It is the main interface through which the system is managed and debugged.

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

This chapter seeks to define various variables/parameters available for configuration in the network.

9.1 Home/Status

We describe the parameters found in the front end of the SME VoIP Administration Interface.



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	Sets the Dial plan or phone numbers for the network.
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/TFTP) settings of Base stations and handsets.
Time	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.
Country	Specifying the country/territory where the SME network is located ensures that your phone connection functions properly. Note: The handset language and country setting are independent of each other.
Security	The users can create account credentials with which they can log in or log out of the embedded HTTP web server.
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.
Settings	This shows detail and complete SME network settings for base station(s), HTTP/DNS/DHCP/TFTP server, SIP server, etc.
Debug Log	Overall network related events or logs is 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.

9.2 Extensions

In this section, we describe the different parameters available whenever the administrator is creating an extension for handset.

Parameter	Description
Extension	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/ Password	Username: SIP authentication username Password: SIP authentication password. Permitted value(s): 8-bit string length

Display Name	Human readable name used for reference purposes on the HTTP web interface.(This does not display on handset) Permitted value(s): 8-bit string length
Mailbox Name/ Number	Name of centralised system used to store phone voice messages that can be retrieved by recipient at a later time. Valid Input(s): 8-bit string length character (Latin characters for the Name and positive integer for the Number) Note: Mailbox Number parameter is available only when its enabled from SIP server.
Server	DNS or IP address of SIP server or Server of SME VoIP Service provider. Valid Input(s): AAA.BBB.CCC.DDD or URL e.g. www.sip-sme.com
Forwarding Unconditional Number	Number to which incoming calls must be re-routed to irrespective of the current state of the SIP node or handset. Note: Feature must be enabled in the SIP server before it can function in the network
Forwarding No Answer Number	Number to which incoming calls must be re-routed to when there is no response from the SIP end node Note: Feature must be enabled in the SIP server before it can function in the network
Forwarding On Busy Number	Number to which incoming calls must be re-routed to when SIP node is busy. Note: Feature must be enabled in the SIP server before it can function in the network

Add extension

Extension:
 Authentication User Name:
 Authentication Password:
 Display Name:
 Mailbox Name:
 Server:
 Forwarding Unconditional Number:
 Forwarding No Answer Number: 90 s
 Forwarding on Busy Number:

9.3 Servers

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

Parameter	Description
NAT Adaption	To ensure all SIP messages goes directly to the NAT gateway in the SIP aware router. NAT Adaption option should be "No" or otherwise choose "Yes" Possible value(s): Yes, No
Registrar	SIP Server proxy DNS or IP address Permitted value(s): AAA.BBB.CCC.DDD:<Port-Number> or <URL>:<Port-####> Note: Specifying the Port Number is optional.
Outbound Proxy	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-####> Examples: "192.168.0.1", "192.168.0.1:5062", "nat.company.com" and "sip:nat@company.com:5065".
Re-registration time	The window period (in seconds) when base stations SIP registers with SIP server. Permitted value(s): Positive integer
Keep Alive	This directive defines the window period (30 secs.) to keep opening the port of relevant NAT-aware router(s), etc. Valid Input(s): Enable, Disable
DTMF Signalling	Conversion of decimal digits (and '*' and '#') into sounds that share similar characteristics with voice to easily traverse networks designed for voice Valid Option(s) In band: Meta-data (e.g.: tone digits) and control information sent in the same voice band, using the same VoIP codec as the human voice (e.g. G.711, G.729, etc.) SIP INFO: Carries application level data along SIP signalling 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.
Codec Priority	Defines the codec priority that base stations uses for audio compression and transmission. Possible Option(s): PCMU, PCMA, iLBC.

Servers

Server 1
192.168.50.77

Server 2:

[Add server](#)

[Remove server](#)

Server 2:

NAT Adaption:

Registrar:

Outbound Proxy:

Re-registration time:

Keep Alive:

DTMF Signalling:

Codec Priority:

Server 2 recently added, press save to save changes

9.4 Network

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

9.4.1 IP Settings

Parameter	Description
DHCP/Static IP	If DHCP is enabled, the device automatically obtains TCP/IP parameters. Possible value(s): Static, DHCP DHCP: IP addresses are allocated automatically from a pool of leased address. Static IP: IP addresses are manually assigned by the network administrator. If the user chooses DHCP option, the other IP settings or options are not available.
IP Address	32-bit IP address of device (e.g. base station). 64-bit IP address will be supported in the future. Permitted value(s): AAA.BBB.CCC.DDD
Subnet Mask	Is device subnet mask. Permitted value(s): AAA.BBB.CCC.DDD This is a 32-bit combination used to describe which portion an IP address refers to the subnet and which part refers to the host. A network mask helps users know which portion of the address identifies the network and which portion of the address identifies the node.
Default Gateway	Device's default network router/gateway (32-bit). Permitted value(s): AAA.BBB.CCC.DDD e.g. 192.168.50.0 IP address of network router that acts as entrance to other network. This device

	provides a default route for TCP/IP hosts to use when communicating with other hosts on hosts networks.
DNS (Primary)	Main server to which a device directs Domain Name System (DNS) queries. Permitted value(s): AAA.BBB.CCC.DDD or <URL> 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.
DNS (Secondary)	This is an alternate DNS server.

Screenshot



IP settings

DHCP/Static IP:

IP Address:

Subnet Mask:

Default gateway:

DNS (primary):

DNS (secondary):

9.4.2 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.

Parameter	Description
VLAN id	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.
VLAN User Priority	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)

Screenshot



VLAN Settings

VLAN Id:

VLAN User Priority:

9.4.3 Boot Server Options

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

Screenshot

Boot Server Options

Boot Server DHCP Option:

Customer DHCP Option:

Option Content Type:

9.4.4 NAT Settings

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

Parameter	Description
Enable RPORT	Define whether RPORT should be used in SIP messages. Enabled by setting to Yes and disable by choosing No Permitted values: Yes, No. This option is disabled by default.
Keep alive time	This defines the frequency of how keep-alives are sent to maintain NAT bindings. Permitted values: Positive integer default is 90, unit is in seconds

NAT Settings

Enable RPORT:

Keep alive time:

9.4.5 SIP/RTP Settings

These are some definitions of SIP/RTP Server settings:

Parameter	Description
Local SIP port	SIP server port number reserved for a specific customer by the network operator. Port used for first user agent (UA) instance. Succeeding UA's will get succeeding ports. Permitted values: Port number default 5060.
SIP ToS/QoS	Priority of call control signalling 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. Permitted values: Positive integer default is 104
RTP port	Usually the first RTP port to use for RTP audio streaming. Permitted values: Port number default 50004 (depending on the setup).
RTP port range	The number of ports that can be used for RTP audio streaming. Permitted values: Positive integers, default is 20
RTP TOS/QoS	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. - o Bit 7..5 defines precedence. - o Bit 4..2 defines Type of Service. - o Bit 1..0 are ignored. Setting all three of bit 4..2 will be ignored. Permitted values: Positive integer default is 160

Screenshot

SIP/RTP Settings

Local SIP port:	5060
SIP ToS/QoS:	104
RTP port:	50004
RTP port range:	40
RTP ToS/QoS:	184

9.5 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.

Parameter	Description
Title name of the web site	This option is optional. It indicates the title that should appear at the top window of the browser i.e. <Enter_title_here> -Browser_name By default: "SME VoIP Configuration"
Configuration server address	Server/device that provides configuration file to base station. Type: DNS or IP address Permitted value(s): AAA.BBB.CCC.DDD (Currently only IPv4 are supported) or URL (e.g.: firmware.rtx.net)
Management Transfer Protocol	The protocol assigned for configuration file and firmware downloads (or uploads) Valid Input(s): HTTP, TFTP Note: Choose TFTP if Bases/handsets firmware are updated over-air via TFTP Server
HTTP Management upload script	The folder location or directory path that contains the configuration file 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 password	Password that should be entered in order to have access to the configuration server. Permitted value(s): 8-bit string length
Upload of Debug Log	Enable this to save low level system debug messages in the configuration server. Further, the user can specify the kind of contents that should be saved. Choose Boot Log option to save only boot related messages (i.e. logs during start up of the system). Choose Everything option if you want to save all debug logs including boot logs. Valid Input: Disable, Boot Log, Everything The Debug log will be saved in the file format <Time_Stamp>b.log in the TFTP server as specified in the upload script. The upload script is a routine enabled at the TFTP/HTTP server.
Upload of SIP Log	Enable this option to save low level SIP debug messages in the configuration server. Enable by choosing the option: Everything . Valid Input: Disable, Everything

	The SIP logs are saved in the file format: <MAC_Address><Time_Stamp>SIP.log
Trace Server	Enable this option to save mail traces. Mail server traces are low level internal log messages or traces used for debug purposes by RTX engineers. Valid Input: Disable, Enable
Trace Server IP Address	The trace server uses the same address as the configuration server. Permitted value(s): AAA.BBB.CCC.DDD (Currently only IPv4 are supported) or url (e.g.: firmware.rtx.net)

Management Settings

Title name of the web site:

Configuration server address:

Management Transfer Protocol:

HTTP Management upload script:

HTTP Management password:

Upload of Debug Log:

Upload of SIP Log:

Trace Server:

Trace Server IP Address:

9.6 Firmware Update Definitions

In this page, the system administrator can configure how base stations and SIP nodes upgrade/downgrade to the relevant firmware.

Parameter	Description
Firmware update server address	IP address or DNS of firmware update files source Valid Inputs: AAA.BBB.CCC.DDD or <URL> Example: firmware.rtx.net or 10.10.104.41
Firmware path	Location of firmware on server (or firmware update server path where firmware update files are located). Example: /East_Fwu Note: Must begin with (/) slash character
Required Version	Version of firmware to be upgraded (or downgraded) on Base station or handset. Base units are referred to as gateways over here. Valid Input(s): 8-bit string length. E.g. 0034, etc.

Firmware Update Settings

Firmware update server address:

Firmware path:

Update handsets

Handset Type	Required version
UXP1240H HW ver 00	51
UXP1240H	51

Update gateways

☒ Update this gateway only

☐ Update all gateways

Required version

9.7 Time Server

In this section, we describe the different parameters available in the Time Server menu. The Time server supplies the time is used in the debug logs and SIP trace information pages. It is also used to determine when to check for new configuration and firmware files.

NOTE:

You should set the time server for multi-cell configuration (mandatory). It is not necessary to set the time server for standalone base stations (optional).

Parameter	Description
Time Server	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.
Time server refresh interval	The window time in seconds within which time server refreshes. Valid Inputs: positive integer
Time Zone	Refers to local time in GMT or UTC format. Min: -12:00 Max: +13:00
Daylight Saving Time (DST)	Enter the start and stop dates if you select Automatic. The system administrator can Enable or Disable DST manually.
DST Fixed By Day	You determine when DST actually changes. Choose the relevant date or day of the week, etc. from the drop down menu.
DST Start Month	Month that DST begins Valid Input(s): Gregorian months (e.g. January, February, etc.)
DST Start Date	Numerical day of month DST comes to effect when DST is fixed to a specific date

	Valid Inputs: positive integer
DST Start Time	DST start time in the day Valid Inputs: positive integer
DST Start Day of Week	Day within the week DST begins
DST Start Day of Week, Last in Month	Specify the week that DST will actually start.
DST Stop Month	The month that DST actually stops.
DST Stop Date	The numerical day of month that DST turns off. Valid Inputs: positive integer (1 to 12)
DST Stop Time	The time of day DST stops Valid Inputs: positive integer (1 to 12)
DST Stop Day of Week Last in Month	The week within the month that DST will turn off.

Time Settings

Time server: 192.168.50.3
Time server refresh interval: 3
Timezone: +1:00
Daylight Saving Time (DST): Automatic
DST Fixed By Day: Use Month and Day of Week
DST Start Month: March
DST Start Date: 1
DST Start Time: 2
DST Start Day of Week: Sunday
DST Start Day of Week Last in Month: Last In Month
DST Stop Month: October
DST Stop Date: 1
DST Stop Time: 2
DST Stop Day of Week: Sunday
DST Stop Day of Week Last in Month: Last In Month

Save Cancel

9.8 Multi-cell Parameter Definitions

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

9.8.1 Settings for Base Unit

Description of Settings for Specific Base units is as follows:

Parameter	Description
Multi cell system	Enable this option to allow the Base unit to be set in multi-cell mode (can be set either as master or slave in the multi-cell chain system – refer to MAC-units in

	Chain section for details). Valid Inputs: Enable, Disable
System chain ID	This is an identifier (in string format e.g. 2275) that is unique for a specific multi-cell system. Note: There can be several multi-cell systems in SME network. Up to 7 levels of base stations chains are permitted in a typical setup. Please refer to accompanied document [2] for further details and description. Valid Input: 16 bit String length
Synchronization time (s)	This specifies the period in seconds when elements/nodes (e.g. Base units) in a specific Multi-cell should synchronise to each other.
Multi cell debug	Enable this feature, if you want the system to catalogue low level multi-cell debug information or traces.

Multi Cell settings

Settings for this unit

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

Multi cell system:

System chain ID:

Synchronization time (s):

Multi cell debug:

Save

Cancel

9.8.2 DECT System Settings

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

Parameter	Description
DECT system RFPI	This is a radio network identity accessed by all Base units in a specific multi-cell system. It composed of 5 octets. It is actually 5 different variables combined together. RFPI Format: XX XX XX XX XX (where XX are HEX values) Note: Only type e.g. 11 6E 60 49 04 the system reformats as 0x11 0x6E 0x60 0x49 0x04 Access Rights Class (ARC): Defines network identity structure used by terminals especially in multi-cell environment. Fixed/default Value=1 (Private multi-cell system). RFPI: 1X XX XX XX XX Equipment Installer's code (EIC): Code that allows terminals to distinguish between separate DECT networks. Example RTX_EIC: 0x16E6 (May change in the future) RFPI: 11 6E 6X XX XX Fixed Part Number(FPN): Is a geographically unique identity transmitted to DECT networks to help PP distinguish between base station communications in different cells/multi-cell systems. E.g. FPN: 0x049 RFPI: 11 6E 60 49 XX

	Location Area Length (Lal): A unique code sent to the terminal during location registration to determine the size of the location or cell area. Type: 8-bit value (from 0x00 to 0xFF). E.g Lal=0x04 RFPI: 11 6E 60 49 04
Auto configure DECT sync source tree	Enable this to allow the network to automatically synchronise the multi-cell chain/tree. (Not available in some base station firmware(s)). Permitted Inputs: Enable, Disable

DECT system settings

These settings are DECT settings for the system.

DECT system RFPI:

Auto configure DECT sync source tree

9.8.3 SIP System Settings

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

Parameter	Description
## of SIP accounts before distributed load	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. Note: A maximum of 8 simultaneous calls can be routed through each Base units in a multi-cell setup. Permitted Input: Positive Integers (e.g. 6)
SIP Support for multiple registrations per account	Enable this option so it is possible to use 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. Note: Choose Yes when the SIP server supports this feature otherwise choose No for the Sip server does not support this feature. Permitted Input: Yes, No

SIP system settings

These settings are SIP settings for the system.

Number of SIP accounts before distributed load:

SIP Server support for multiple registrations per account: (used for roaming signalling)

9.8.4 MAC-units in Chain

The definitions for various parameters settings of various chain levels for a typical multi-cell system.

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)
MAC Address	Contains the hardware Ethernet MAC address of the base station. It varies from Base station to Base stations.
Version	Base station current firmware version. Permitted Output: positive Integers (e.g. 34)
Status	Current Base station behaviour in the SME network. Possible Outputs Connected: The relevant Base station(s) is online in 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	The administrator should choose the relevant “multi cell chain” level its wants a specific Base unit be placed. Maximum number of “multi-cell chain” levels is 6.
Dect Property	Base station characteristics in connection to the current multi cell network. Possible Output(s) Master: Main Base station unto which all other nodes in the chain synchronises 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 Free Running: A locked Base unit that suddenly lost synchronisation to the Master. Unknown: No current connection information from specific Base unit

MAC-units in chain

	ID	RPN	Version	MAC address	IP address	IP Status	DECT sync source	DECT Property
☐	0	00	51	00:08:7B:D7:91:6E	<u>192.168.10.106</u>	This unit	0 - RPN: 00 ▾	Master
☐	1	04	51	00:08:7B:D7:91:74	<u>192.168.10.105</u>	Connected	0 - RPN: 00 ▾	Locked

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

With selected: [Remove from chain](#)

9.9 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:

- 1) Using the SME VoIP Configuration interface to make changes. Each page of the HTTP web interface is a template for which the user can customise settings in the configuration file.

- 2) Retrieving the relevant configuration file from the TFTP and modify and enter new changes. This should be done with an expert network administrator.
- 3) 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=NUMBER FP V0054
%GMT_TIME_ZONE%:16
%COUNTRY_VARIANT_ID%:18
%FWU_POLLING_ENABLE%:0
%FWU_POLLING_MODE%:0
%FWU_POLLING_PERIOD%:86400
%FWU_POLLING_TIME_HH%:3
%FWU_POLLING_TIME_MM%:0
%DST_ENABLE%:2
%DST_FIXED_DAY_ENABLE%:0
%DST_START_MONTH%:3
%DST_START_DATE%:1
....
....
```

9.10 Debug Logs

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
```

9.11 SIP Logs

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

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

10 Firmware Upgrade Management

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

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

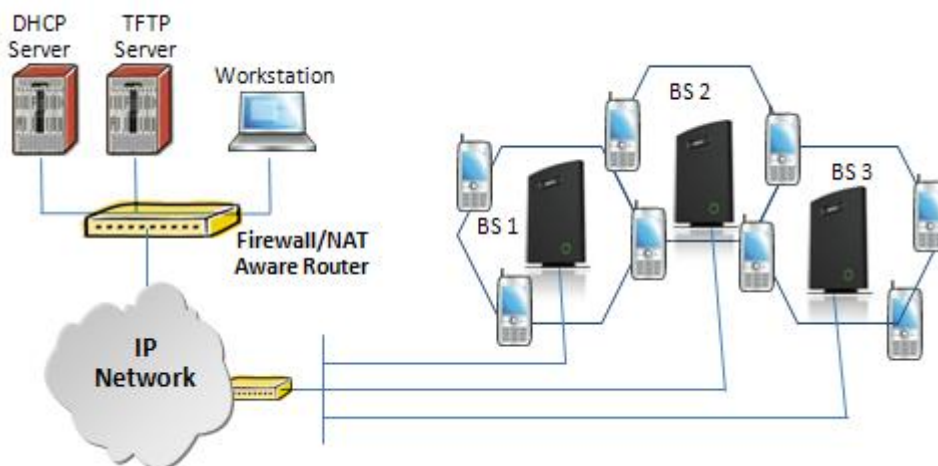
- 1) Verify whether the new firmware package is compatible with the device.
- 2) Upgrade the firmware on the device to the new firmware
- 3) Roll back the firmware on the device to the previous firmware version (where necessary)

10.1 Network Dimensioning

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

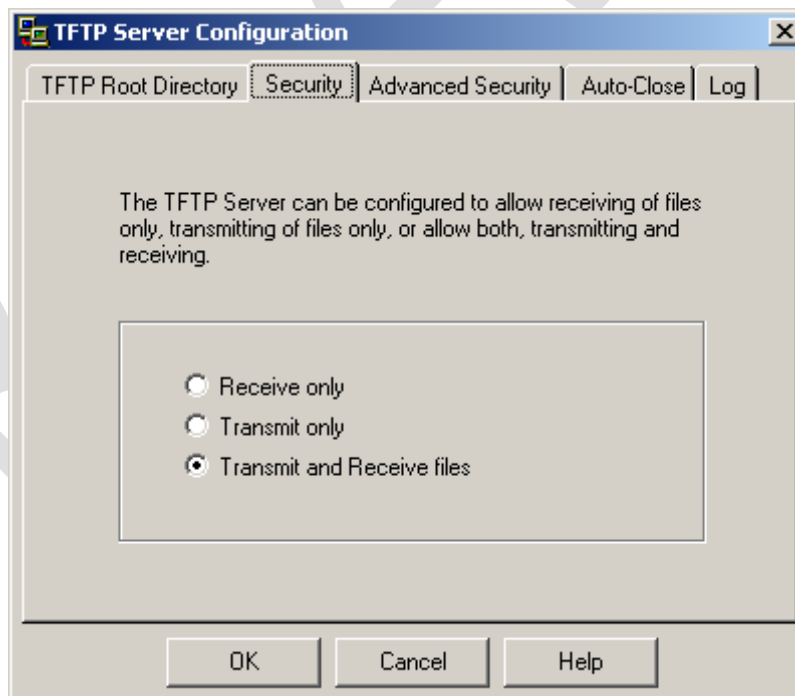
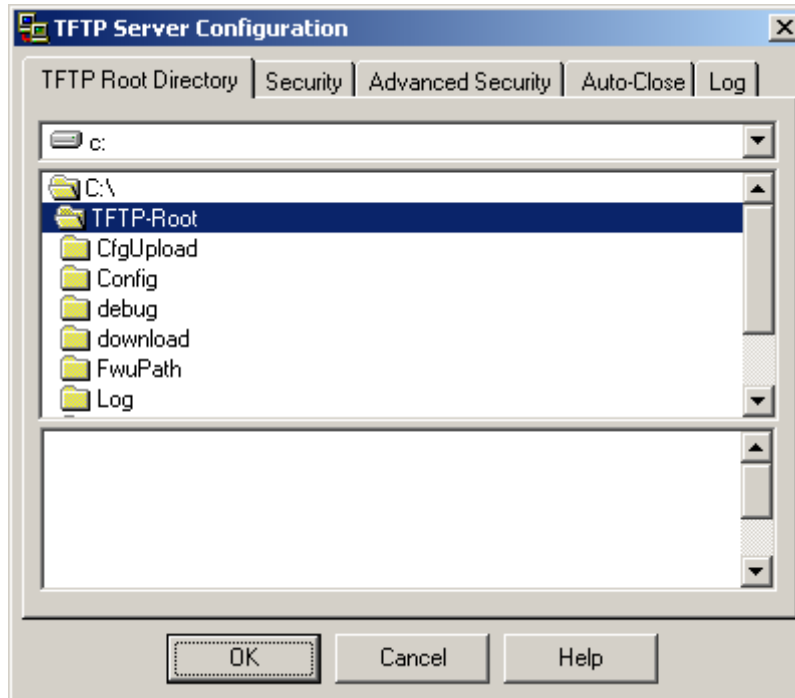
The minimum hardware and software components that are required to be able update via TFTP include the following (but not limited to):

- 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



10.2 TFTP Configuration

This section illustrate 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.



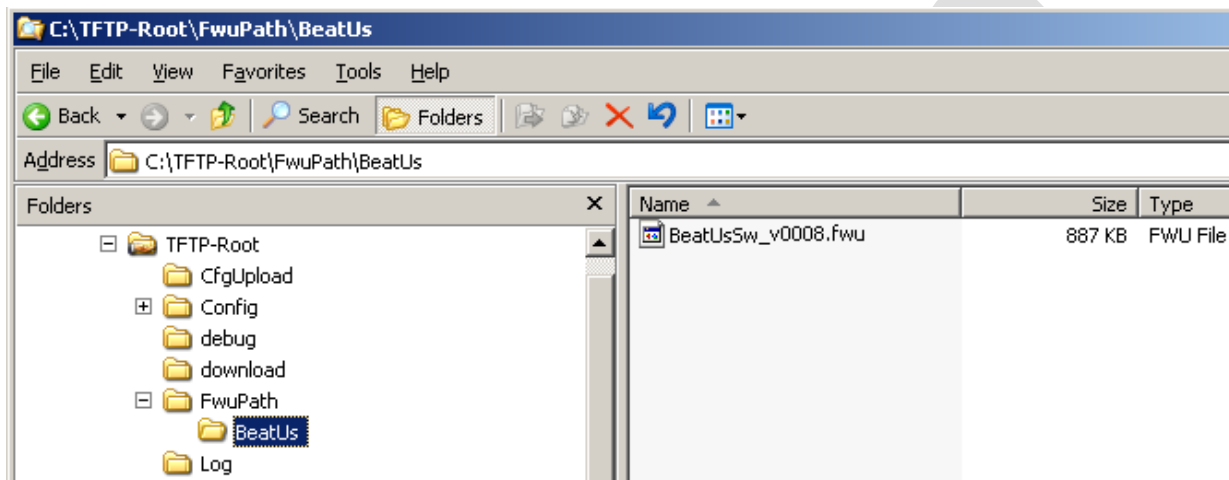
10.3 Create Firmware Directories

Within the same TFTP Server Interface do the following:

- STEP 1** Make a folder named “**BeatUs**” in the TFTP-Root and place the fwu file(s)/(Firmware) in this folder. The base firmware must be renamed to “**BeatUsSw_v00xx.fwu**”.
- STEP 2** 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)
- The firmware directory or path should be \<Server>\<FwuPath>\<BeatUs>, where <Server> is the root directory of the server (e.g. C:\TFTP-Root) and <FwuPath> is a folder within the <Server> that contains the **BeatUs** directory.

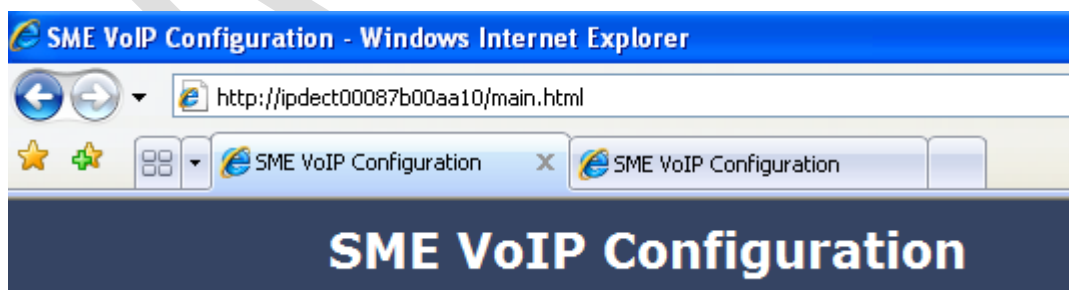
IMPORTANT:

The **BeatUs** directory name cannot be changed.



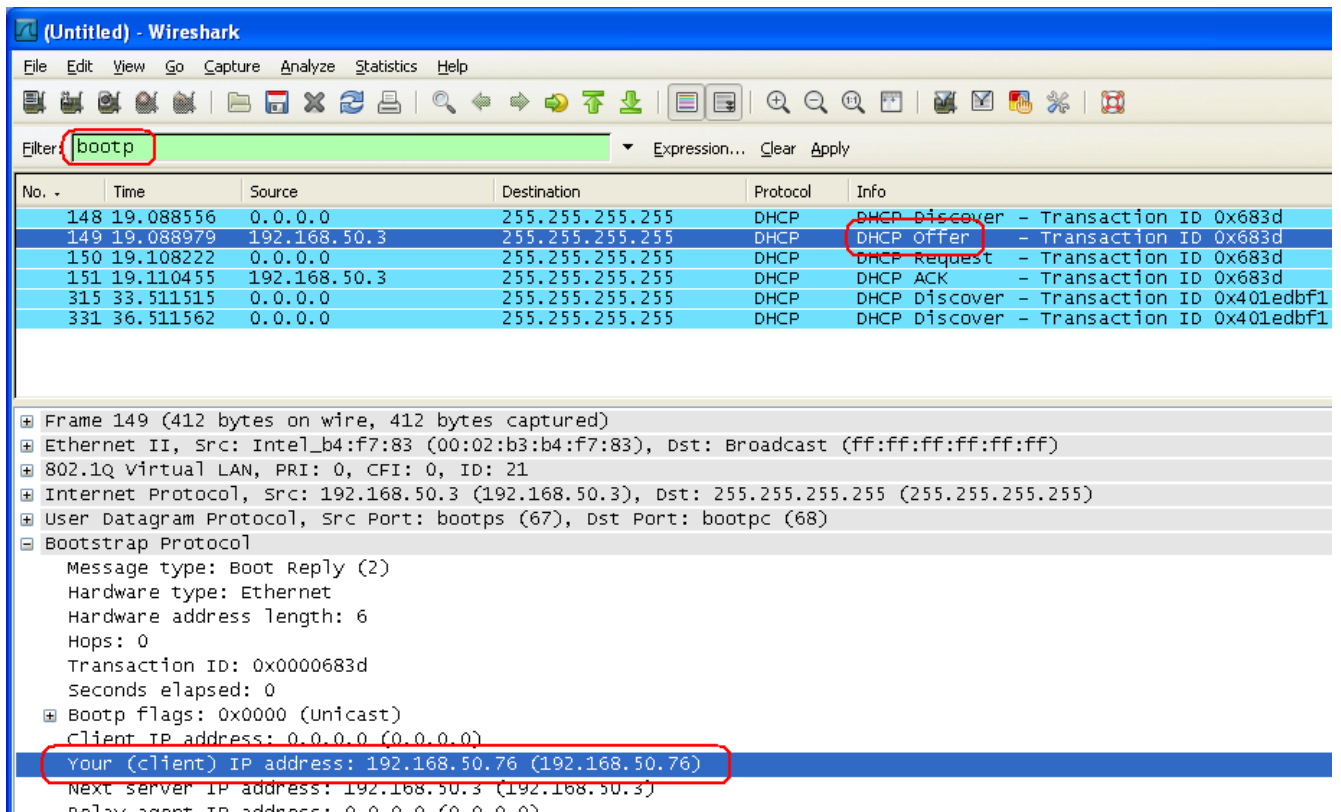
10.4 Login to Base SME Configuration Interface

- STEP 3** Connect the Base station to a private network via standard Ethernet cable (CAT-5).
- STEP 4** Open any standard browser and enter the address:
<http://ipdetect<MAC-Address-Base-Station>>
 e.g. <http://ipdetect00087B00AA10>. This will retrieve the HTTP Web Server page from the base station with hardware address 00087B00AA10.



- STEP 5** You can also use an IP/network protocol analyser e.g. Wireshark (freeware program) to identify which IP the base has received.

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



(Untitled) - Wireshark

File Edit View Go Capture Analyze Statistics Help

Filter: **bootp** Expression... Clear Apply

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

Frame 149 (412 bytes on wire, 412 bytes captured)

Ethernet II, Src: Intel_b4:f7:83 (00:02:b3:b4:f7:83), Dst: Broadcast (ff:ff:ff:ff:ff:ff)

802.1Q Virtual LAN, PRI: 0, CFI: 0, ID: 21

Internet Protocol, Src: 192.168.50.3 (192.168.50.3), Dst: 255.255.255.255 (255.255.255.255)

User Datagram Protocol, Src Port: bootps (67), Dst Port: bootpc (68)

Bootstrap Protocol

Message type: Boot Reply (2)

Hardware type: Ethernet

Hardware address length: 6

Hops: 0

Transaction ID: 0x0000683d

Seconds elapsed: 0

Bootp flags: 0x0000 (Unicast)

Client IP address: 0.0.0.0 (0.0.0.0)

Your (client) IP address: 192.168.50.76 (192.168.50.76)

Next server IP address: 192.168.50.3 (192.168.50.3)

Relay agent IP address: 0.0.0.0 (0.0.0.0)

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



Connect to ipdetect00087b00aa10

The server ipdetect00087b00aa10 at requires a username and password.

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

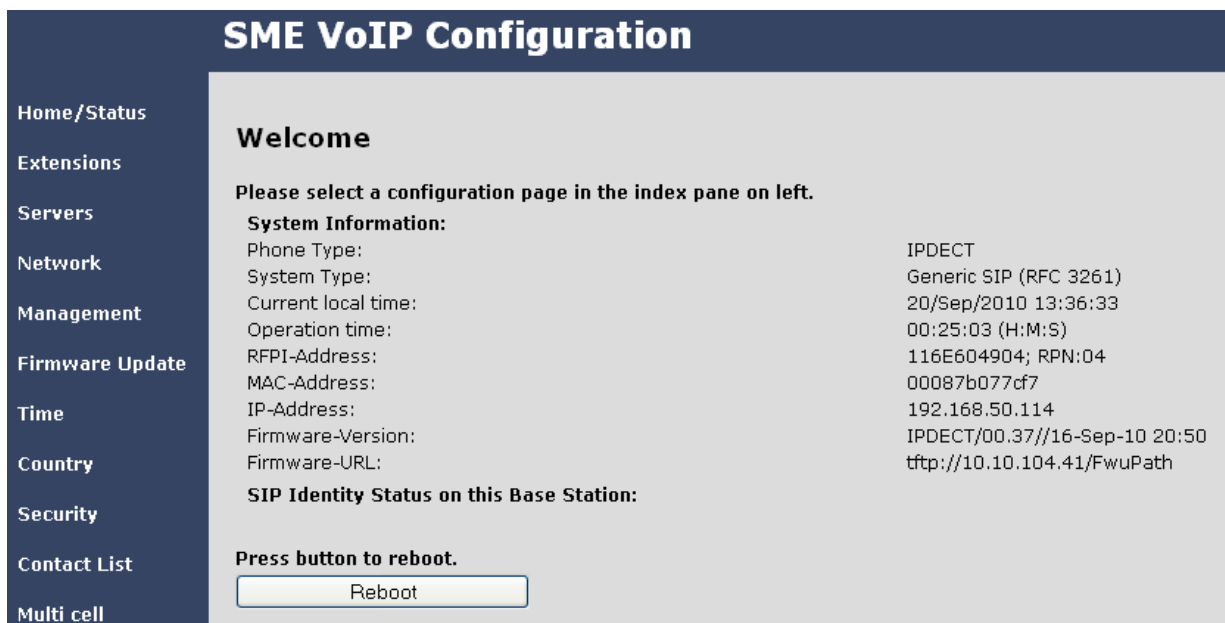
User name:

Password:

☐ Remember my password

OK Cancel

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



SME VoIP Configuration

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

Welcome

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

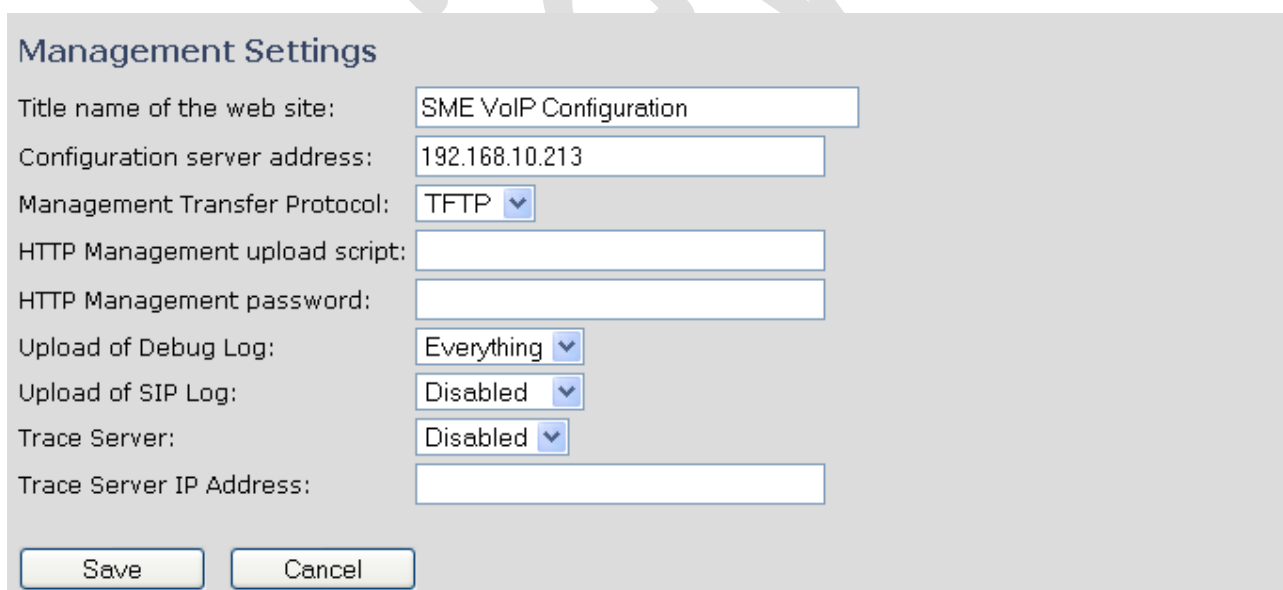
System Information:

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

SIP Identity Status on this Base Station:

Press button to reboot.

STEP 8 Click on **Management** URL. Enter the relevant Management server information in the system. Select the Management transfer protocol **"TFTP"** drop down menu.



Management Settings

Title name of the web site:

Configuration server address:

Management Transfer Protocol:

HTTP Management upload script:

HTTP Management password:

Upload of Debug Log:

Upload of SIP Log:

Trace Server:

Trace Server IP Address:

10.5 Firmware Update Settings

STEP 9 Scroll down and Click on **Firmware Update** url link in the **SME VoIP Configuration Interface** to view the **Firmware Update Settings** page.

Firmware Update Settings

Firmware update server address:

Firmware path:

Update handsets

Handset Type Required version

Update gateways

☒ Update this gateway only
☐ Update all gateways

Required version

Parameters	Description
Firmware Update Settings	
Firmware update server address	This is the IP address of server where the firmware is located. Currently, only 32-bit is supported (i.e. IPv4 type – <aaa.bbb.ccc.ddd>)
Firmware path	The firmware is found at the \<Server>\<FwuPath>\BeatUs\ directory found in the FTP or TFTP server. Note: Either / or \ can be used The <Server> is the root directory of the server created by the administrator and should <u>NOT</u> be specified. The <FwuPath> is a folder within the <Server> that contains the BeatUs directory. This MUST be specified. By default the ...\\BeatUs is hard-coded into the firmware. Therefore it should not be specified in the firmware path. Example of firmware path is \\HQ_Office, \\South_Office, or \\FwuPath, etc. in that manner.
Update Gateways/Handsets	
Required Version	This is 8-bit value. The firmware filename is BeatUsSw_v00XX.fwu . The administrator has to enter a numerical value XX or 00XX , where XX is a positive integer.

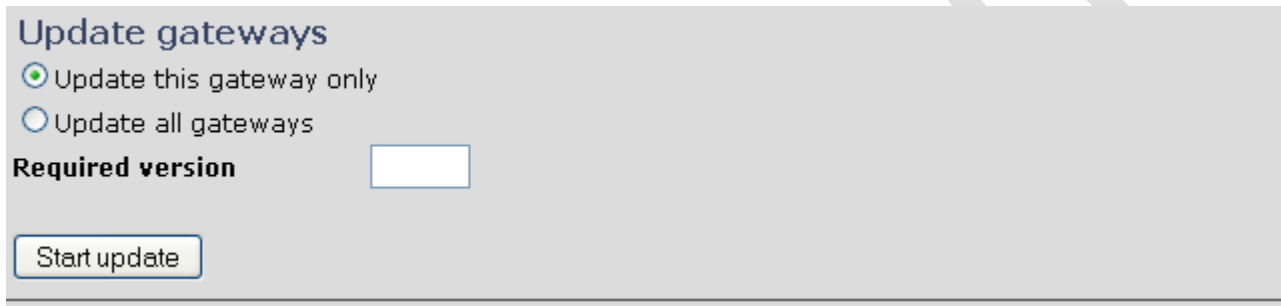
STEP 10 Click on **Firmware Update** URL. On the **Firmware Update Settings** page enter the relevant parameters as described in the table above.

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

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

10.6 Base Station(s) Firmware Upgrade

STEP 11 On the **Firmware Update Settings** page > scroll down to the **Update Gateways** section > Enter the relevant firmware version (e.g. **11**) of the base station to upgrade or to downgrade. It is possible to upgrade a single base station and/or several base stations > the admin should choose right the radio button.

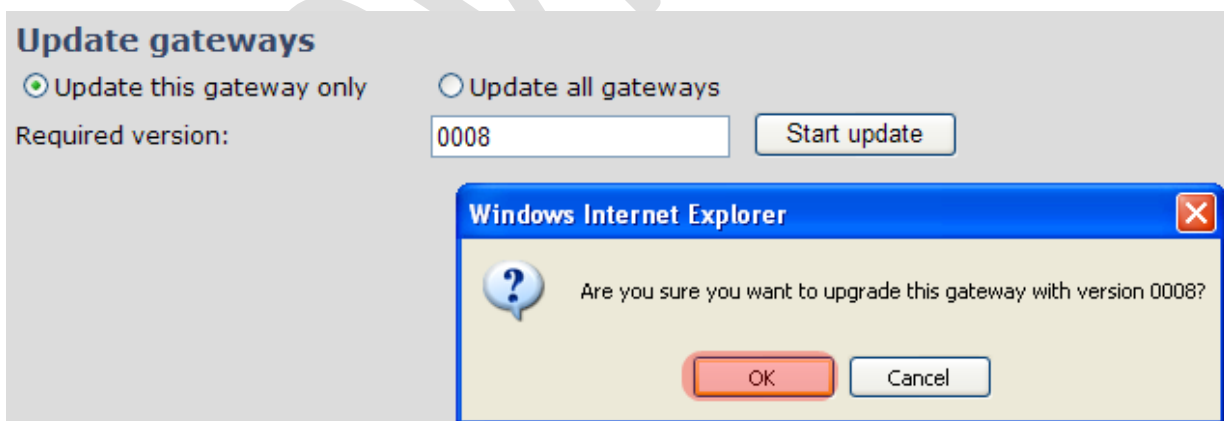


Update gateways

☒ Update this gateway only
☐ Update all gateways

Required version

STEP 12 Still on the same **Update Gateway** section > choose **Start update** button > select **OK** button from the dialog window to start the update/downgrade procedure. The relevant base station(s) will automatically reboot and retrieve the firmware specified from the server and update itself accordingly.



Update gateways

☒ Update this gateway only ☐ Update all gateways

Required version:

Windows Internet Explorer

Are you sure you want to upgrade this gateway with version 0008?

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

10.7 Handset (s) Firmware Upgrade

STEP 13 Scroll down to **Update handsets** section on the **Firmware Update Settings** page > Enter the relevant handset firmware (e.g. 11) to upgrade or downgrade > press **Start update** button > Click on **OK** button from the dialog window to initialize the process of updating all handsets in the private network.

As at the time of documenting this chapter, two different handset hardware module exist i.e. **UXP1240H HW ver 00** and the native hardware **UXP1240H**.

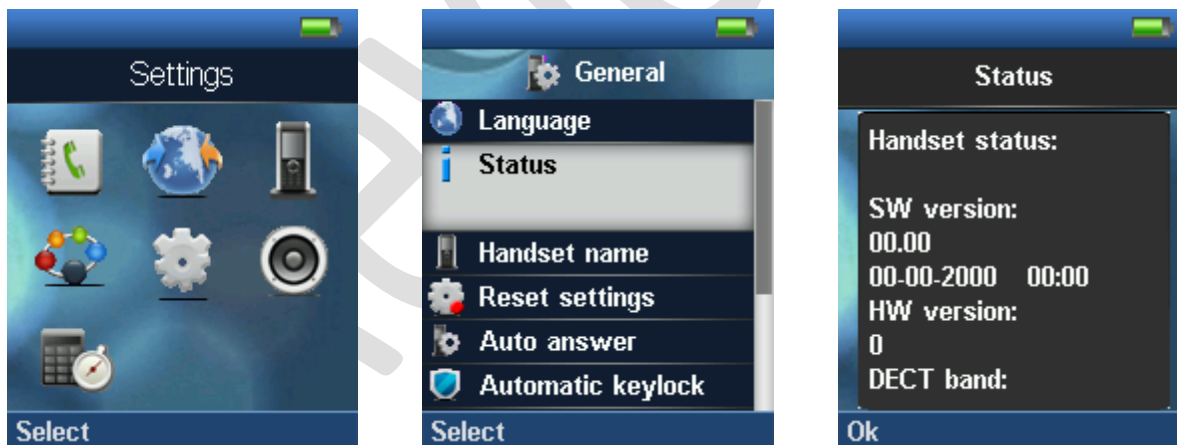
Update handsets

Handset Type	Required version
UXP1240H HW ver 00	51
UXP1240H	51

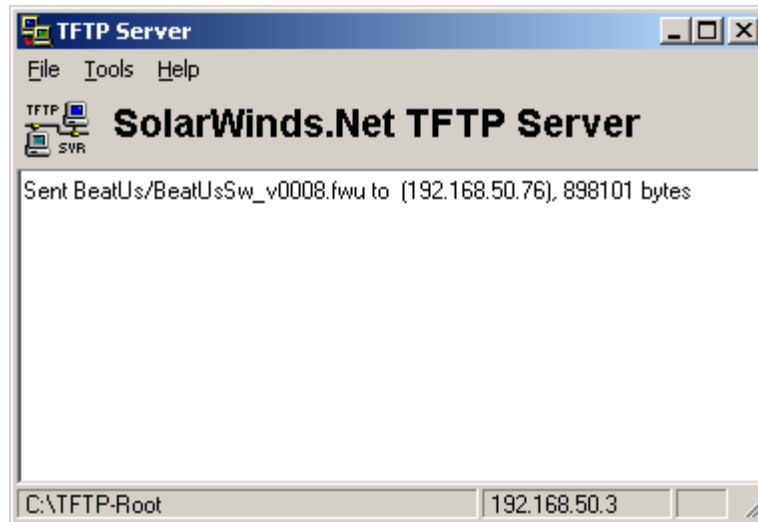
Save

10.8 Verification of Firmware Upgrade

STEP 14 From the Handset **Menu** navigate to **Settings** > Scroll down to **Status** this will list information regarding Base station and Handset firmware versions.



STEP 15 Now the download should be initiated and it should be stated in the log window of the TFTP server:



STEP 16 During the download, the Wireshark shows the download as shown below:

No.	Time	Source	Destination	Protocol	Info
203	26.639841	192.168.50.79	192.168.50.3	TFTP	Read Request, File: /BeatUs/BeatUsSw_v0008.fwu
204	26.654789	192.168.50.3	192.168.50.79	TFTP	Data Packet, Block: 1
205	26.660174	192.168.50.79	192.168.50.3	TFTP	Acknowledgement, Block: 1
206	26.660610	192.168.50.3	192.168.50.79	TFTP	Data Packet, Block: 2
207	26.663632	192.168.50.79	192.168.50.3	TFTP	Acknowledgement, Block: 2
208	26.663965	192.168.50.3	192.168.50.79	TFTP	Data Packet, Block: 3
209	26.667229	192.168.50.79	192.168.50.3	TFTP	Acknowledgement, Block: 3
210	26.667546	192.168.50.3	192.168.50.79	TFTP	Data Packet, Block: 4
211	26.670955	192.168.50.79	192.168.50.3	TFTP	Acknowledgement, Block: 4
212	26.671270	192.168.50.3	192.168.50.79	TFTP	Data Packet, Block: 5
213	26.674694	192.168.50.79	192.168.50.3	TFTP	Acknowledgement, Block: 5
214	26.675007	192.168.50.3	192.168.50.79	TFTP	Data Packet, Block: 6
215	26.678754	192.168.50.79	192.168.50.3	TFTP	Acknowledgement, Block: 6
216	26.679280	192.168.50.3	192.168.50.79	TFTP	Data Packet, Block: 7
217	26.682781	192.168.50.79	192.168.50.3	TFTP	Acknowledgement, Block: 7
218	26.683110	192.168.50.3	192.168.50.79	TFTP	Data Packet, Block: 8
219	26.686694	192.168.50.79	192.168.50.3	TFTP	Acknowledgement, Block: 8
220	26.687023	192.168.50.3	192.168.50.79	TFTP	Data Packet, Block: 9
221	26.693048	192.168.50.79	192.168.50.3	TFTP	Acknowledgement, Block: 9
222	26.693400	192.168.50.3	192.168.50.79	TFTP	Data Packet, Block: 10
223	26.698878	192.168.50.79	192.168.50.3	TFTP	Acknowledgement, Block: 10
224	26.699199	192.168.50.3	192.168.50.79	TFTP	Data Packet, Block: 11
225	26.705615	192.168.50.79	192.168.50.3	TFTP	Acknowledgement, Block: 11
226	26.705931	192.168.50.3	192.168.50.79	TFTP	Data Packet, Block: 12
227	26.712233	192.168.50.79	192.168.50.3	TFTP	Acknowledgement, Block: 12
228	26.712540	192.168.50.3	192.168.50.79	TFTP	Data Packet, Block: 13

Frame 203 (81 bytes on wire, 81 bytes captured)
 # Ethernet II, Src: RtxTelec_07:7c:73 (00:08:7b:07:7c:73), Dst: Intel_b4:f7:83 (00:02:b3:b4:f7:83)
 # 802.1Q Virtual LAN, PRI: 0, CFI: 0, ID: 21
 # Internet Protocol, Src: 192.168.50.79 (192.168.50.79), Dst: 192.168.50.3 (192.168.50.3)
 # User Datagram Protocol, Src Port: 60769 (60769), Dst Port: tftp (69)
 # Trivial File Transfer Protocol

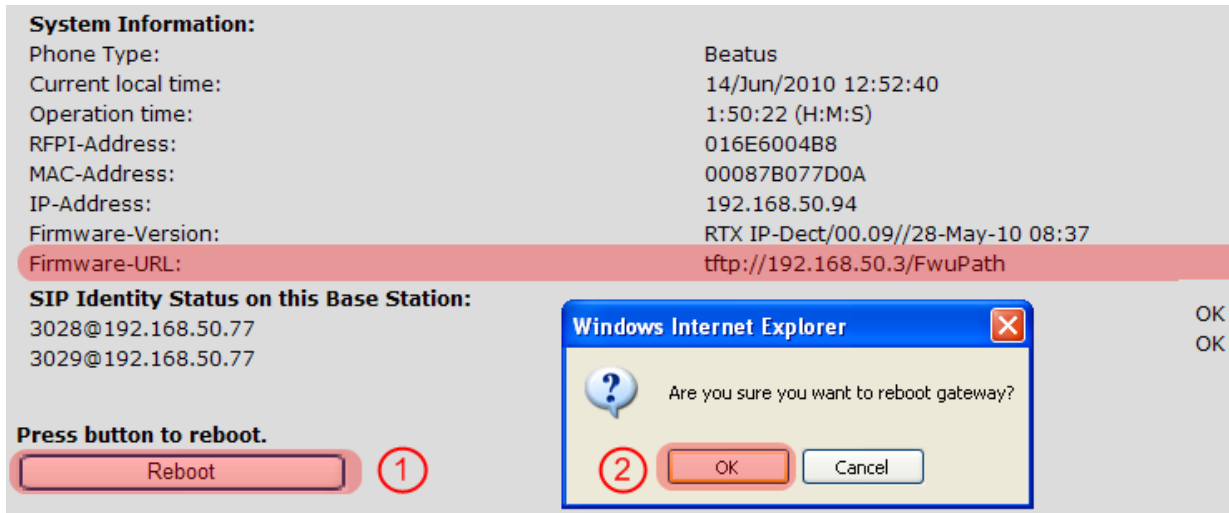
10.9 Reboot the Base station(s)

STEP 17 In principle the base station(s) should reboot automatically when the **Start update** button is selected > to begin the firmware update procedure.

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

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

tftp://192.68.50.1/FwuPath



System Information:

Phone Type:	Beatus
Current local time:	14/Jun/2010 12:52:40
Operation time:	1:50:22 (H:M:S)
RFPI-Address:	016E6004B8
MAC-Address:	00087B077D0A
IP-Address:	192.168.50.94
Firmware-Version:	RTX IP-Dect/00.09//28-May-10 08:37
Firmware-URL:	tftp://192.168.50.3/FwuPath

SIP Identity Status on this Base Station:

3028@192.168.50.77
3029@192.168.50.77

Press button to reboot.

①

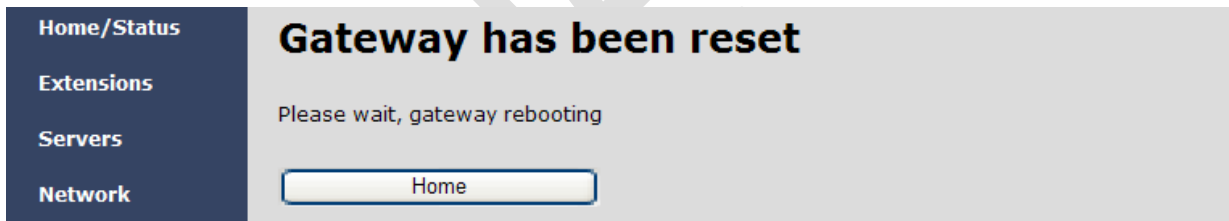
Windows Internet Explorer

Are you sure you want to reboot gateway?

②

OK
OK

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



Home/Status

Gateway has been reset

Please wait, gateway rebooting

STEP 18 Wait about 3-5 minutes, Reboot the base/gateway.

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

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

Reviewed

11 Registration Management - Handset

In this chapter we briefly describe how to add server and register handsets in the SME VoIP Network.

11.1 Hardware required

This section describes what hardware is needed to execute the guideline. You need the following to perform a registration of a handset to a base station (gateway):

- 1 x base station
- 1 x handset
- 1 x Ethernet cable (PoE)
- 1 x PC connected to the LAN, VLAN or WAN



Plug the Ethernet cable into the base station and connect the other end of the cable to your network (LAN, VLAN or WAN). The base station is powered via the Ethernet cable (PoE). PC must be connected to the same network as the base station.

If your network doesn't support PoE (Power over Ethernet), the a PoE adaptor must be used.



11.2 Software required equipment

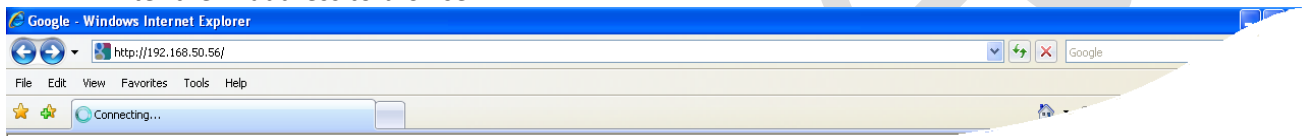
This section describes what software is needed. You will need the following to access the web configuration interface on the base station:

- Any standard browser e.g. Windows IE installed on the PC

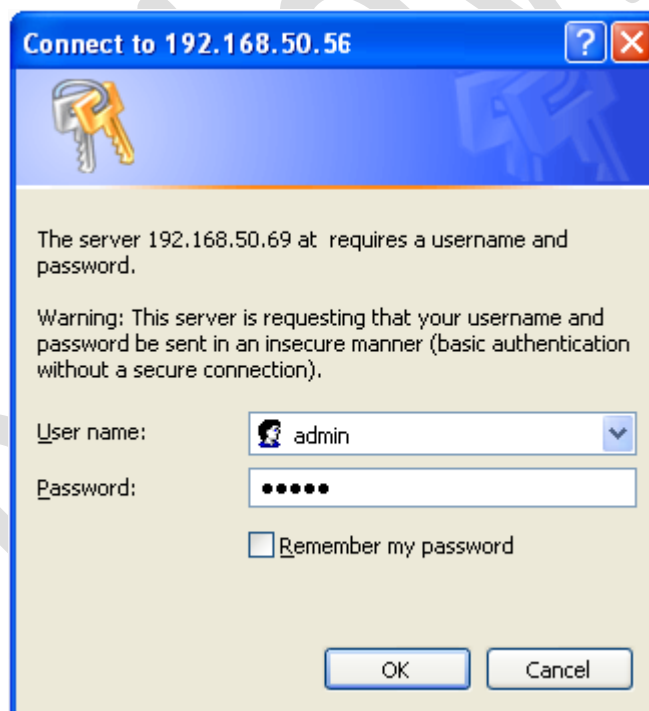
11.3 Add server

This section describes how to add a SIP server to the base station (gateway).

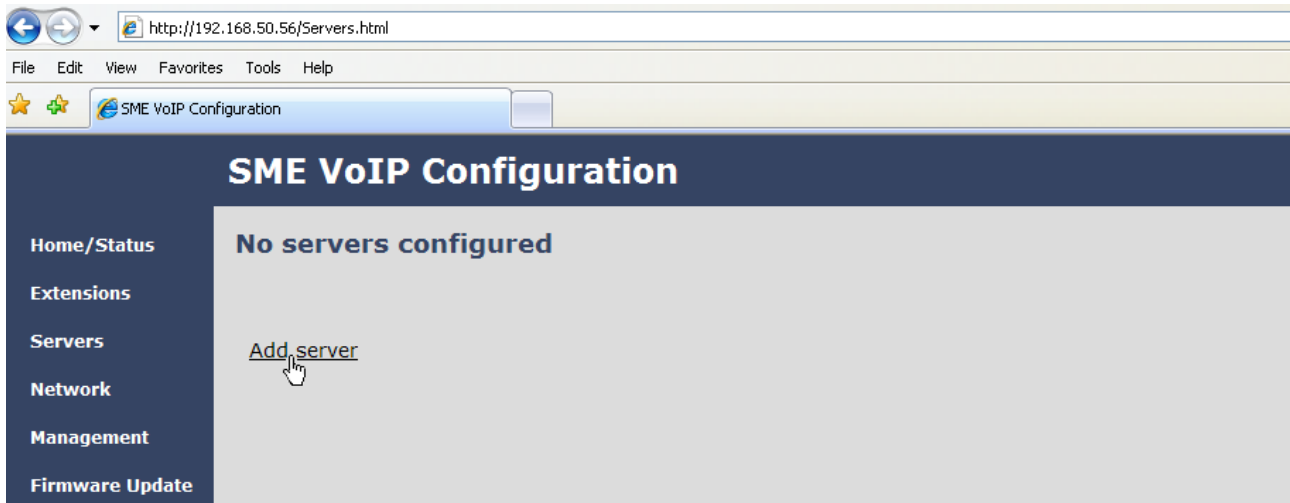
- STEP 1** Open browser on the computer and type in the IP address of the base. Press “Enter” to access the base. If you don’t know the IP address, then write “ipdetect<MAC address>”. The MAC address is written on the base/gateway.
If the MAC-address format does not work then use the network protocol analyser (e.g. wireshark) to retrieve the IP address of Base station.
Enter the IP address to browser.



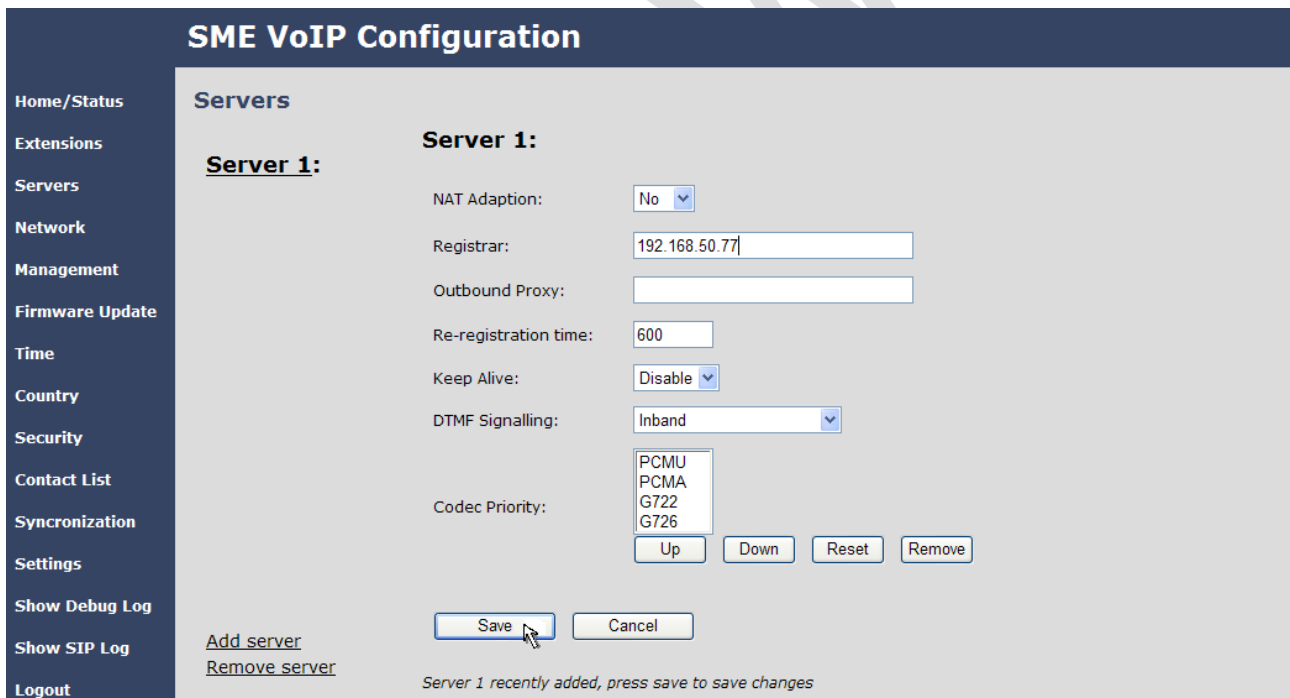
- STEP 2** Enter the “Username” and “Password” when prompted. The default username and password is “admin”.



STEP 3 A SIP server must be configured on the base before handsets can be registered to the base. To add a SIP server, select sheet “Server” and click the link “Add server”.

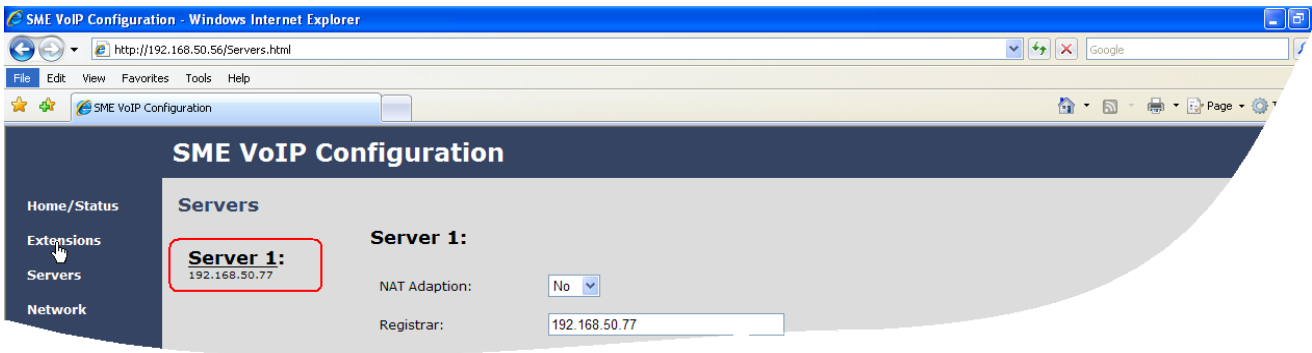


STEP 4 Fill out the displayed form and click “Save”. In the shown example we configure a SIP server located on the IP address 192.168.50.77 and no Outbound proxy is used. Set “NAT adaption” if the base is behind NAT . It is also possible to type in the URL’s direct link, i.e. like “sipphone.com”



NOTE:

The new server is displayed to the left when it is successfully saved.



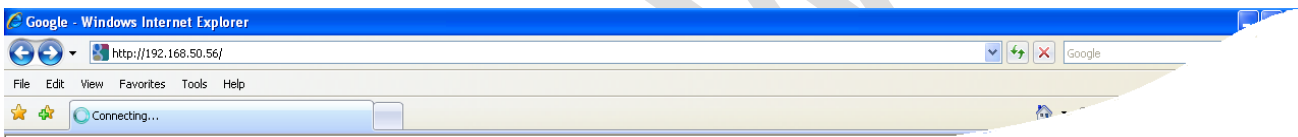
11.4 Register handset to base

This section describes how to register the wireless handset to the base station.

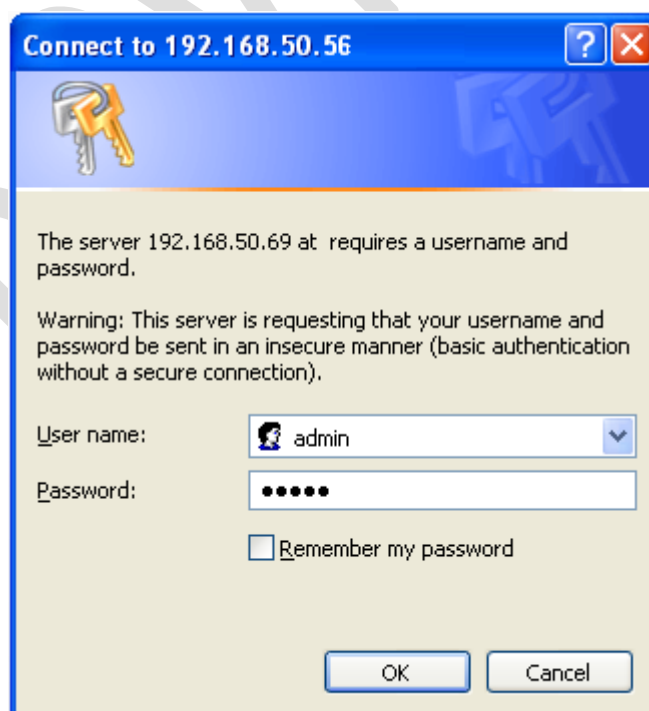
NOTE:

Minimum one server must be registered to the base (system), otherwise a handset cannot be registered to the system. Please see chapter “Add server”.

- STEP 1** Open Windows Internet Explorer on the computer and type in the ipdetect<MAC address> or IP address of the base. Press “Enter” to access the base.



- STEP 2** Type in the “Username” and “Password” when prompted. The default username and password is “admin”.



STEP 3 Select “Extensions” URL and click “Add extension” link



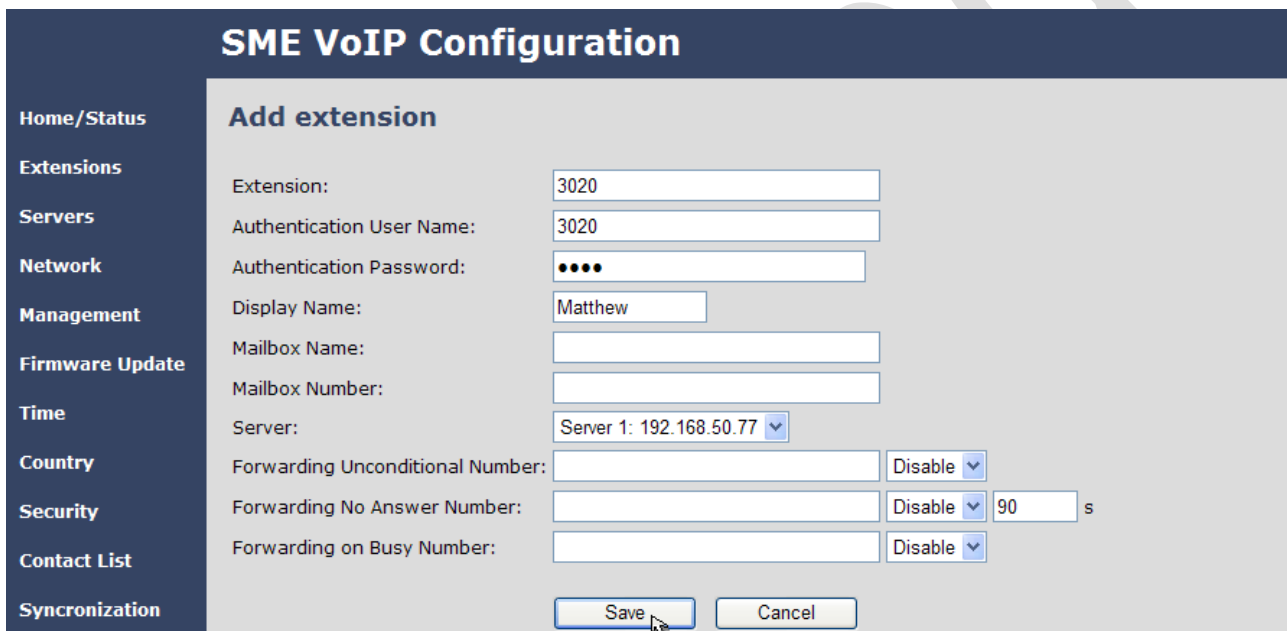
Extensions

Server 1:
192.168.50.77

Idx	Extension	Display Name	IPEI
There are currently no extensions for server 1			

[Add extension](#)

STEP 4 Fill out the form and click “Save”. In the example below we add the extension “3020” and this SIP account got the same number as “Authentication User Name” and “Password”. The “Server 1” is selected by default as server for this extension.



SME VoIP Configuration

Add extension

Extension: 3020

Authentication User Name: 3020

Authentication Password: ●●●●

Display Name: Matthew

Mailbox Name:

Mailbox Number:

Server: Server 1: 192.168.50.77

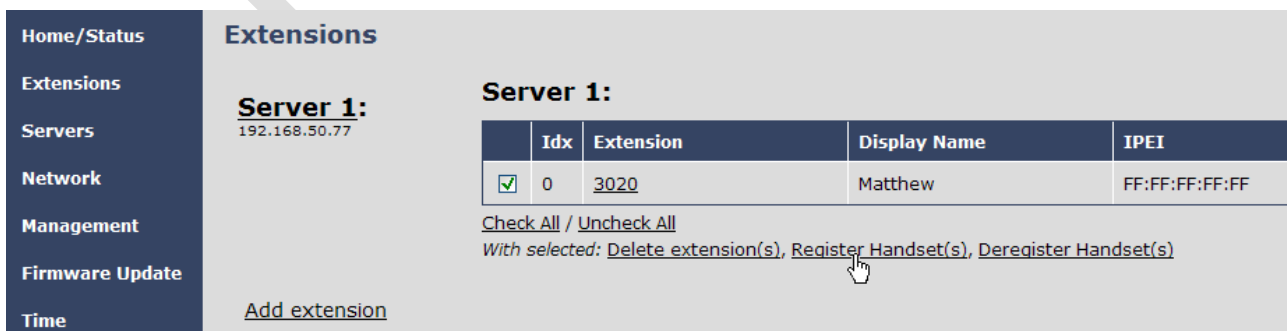
Forwarding Unconditional Number: Disable

Forwarding No Answer Number: Disable 90 s

Forwarding on Busy Number: Disable

[Save](#) [Cancel](#)

STEP 5 Set a Check mark on the extension which shall be assigned to the handset you want to register and click “Register handset (s)”. The base is now open (ready state) for handset registrations for 5 minutes.



Extensions

Server 1:
192.168.50.77

Idx	Extension	Display Name	IPEI
☒ 0	3020	Matthew	FF:FF:FF:FF

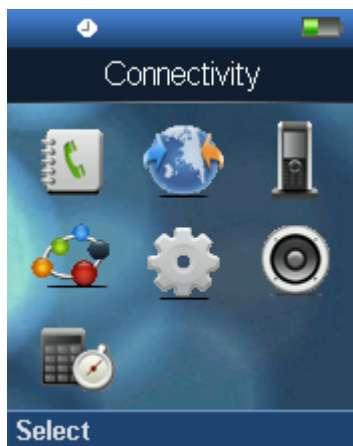
[Check All / Uncheck All](#)

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

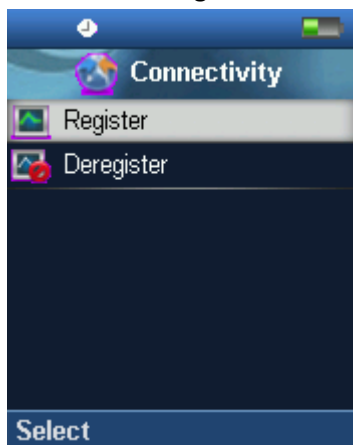
[Add extension](#)

STEP 6 Start the registration procedure on the handset by following step “a” to “d” below.

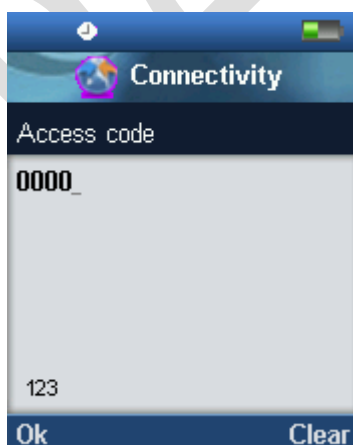
a) Select main menu “Connectivity”



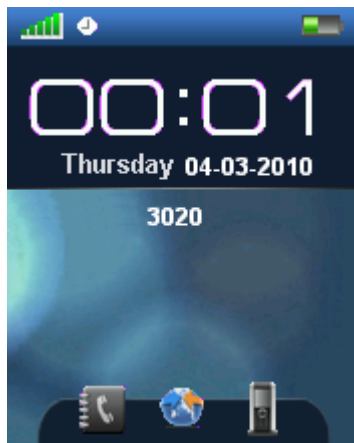
b) Select menu “Register”



c) Type in the “AC code” and press “OK” to start the registration. The default AC code is “0000”.



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



NOTE:

The unique handset IPEI is displayed on sheet “Extensions” when the handset is successfully registered. 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.

We illustrate how extensions page will be when you register several handsets.

Extensions

Server 1:

Server 1:
192.168.10.99
[Add extension](#)
[Refresh](#)

	Idx	Extension	Display Name	IPEI	State
☐	0	165	165	11:6E:50:02:17	Present@RPN00
☐	1	164	164	11:6E:50:01:19	Present@RPN00
☐	2	163	163	01:6E:50:00:78	
☐	3	162	162	11:6E:50:00:F6	Present@RPN04
☐	4	161	161	11:6E:50:01:10	Present@RPN00
☐	5	160	160	11:6E:50:01:23	Present@RPN04

12 VLAN Setup Management

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

12.1 Introduction

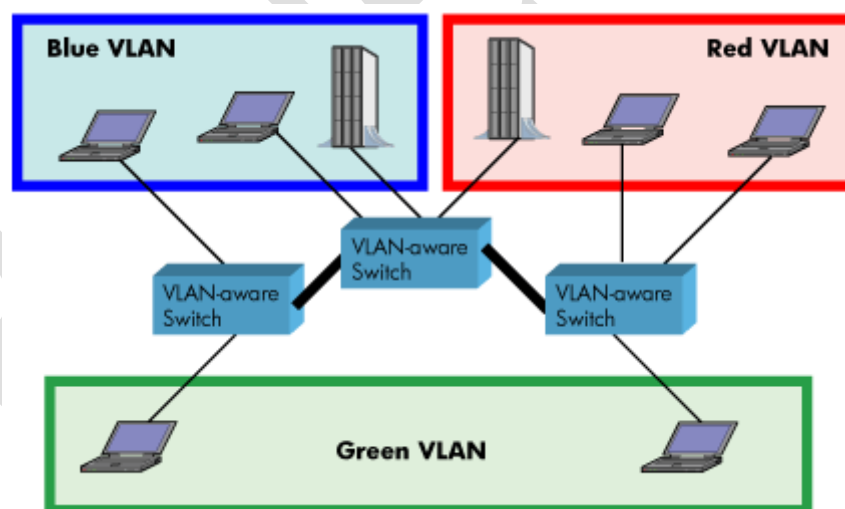
In this chapter, we describe how to setup VLAN to typical network. There are three main stages involved in this procedure:

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

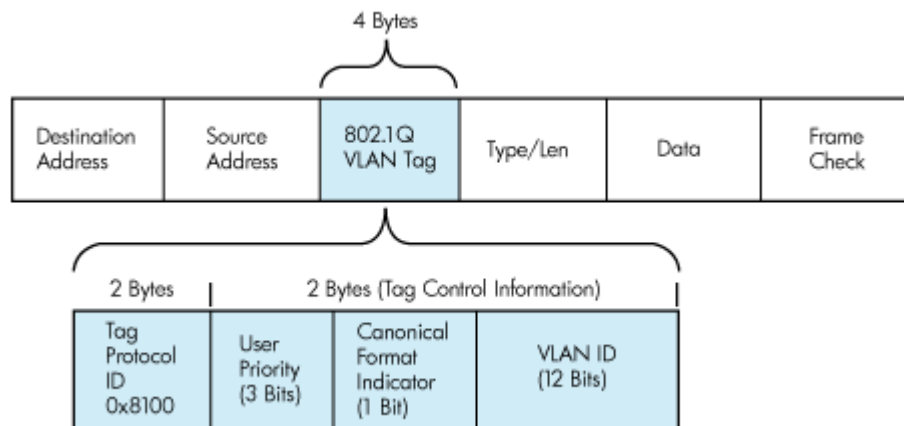
1. When the switch receives a broadcast or multicast frame from a port, it floods the frame to only those ports that belong to the same VLAN as the frame.
2. When a switch receives a unicast frame, it forwards it to the port to which it is addressed, only if the port belongs to the same VLAN as the frame.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

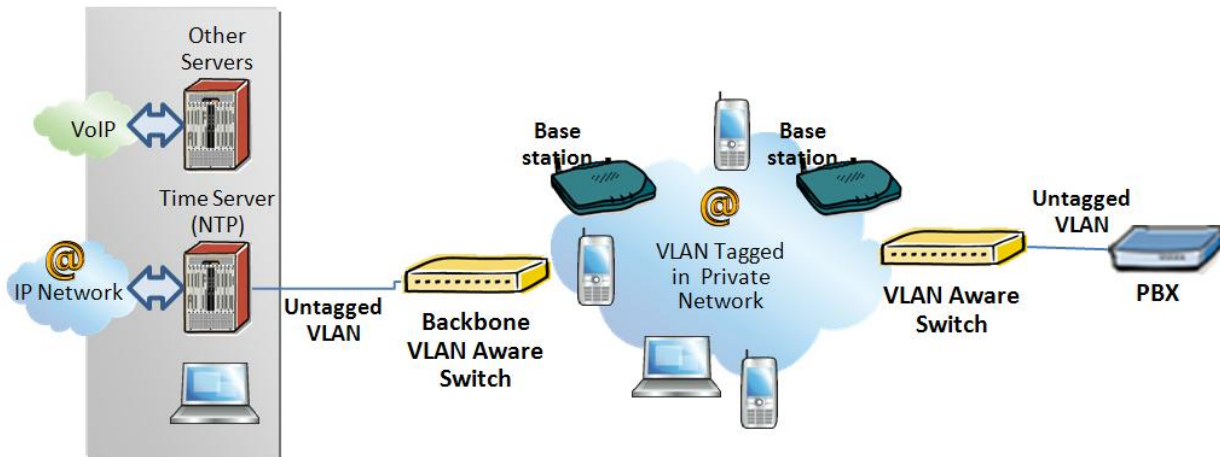
12.4 Implementation Cases

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.



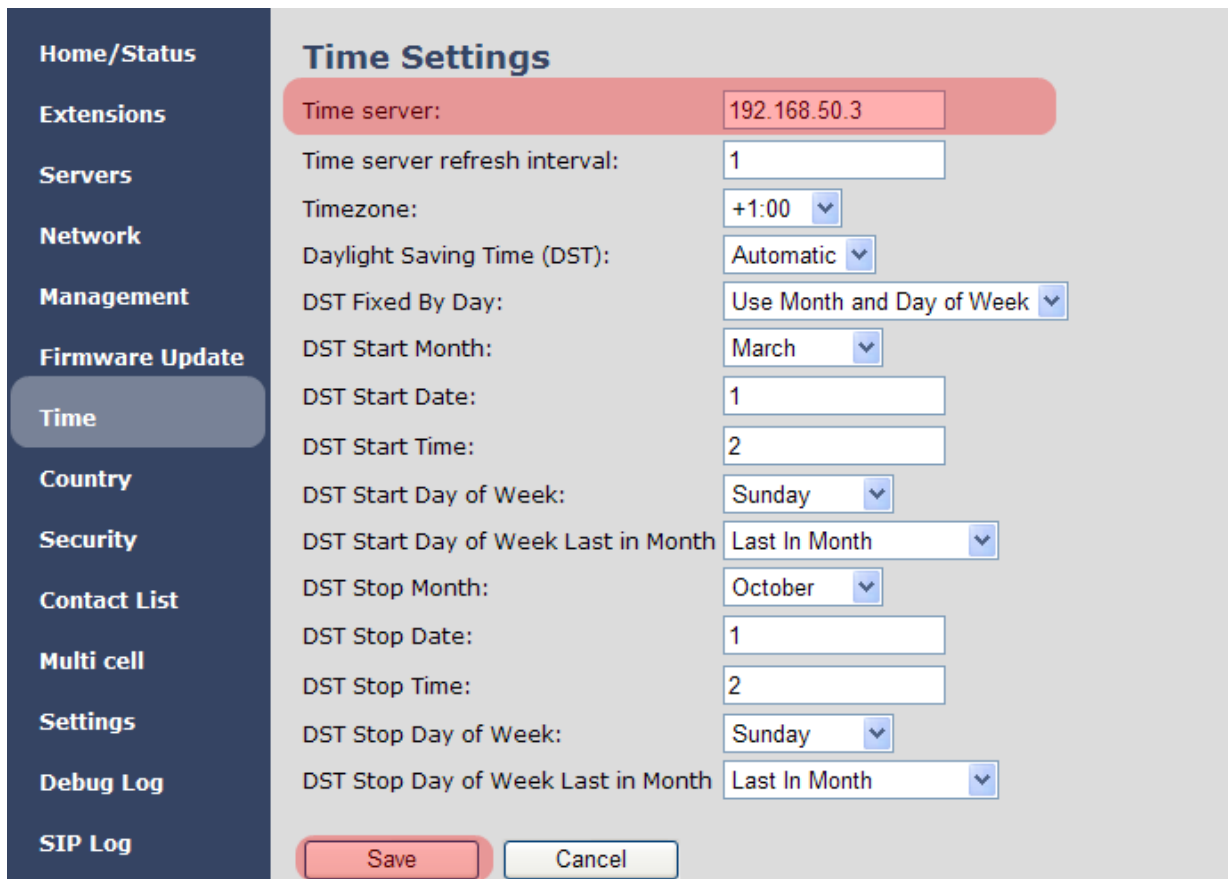
12.5 Base station Setup

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

- STEP 1** Connect the Base station to a private network via standard Ethernet cable (CAT-5).
- STEP 2** Open any standard browser and enter the address:
<http://ipdetect<MAC-Address-Base-Station>> or <http://<IP-address of base station>>
 This will retrieve the HTTP Web Server page from the base station.
- 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 SME 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.



Time Settings	
Time server:	192.168.50.3
Time server refresh interval:	1
Timezone:	+1:00
Daylight Saving Time (DST):	Automatic
DST Fixed By Day:	Use Month and Day of Week
DST Start Month:	March
DST Start Date:	1
DST Start Time:	2
DST Start Day of Week:	Sunday
DST Start Day of Week Last in Month	Last In Month
DST Stop Month:	October
DST Stop Date:	1
DST Stop Time:	2
DST Stop Day of Week:	Sunday
DST Stop Day of Week Last in Month	Last In Month

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.

Home/Status
Extensions
Servers
Network
Management
Firmware Update
Time
Country
Security
Contact List
Multi cell
Settings
Debug Log
SIP Log
Logout

Network Settings

IP settings

DHCP/Static IP:
IP Address:
Subnet Mask:
Default gateway:
DNS (primary):
DNS (secondary):

NAT Settings

Enable RPORT:
Keep alive time:

SIP/RTP Settings

Local SIP port:
SIP ToS/QoS:
RTP port:
RTP port range:
RTP ToS/QoS:

VLAN Settings

VLAN Id:
VLAN User Priority:

Boot Server Options

Boot Server DHCP Option:
Customer DHCP Option:
Option Content Type:

13 Multi-cell Setup & Management

This chapter seeks to describe how to install, add and synchronize one or multiple base stations to the network. There are two main procedures involved:

- 1) Proper placement of the base stations (which is called network dimensioning). The present chapter does not address this issue. Refer to Chapter 4 for details.
- 2) Creating and adding base station profiles to the network via the SME Configuration Tool (to form a multi-cell system).

This chapter describes the second procedure.

NOTE This chapter is valid for Base station firmware version 00.49 and above.

13.1 SME Configuration Interface

RTX have offered HTTP interface in base station firmware that can be used as HTTP Web Server. The SME Configuration Interface can be retrieved from this HTTP Web Server in each Base station.

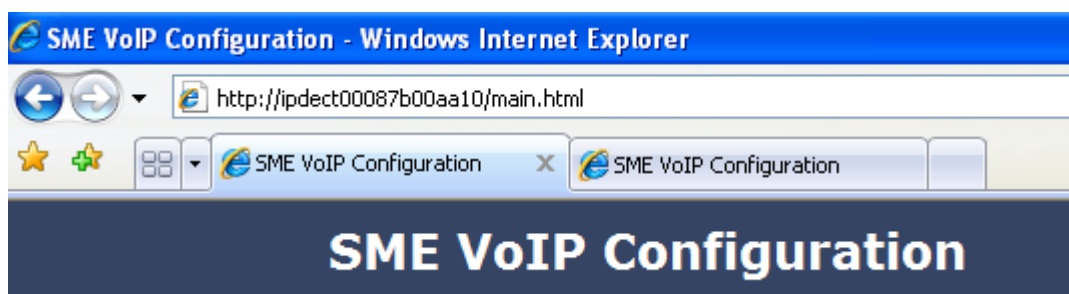
The HTTP Web Server is enabled in the base station by default.

NOTE This procedure is valid for Base station firmware version 00.34 and above. The system administrator must update the relevant Base station(s) to the latest firmware before proceeding to the next section. Refer to Chapter 10.

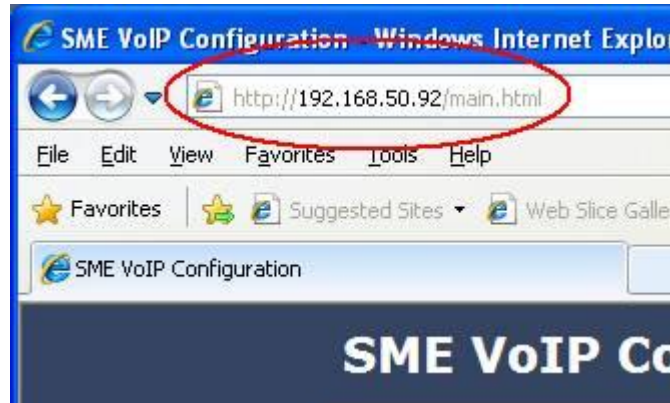
13.2 Adding Base stations via SME Configuration Interface

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** Open any standard browser and enter the address:
<http://ipdetect<MAC-Address-Base-Station>>
 e.g. <http://ipdetect00087B00AA10>. This will retrieve the HTTP Web Server page from the base station with hardware address 00087B00AA10.



- STEP 3** Skip this step if you were successful with STEP 2. If the **MAC-address** method as described above does not work, then use a standard network protocol analyzer (e.g. **Wireshark**) to eavesdrop the IP address allocated to the base unit by the DHCP server. You can download Wireshark follow its documentation to know how it is done.
- Enter the IP address into the address bar of the browser to retrieve base station HTTP Web Server Page.



- STEP 4** On the Login page, enter your authenticating credentials (i.e. username and password is default “admin”). Click **OK** button.



- STEP 5** Once you have authenticated, the browser will display front end of the SME Configuration Interface. The front end will show relevant information of the base station (in this case MAC-Addr: **00087B00AA10** as highlighted in the snap-shot below).

[Home/Status](#)
[Extensions](#)
[Servers](#)
[Network](#)
[Management](#)
[Firmware Update](#)
[Time](#)
[Country](#)
[Security](#)
[Contact List](#)
[Multi cell](#)
[Settings](#)
[Debug Log](#)
[SIP Log](#)
[Logout](#)

SME VoIP Configuration

Welcome

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

System Information:

Phone Type:	IPDECT
Current local time:	08/Sep/2010 11:48:02
Operation time:	00:04:26 (H:M:S)
RFPI-Address:	116E604900; RPN:00
MAC-Address:	00087B00AA10
IP-Address:	192.168.50.71
Firmware-Version:	IPDECT/00.34//26-Aug-10 13:55
Firmware-URL:	tftp://192.168.50.3/FwuPath

SIP Identity Status on this Base Station:

Press button to reboot.

Reboot

13.2.1 Time Server Setup

- 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.
- 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 making sure the correct Time Server IP address is still in place.

Home/Status Extensions Servers Network Management Firmware Update Time Country Security Contact List Multi cell Settings Debug Log SIP Log	Time Settings	
	Time server:	192.168.50.3
	Time server refresh interval:	1
	Timezone:	+1:00
	Daylight Saving Time (DST):	Automatic
	DST Fixed By Day:	Use Month and Day of Week
	DST Start Month:	March
	DST Start Date:	1
	DST Start Time:	2
	DST Start Day of Week:	Sunday
	DST Start Day of Week Last in Month:	Last In Month
	DST Stop Month:	October
	DST Stop Date:	1
	DST Stop Time:	2
	DST Stop Day of Week:	Sunday
DST Stop Day of Week Last in Month:	Last In Month	
Save Cancel		

A successful reboot will reset the time in the base station. Ensure the Time Server IP address is correct.

Please select a configuration page in the index pane on left.	
System Information:	Multi Cell Ready(Keep-alive) Master
Phone Type:	IPDECT HW ver 00
System Type:	Generic SIP (RFC 3261)
RF Band:	EU
Current local time:	05/Nov/2010 08:59:54
Operation time:	15:59:49 (H:M:S)

13.2.2 SIP Server (or PBX Server) Setup

- STEP 7** 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, 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 **"No"** 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. Select **Save** button.

Servers

Server 1:

[Add server](#)
[Remove server](#)

Server 1:

NAT Adaption: No

Registrar: 192.168.50.57

Outbound Proxy:

Re-registration time: 3600

Keep Alive: Enable

DTMF Signalling: RFC 2833

Codec Priority:

PCMU

PCMA

Up

Down

Reset

Remove

Save Cancel

Server 1 recently added, press save to save changes

13.2.3 Multi-cell Setup

- STEP 8** Click on **Multi Cell** url link in the **SME VoIP Configuration** to view the current **Multi cell settings** status of the current base station. Most brand new base stations have **Multi cell system** feature disabled by default.

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

Multi Cell settings

Settings for this unit

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

Multi cell system:

System chain ID:

Synchronization time (s):

Multi cell debug:

Save Cancel

- STEP 9** Next, the system administrator needs to create and Enable Multi 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.

Multi Cell settings

Settings for this unit

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

Multi cell system:

System chain ID:

Synchronization time (s):

- 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 **2275**. The **Synchronization time (s)** parameter is defined as window/period of time in seconds a specific base station synchronises to the master base station unit (by default 60). Synchronising the slaves to the master updates them with the latest network information.

Multi Cell settings

Settings for this unit

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

Multi cell system:

System chain ID:

Synchronization time (s):

Multi cell debug:

Save

Cancel

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

The parameters are successfully saved

You will be redirected after 3 seconds

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 6**.

IMPORTANT:

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

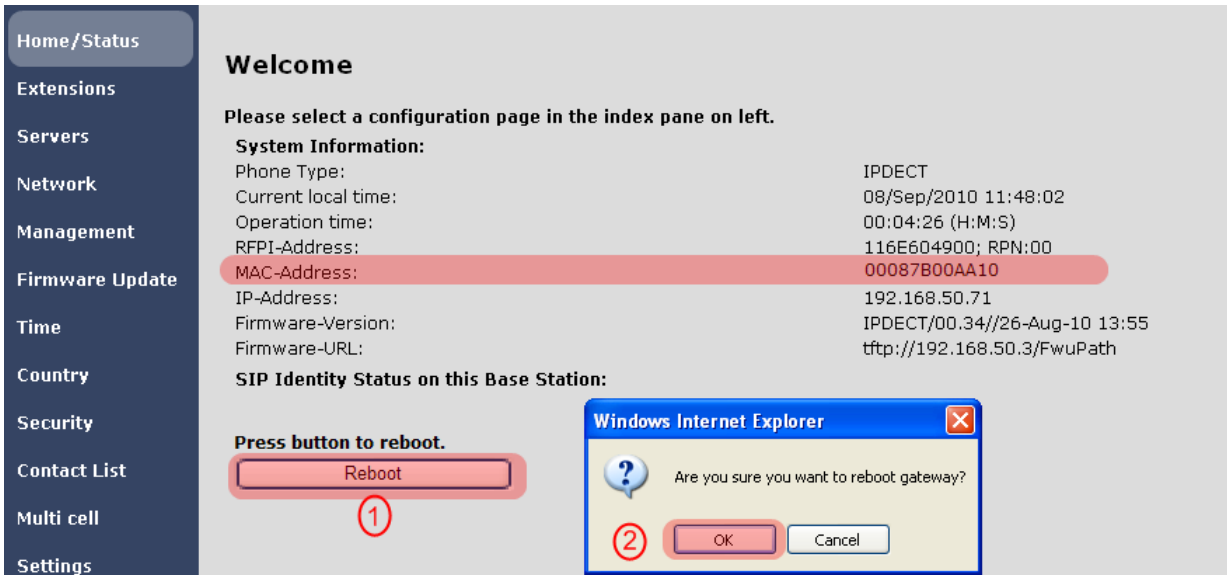
STEP 11 Repeat **STEP 1-10** as explained above for each base stations.

IMPORTANT:

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

13.3 Synchronizing the Base stations

STEP 12 On each **SME VoIP Configuration** interface for the base station(s) navigate to the Home/Status page and Click the Reboot button.



Home/Status

Welcome

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

System Information:

Phone Type:	IPDECT
Current local time:	08/Sep/2010 11:48:02
Operation time:	00:04:26 (H:M:S)
RFPI-Address:	116E604900; RPN:00
MAC-Address:	00087B00AA10
IP-Address:	192.168.50.71
Firmware-Version:	IPDECT/00.34//26-Aug-10 13:55
Firmware-URL:	tftp://192.168.50.3/FwuPath

SIP Identity Status on this Base Station:

Press button to reboot.

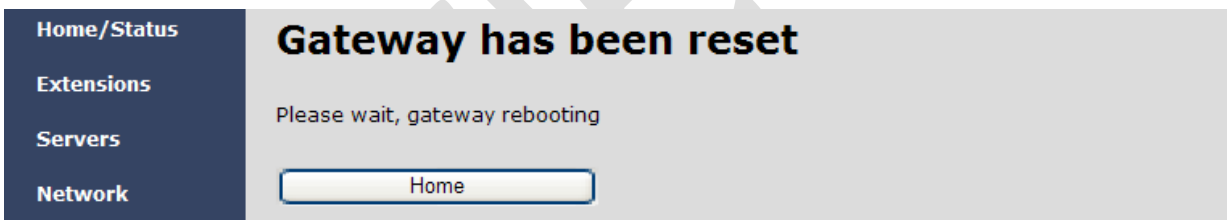
Reboot (1)

Windows Internet Explorer

Are you sure you want to reboot gateway?

OK (2) **Cancel**

This will trigger **Are you sure you want to reboot gateway?** window. Click **OK** button on this window. A successful restart of the base stations will lead to a display of the page: **Gateway has been reset**.



Home/Status

Gateway has been reset

Please wait, gateway rebooting

Home

STEP 13 Navigate back to the **Multi cell settings** page by clicking **Multi-cell** url link at the left column. The revised **Multi cell settings** page shows the relevant base stations synchronized together. By default, the system uses the first registered base station as the master base unit.

Home/Status
Extensions
Servers
Network
Management
Firmware Update
Time
Country
Security
Contact List
Multi cell
Settings
Debug Log
SIP Log
Logout

Multi Cell settings

Settings for this unit

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

Multi cell system:

System chain ID:

Synchronization time (s):

Multi cell debug:

DECT system settings

These settings are DECT settings for the system.

DECT system RFPI:

Auto configure DECT sync source tree

SIP system settings

These settings are SIP settings for the system.

Maximum number of SIP register per base station:

MAC-units in chain

	ID	RPN	MAC address	IP address	Version	Status	DECT sync source	Property	Dect Property
☐	0	00	00:08:7B:07:7C:BC	0.0.0.0	0	Connection lost!	1 - RPN: 04		Unknown!
☐	1	04	00:08:7B:07:7C:F7	192.168.50.114	34	Connected	0 - RPN: 00		Unknown!

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

- STEP 14** On the Multi-cell settings page, scroll to the **DECT system settings** and Enable or Disable the “Auto configure DECT sync option source tree” (See description in the table below). The DECT system RFPI parameter is computed by the system (Its often greyed in a multi-cell system configuration).

DECT system settings

These settings are DECT settings for the system.

DECT system RFPI:

Auto configure DECT sync source tree

- STEP 15** Scroll to the **SIP system settings** section, configure and save the parameter based on the description below:

Parameter	Description
## of SIP accounts before distributed load	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. Note: A maximum of 8 simultaneous calls can be routed through each Base units in a multi-cell setup. Permitted Input: Positive Integers (e.g. 6)
SIP Support for multiple registrations per	Enable this option so it is possible to use 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

account	from Base X to Base Y, this phone will de-register from Base X, and register to Base Y automatically. Note: Choose Yes when the SIP server supports this feature otherwise choose No if the Sip server does not support this feature. Permitted Input: Yes, No
----------------	---

SIP system settings

These settings are SIP settings for the system.

Number of SIP accounts before distributed load:

SIP Server support for multiple registrations per account: (used for roaming signalling)

STEP 16 Next, on the **MAC-units in chains** section, you can manually configure the synchronisation source tree of the multi-cell system. Multi-cell settings page, scroll to the DECT system settings and Enable or Disable the “**Auto configure DECT sync option source tree**” (See description in the table below). The DECT system RFPI parameter is computed by the system (Its often grayed in a multi-cell system)

MAC-units in chain

ID	RPN	MAC address	IP address	Version	Status	DECT sync source	Dect Property
☐ 0	00	00:08:7B:07:7C:BC	<u>192.168.50.71</u>	34	Connected	0 - RPN: 00	Master
☐ 1	04	00:08:7B:07:7C:F7	<u>192.168.50.114</u>	34	Connected	0 - RPN: 00	Unknown!

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

13.4 Summary of Procedure – Creating a Chain

We enumerate the short version of how to add 3 base stations units in a multi-cell setup. This can be applied for up to 40 number of base units. The procedure below is valid **ONLY** for base station firmware version 00.36 and above.

This procedure is divided into four (4) main stages. Apply this procedure if all base unit are straight from production.

13.5 Stage 1

Skip this stage if relevant base stations are already in the network.

- Add 3 base stations i.e. RFP1, RFP2, RFP3 > Disable the “Multi cell system” option and “Save”
- RFP1, RFP2, RFP3: Reboot from the HTTP SME Configuration Main Page
- RFP1, RFP2, RFP3: Default by pressing reset button 12-sec.

13.6 Stage 2

Choosing 1st base unit i.e. RFP1 as Master

- RFP1: Define Time server and “Save” from the **Time** page
- RFP1: Reboot

- c) RFP1: Press “Add server” and define SIP server IP and “Save” from the **Servers** page
- d) RFP1: Multi cell system = enable and “Save” from the **Multi-cell** page
- e) RFP1: Reboot (Verify the message:

“SYNCMGR: This base is ready to be master in a Chain”

From the debug logs)

13.7 Stage 3

Choose another base unit, RFP2 as Slave1

- a) RFP2: Multi cell system = enable and “Save”
- b) RFP2: Reboot (Verify from Debug log **“SYNCMGR: This base is ready to join into another Chain”**)
- c) RFP1, RFP2: Wait 2min for stable Master-Slave chain (check for the message:

SYNCMGR: Socket#10 creation success

from the debug log)

- d) After a successful restart, on each base [RFP1 and RFP2] Multi-cell page you will find the other base connected and synchronized (the IP status shows **This Unit** or **Connected**) to the system as illustrated below.

DECT system settings

These settings are DECT settings for the system.

DECT system RFPI:

SIP system settings

These settings are SIP settings for the system.

Number of SIP accounts before distributed load:

SIP Server support for multiple registrations per account: (used for roaming signalling)

MAC-units in chain

	ID	RPN	Version	MAC address	IP address	IP Status	DECT sync source	DECT Property
☐	0	00	51	00:08:7B:D7:91:6E	<u>192.168.10.106</u>	This unit	0 - RPN: 00	Master
☐	1	04	51	00:08:7B:D7:91:74	<u>192.168.10.105</u>	Connected	0 - RPN: 00	Locked

Check All / Uncheck All

With selected: [Remove from chain](#)

You can register an arbitrary HS to the extension and verify whether its successful from the “Home” page and Handset UI

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

System Information:

Phone Type:	IPDECT HW ver 00
System Type:	Generic SIP (RFC 3261)
RF Band:	EU
Current local time:	05/Nov/2010 08:59:54
Operation time:	15:59:49 (H:M:S)
RFPI-Address:	116E611100; RPN:00
MAC-Address:	00087bd7916e
IP-Address:	192.168.10.106
Firmware-Version:	IPDECT/00.51//03-Nov-10 13:34
Firmware-URL:	tftp://192.168.10.213

Multi Cell Ready(Keep-alive) Master

SIP Identity Status on this Base Station:

165 165@192.168.10.99	Identity 1 Status:	OK
164 164@192.168.10.99	Identity 2 Status:	OK
161 161@192.168.10.99	Identity 7 Status:	OK
157 157@192.168.10.99	Identity 8 Status:	OK

13.8 Stage 4

Choose the 3rd base unit, RFP3 as Slave2

- e) RFP3: Multi cell system = enable and "Save"
- f) RFP3: Reboot (Verify Debug log "SYNCMGR: This base is ready to join into another Chain")
- g) RFP1, RFP3: Wait 2min for stable Master-Slave chain (SYNCMGR: Socket#10 creation success)
- h) RFP3: Check mark ID2/RPN08 and select dropdown "1 – RPN: 04" and "Save"
- i) RFP3: Reboot (Confirm from the Debug log the message:

SYNCMGR: Socket#8 creation success

)

Multi-cell chain of 3 base stations has been created successfully. Next step involves adding extensions to the system.

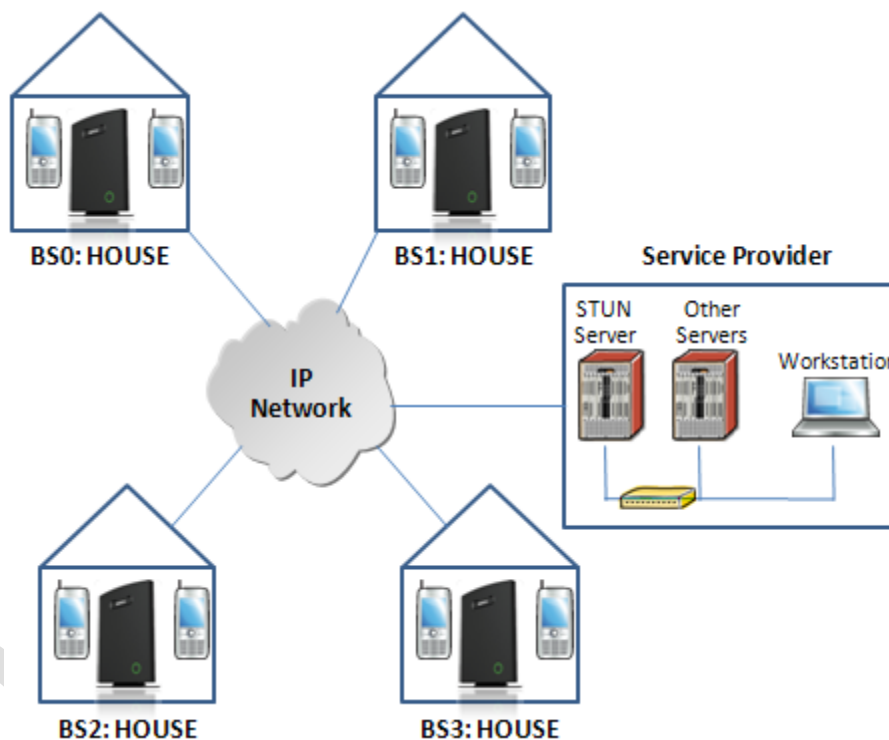
13.9 Practical Configuration of Multi-cell System

In chapter 3 we described different scenarios where the SME VoIP system can be deployed. In this chapter we describe what exactly to configure in the SME VoIP Configuration Interface ensure these scenarios really work.

13.9.1 Case ##1: Isolated Buildings

The optimal configuration for isolated buildings is standalone base stations setting. In this setting, you must:

- STEP 1** Using the figure below as illustration, log into the Configuration Interface of each base station.
- STEP 2** Configure the Time Server, SIP Server, Extensions as described in the previous chapters.
- STEP 3** On the main page of the configuration interface, click **Network** URL > disable the Multi-cell parameter of each base station > Save and Reboot each base to complete the Case ##1 setup.



Disable Multi Cell option of Base Stations

Settings for this unit

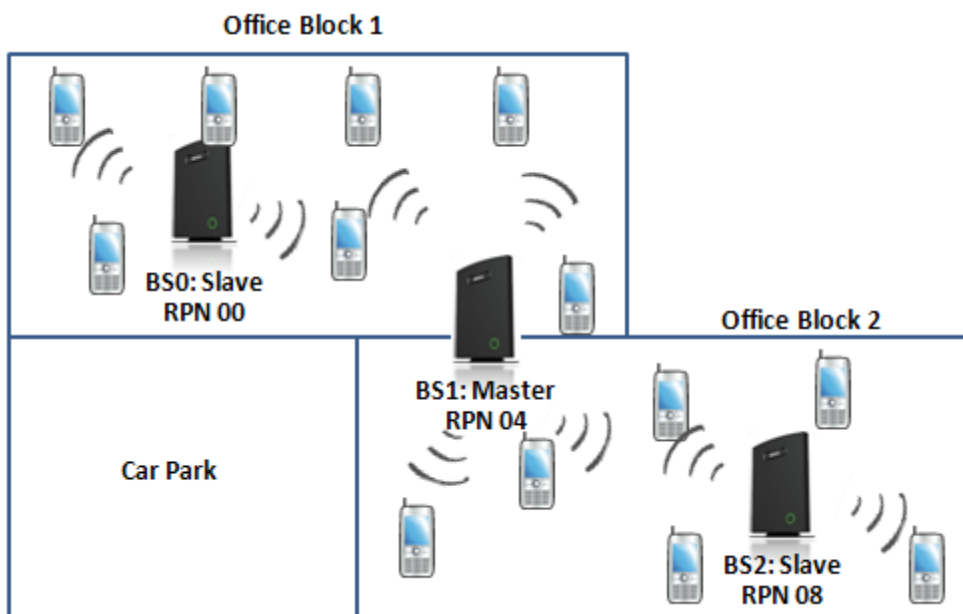
These settings are used to connect this unit to a system.

Multi cell system:	Disable ▼
System chain ID:	2275
Synchronization time (s):	60
Multi cell debug:	Disable ▼

13.9.2 Case ##2: Location with co-located partners

To illustrate this setup, two slave base stations are synchronised to one master base in the two office blocks.

It is not necessary to deploy a dedicated Base unit at the car park area because it is likely no telephony traffic or call will be placed at the area. Here is diagram to illustrate Case ##2.



The procedure:

- STEP 1** Follow the steps described in sections 13.4 to 13.8
- STEP 2** On the **Network** page of each base define the **DECT sync source** settings as illustrated in the table below.
- STEP 3** Save and reboot each base to complete case ##2 setup

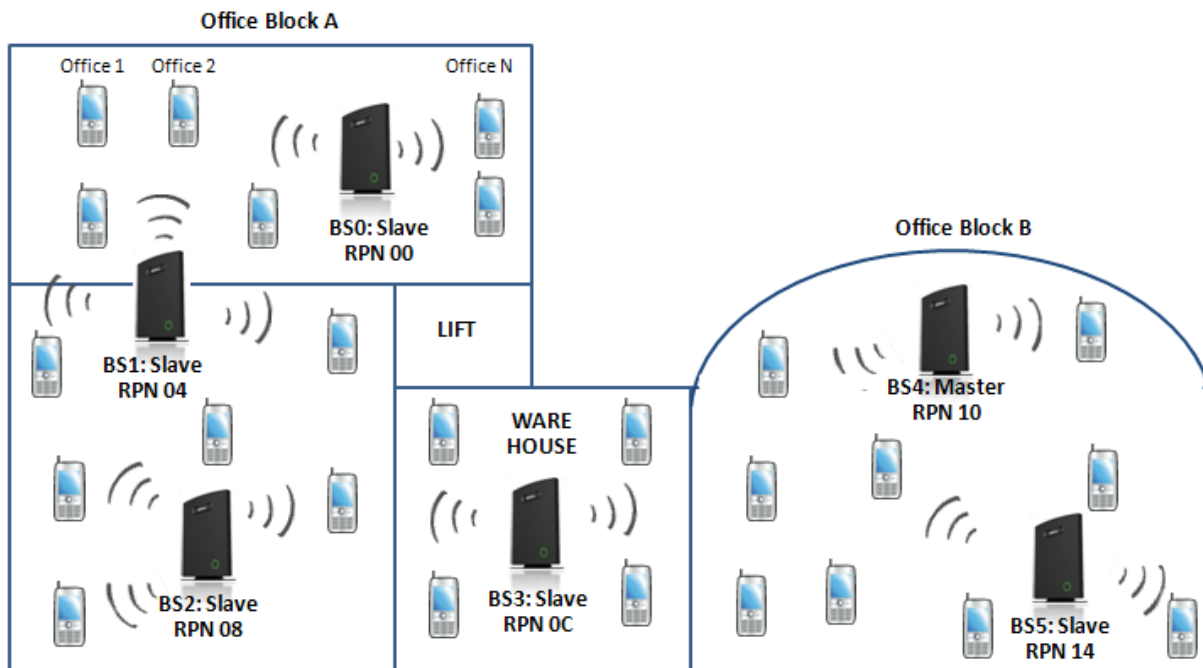
Multi Cell Page of Base Stations

Recommended settings of MAC-units in Chain section of page (Other different settings exist):

RPN	Ver	MAC Addr	IP Addr	IP Status	DECT sync source	DECT Property
00	XX	XX:XX:XX...	XXX.XXX...	Connected	1: RPN:04	
04	XX	XX:XX:XX...	XXX.XXX...	Connected	1: RPN:04	Master
08	XX	XX:XX:XX...	XXX.XXX...	Connected	1: RPN:04	

13.9.3 Case ##3: Large to Medium Sized Enterprises

In this scenario, we have five slave bases synchronised to one master base. The master base is located in office block B while the slave bases are spread across the whole enterprise. No base station is deployed in the lift because it has high attenuation properties that will drastically reduce radio signals.



The procedure:

- STEP 1** Follow the steps described in sections 13.4 to 13.8
- STEP 2** On the **Network** page of each base define the **DECT sync source** settings as illustrated in the table below.
- STEP 3** Save and reboot each base to complete case ## 3 setup

Multi Cell Page of Base Stations

Recommended settings of MAC-units in Chain section of page (Other valid setting exists):

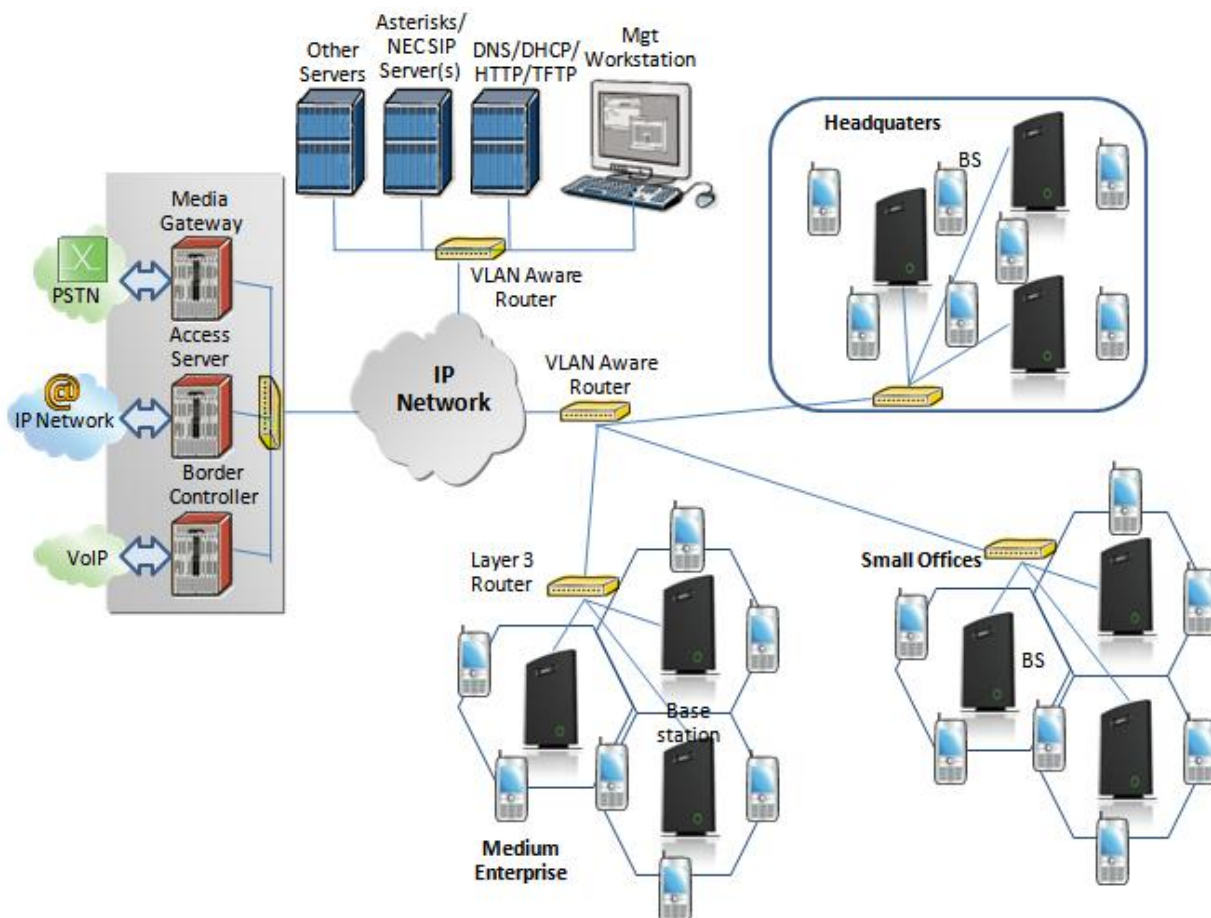
NOTE:

The number of chains cannot exceed 6 levels.

RPN	Ver	MAC Addr	IP Addr	IP Status	DECT sync source	DECT Property
00	XX	XX:XX:XX...	XXX.XXX...	Connected	1: RPN:04	
04	XX	XX:XX:XX...	XXX.XXX...	Connected	2: RPN:08	
08	XX	XX:XX:XX...	XXX.XXX...	Connected	3: RPN:0C	
0C	XX	XX:XX:XX...	XXX.XXX...	Connected	4: RPN:10	
10	XX	XX:XX:XX...	XXX.XXX...	Connected	4: RPN:10	Master
14	XX	XX:XX:XX...	XXX.XXX...	Connected	4: RPN:10	

13.9.4 Case ##4: Large Enterprises at Different Locations

In this scenario, multi-cell systems are deployed at different locations; geographically separated from each other. Each location has a master base station with more than one slave base synchronise to it.



The procedure:

- STEP 1** Follow the steps described in sections 13.4 to 13.8
- STEP 2** On the **Network** page of each base define the **DECT sync source** settings as illustrated in the table below.
- STEP 3** Save and reboot each base to complete case ## 4 setup

Multi Cell Page of Base Stations

Recommended settings of MAC-units in Chain section of page (Other valid setting exists):

RPN	Ver	MAC Addr	IP Addr	IP Status	DECT sync source	DECT Property
00	XX	XX:XX:XX...	XXX.XXX...	Connected	0: RPN:00	Master for HQ
04	XX	XX:XX:XX...	XXX.XXX...	Connected	0: RPN:00	
08	XX	XX:XX:XX...	XXX.XXX...	Connected	1: RPN:04	
0C	XX	XX:XX:XX...	XXX.XXX...	Connected	3: RPN:0C	Master for Offices

10	XX	XX:XX:XX...	XXX.XXX...	Connected	3: RPN:0C	
14	XX	XX:XX:XX...	XXX.XXX...	Connected	4: RPN:10	
18	XX	XX:XX:XX...	XXX.XXX...	Connected	6: RPN:18	Master for Enterprises
1C	XX	XX:XX:XX...	XXX.XXX...	Connected	6: RPN:18	
20	XX	XX:XX:XX...	XXX.XXX...	Connected	7: RPN:1C	

Reviewed

14 Functionality Overview

So far we have setup our SME VoIP system. Next, in this chapter we describe 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 diversion, conference calls, etc. A brief description of SME VOIP network functionalities are:

- **Outgoing/incoming voice call management:** The SME VOIP system can provide multiple priority user classes. Further, about 3 repeaters can be linked to a Base-station depending on customer requirements and assuming that the DECT RPN values are geographically unique.
- **Internal/external handover:** User locations are reported to SIP Server in order to provide differentiated services and tariff management. Within a DECT traffic area, established calls can seamlessly be handover between Base-stations using connection handover procedures. External handover are supported for terminals within roaming regions.
- **Mobility:** The network supports seamless mobility where handset subscription information controls allowed mobility. A user terminal can be assigned 2 mobility options:
 - Mobility within in single DECT traffic area.
 - Mobility within a group of DECT traffic areas. Registration procedure can be activated in one or multiple cells.
- **Security:** The RTX SME VOIP system also supports robust security functionalities for Base-stations. Most security¹ functionality is intrinsically woven into the SME VOIP network structure so that network connections can be encrypted and terminal authentication can be performed.

14.1 System Feature List

This section gives a summary of some essential functionality within the wireless IP network.

Components	System Features
Speech Coding	10 channels ADPCM G.726 on air interface ² 10 channels of G729a/b on IP interface ^{3, 2} 10 channels of G711 on IP interface ² Support of mixed types of Codecs in one Base Station
In-band Tones	Dial tone Busy tone Error tone Call waiting tone Messages waiting tone Ring Back tone

¹ With active security 4 channels is supported

² In a multicell configuration 8 channels is supported

³ G729a requires an additional hardware module.

Components	System Features
Radio Access Mechanism	Bearer Handover and Connection Handover: – Intra Cell – Inter Cell – RFP (Own/Other) ⇔ Repeater, Repeater ⇔ Repeater Busy indication and support Connection re-establishment Emergency Calls⁴: Inside or outside roaming areas
SIP support	REGISTER, INVITE, and TERMINATE sessions Session Description Protocol (SDP), HTTP authentication Support 200 DECT instances (depending on SME VOIP configuration) locating SIP servers Support for re-INVITE Support for fail-over SIP proxy Message Waiting Indication Support for “302” response between UA ⇔ SIP Server
Internal Synchronization	Internal Synchronization lock, timing and transmission
Management Features	Assignment of Base-stations Logging calls and internal events, and tracking use of resources Logging system faults TFTP server for software upgrade. WEB interface for remote management of network devices Remote debugging of network devices, including log features

14.2 Detail Feature Description

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/AB (including VAD, CN generation) G.729.1 (ehem. G.729 EV) Note: Only with additional module, this is a extra option that requires a board connector mounted in Gateway. Per default not mounted.
SIP	
RFC2327	SDP: Session Description Protocol
RFC2396	Uniform Resource Identifiers (URI): Generic Syntax
RFC2833	In-Band DTMF/Out of band DTMF support
RFC2915	The Naming Authority Pointer (NAPTR) DNS Resource Record
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)

⁴ Emergency call is not possible if the Network connection is not working or in case of power failure.

RFC3264	Offer/Answer Model with SDP
RFC3265	Specific Event Notification
RFC3326	The Reason Header Field for the Session Initiation Protocol
RFC3311	The Session Initiation Protocol UPDATE Method
RFC3325	P-Asserted Identity
RFC3326	The Reason Header Field for the Session Initiation Protocol (SIP)
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	
In-band DTMF	
SRTP	Will limit number of active calls pr. base when enabled.
Web server	
	Embedded web server HTTP/HTTPS
	Easy configuration of the phone, remote configuration via Management Interface
	Reasonable customization of the Web Interface to customer branding
	Password protection
	Status information on webpage. Minimum: HW/FW version Serial number + MAC address Connected handsets with serial number SIP-status Connected DECT handsets
Other features	
	Remote firmware update (HTTPS/TFTP)
Quality of service	Type of Service (ToS) including DiffServ Tagging, and QoS per IEEE 802.1p/q
IP quality	NetEQ by GIPS (License applies)
	WiFi friendly
	Warning – Network outage, VoIP service outage
	Packet Loss Concealment support
	Sequence Error Handling
	Adaptive Jitter Buffer support
Import of phonebook	Import of phonebooks in csv format (Office 2003)
Automatic DST	
Tone Scheme	Country Depend Tone Scheme
Ethernet features	
VLAN	VLAN (802.1p/q)
DHCP Support	
Static IP	
TLS	For secure connections
TFTP	For configuration download.
HTTP	For configuration download.
HTTPS	For secure configuration download.
TCP/IP/UDP	
SNTP	For internet clock synchronization
VPN	Add-on in the future
Quality of service	Type of Service (ToS) including DiffServ Tagging, and QoS per IEEE 802.1p/q
DHCP option	66 and 160
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)
VoIP Accounts	30 VoIP accounts per base – (maximum 40 bases per installation)
	Maximum 200 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 log	50 mixed between Incoming, outgoing, missed calls
Phone Book	Common Phonebook with up to 200 entries
DND	Do Not Disturb
Call Forward	All
	No Answer
	Busy

Reviewed

15 Network Operations

15.1 Introduction

In this chapter, we will provide an overview of the operation of the network during system start-up, location registration and speech calls including illustration of different call scenarios.

15.2 System Start Up

When a Base station Unit is powered up, it achieves IP address from DHCP server and time from the Time-Server.

Optionally the base retrieves its configuration from a file on the TFTP server. This configuration file describes used network and cluster configuration parameters (optional and not needed).

The SME VoIP network has successfully started up.

15.3 Terminal Attachment

When a DECT Terminal (also called handset or SIP node) is turned on or moved into the coverage area of a Base-station it has to get attached to the network. When more Base-stations are available, the Terminal selects the one with best RF signal. This procedure, called *Location Registration*, always keeps the network informed about where a Terminal is located and enables it receive or originate calls. This procedure also authenticates the Terminal and checks the validity of the associated subscription.

15.4 Outgoing Calls

Outgoing calls are initiated by the Terminal. It selects the Base-station with best RF signal and establishes a radio communication link to Base-station. DECT call control messages are exchanged between Terminal, Base station and other servers. This server forwards the outgoing call as SIP messages to the external SIP Server. The RTP stream is established between the involved Base-station (and the Media Gateway for PSTN calls). If the call is between two Terminals the media stream may be routed directly between the two involved Base-stations depending on the SIP Server routing strategy.

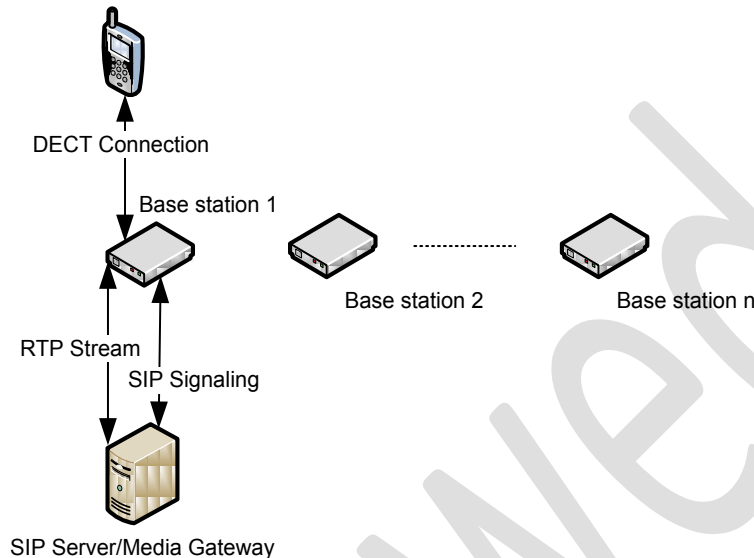
15.5 Incoming Calls

Incoming calls are initiated by SIP INVITE messages from the SIP Server to the Base unit; inviting it to participate in an incoming session. The system sends paging messages to all the Base-station where the Terminal last performed a *Location Registration*. When the paging is received the Terminal establishes a radio communication link to the best available Base-station and sends a response back to DECT controller. DECT call control messages are exchanged and the Terminal starts ringing. When the user answers the call, a connect message is sent to the IP DECT controller that completes the incoming call by sending 200 OK back to the SIP Server and establishes an RTP media stream between Base-station (and Media Gateway from PSTN line). For internal calls the media stream may be routed directly between the involved Base-stations.

15.6 Handover

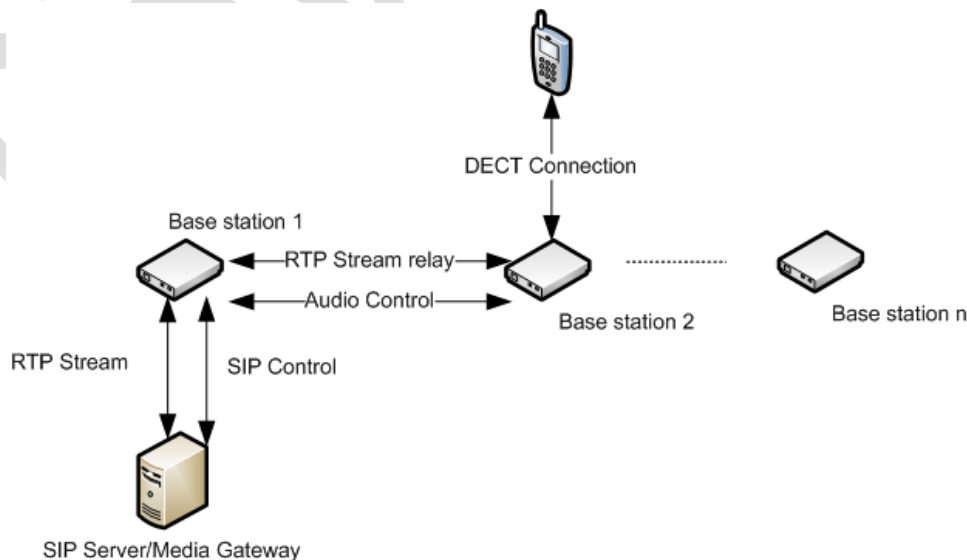
15.6.1 RTP Stream Remains at Initial Base Station

When the call is set up, the handset is located at base station 1. Thus, the DECT communication takes place between the handset and station 1, and the SIP signalling as well as the RTP stream takes place between base station 1 and the SIP server/media gateway. The figure below illustrates this application:



Stage 1: Before handover the handset is located at BS 1.

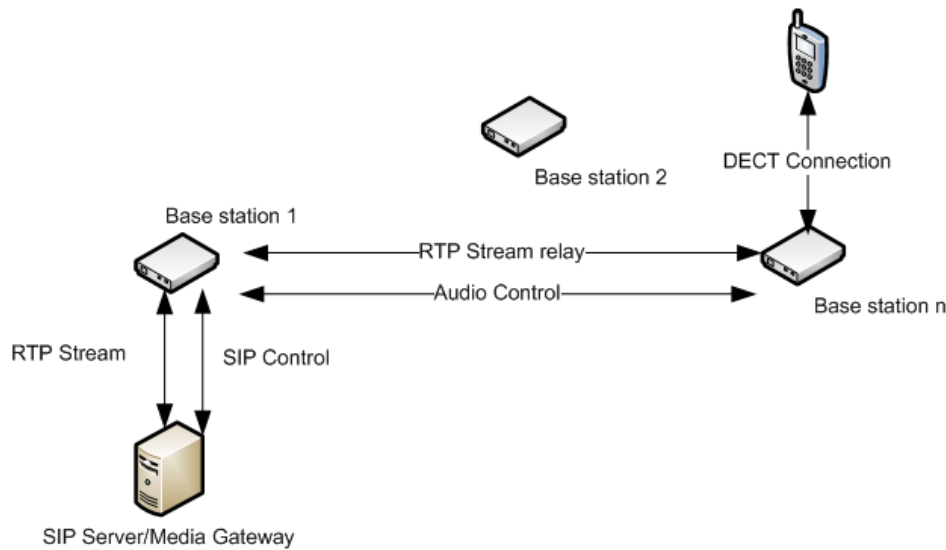
After handover, the handset is located at base station 2, and hence the DECT communication goes on between the handset and base station 2. However, to avoid disruption of the audio, the RTP stream is relayed via the initial base station, since a transfer of the RTP stream to another base station may cause the media gateway (or whatever the remote endpoint is) to re-initialize the RTP stream with a small disruption of the RTP stream as consequence. Thus, from the point of view of the remote endpoint, the RTP stream is not affected by the handover, and since the call control also remains at base station 1 the SIP signalling is also unaffected, as shown below:



Stage 2: After handover to BS 2, the HS is located at BS 2, and the RTP stream is relayed via BS 1.

Since the call control and hence the SIP User Agent remains at the initial base station, the SIP registration is also unaffected by the handover.

If the handset makes yet another handover, the RTP stream will still be relayed via the base station at which, the call was established (here base station 1). This is illustrated as follows:



After handover to BS *n* the handset is located at BS *n*, and the RTP stream is relayed via BS 1.

15.7 Roaming

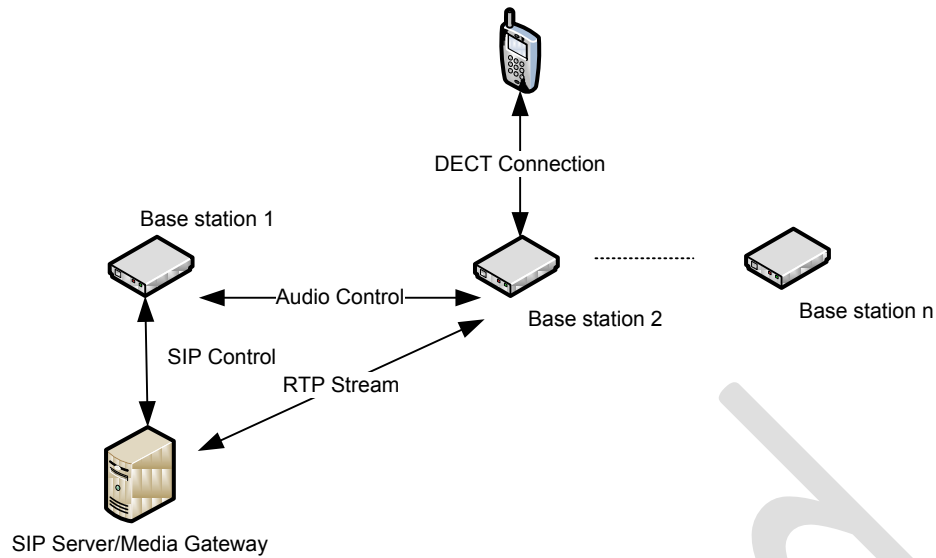
By roaming means the handset moves its SIP and DECT registration from one base station to another base station. Roaming can only be initiated from idle.

Roaming does not immediately result in a new SIP registration, because this may cause a lot of unnecessary signalling. Therefore, the handset will not perform a new DECT Location Registration until it has resided on the same base station for a defined period of time. Since the SIP registration is initiated by the completion of the Location Registration, a new SIP registration will also not be done until this procedure has completed on a new base station. Thus, a handset must stay on the same base station as given in the rules stated below, before a new SIP registration will be made.

Timing Criteria for Location Registration; or roaming will be initiated when:

1. Handsets lose contact to first base unit due to reset/power off/heavy DECT traffic.
2. After 5 minutes (configuration is possible) but before 5+2 minutes
 - a. The plus maximum 2 minutes will occur when service connection traffic is signaled at the same time as location should happen. In this case the location registration procedure will be delayed.

If an incoming call arrives while the handset has moved to another base station (base station 2) but still not performed a new Location Registration, the SIP call will arrive at the initial base station (base station 1), but the RTP stream will be set up between base station 2 and the remote endpoint (refer to figure below). Alternatively, in the case of an outgoing call, the SIP call will be established from the initial base station, and the RTP stream will be set up between base station 2 and the remote endpoint.



An illustration of Handset moving to another base station, but call control is still handled by the initial base station.

16 Operation Setup – Bases/Handsets/SIP Sever

In this chapter, we describe the operation of the base unit and handsets during power up/down. Next we describe the signal flow graphs for some selected operations of the system.

16.1 Power Up

Handset

The handset is still off after the battery has been put into the Handset. The user has to Long Key Press the Red-key (On-hook key) to power up the handset.

If the handset is registered, it will start searching for a base and if the handset is in range of a base, then it will location register to the base.

The handset will display “Unregistered” if the handset isn’t registered. If the handset is not registered, then the user has to enable the registration mode on the base and afterwards register the handset by selecting “Connectivity → Register → *<type in Access code>* → [OK]” on the MMI of handset.

The handset supports connectionless handover between bases and inter-cell handover between a base and repeaters.

Base Station

Power is supplied to the base (gateway) via PoE. The base will start operation when connected to the LAN or WAN. The wireless handset must be registered to the base and a SIP proxy must be configured on the base (refer to Chapter(s) 11,13 for details). The registration mode must be enabled to make it possible to register a handset to the base. The registration mode is enabled on the base by accessing the web-interface on the base. This is done by typing in the IP address of base in the browser on a computer connected to the same network as the base. The user will be prompted for a user name and Password to access the web interface on the base. The user selects an extension via the web interface and click “Register”. The base will afterwards be open for registrations for 5 minutes.

Up to 40 bases can be “linked” together and synchronisation between the bases is done via the air and the network. The base supports up to 10 SIP-proxies and 30 handsets.

16.2 Power Down

Handset

If the Handset loses battery or the battery level is less than a threshold that is in the EEPROM, it goes to power down mode. A battery warning will be given before the handset power down.

Base Station

One of the bases will be a master base and another base will work as fall back base in case of power failure on the master base. All handsets located on a base will be un-located in case of power down of the base. In case of power failure on one of the bases, the user can move to another base area and the handset will then locate on this base and be workable on the new base.

16.3 Call Operations

In this section we describe call procedures in the SME VoIP system. We will narrow our description to call transfer and call conference. Please view accompanied document for detail description of Handset operations [3].

Some Definitions

There are three actors in a given transfer event, each playing one of the following roles:

- **Transferee:** the party being transferred to the Transfer Target.
- **Transferor:** the party initiating the transfer
- **Transfer Target:** the new party being introduced into a call with the Transferee.

The following roles are used to describe transfer requirements and scenarios:

1. **Originator** - wishes to place a call to the Recipient. This actor is the source of the first INVITE in a session, to a Facilitator or a Screener.
2. **Facilitator** - receives a call or out-of-band request from the Originator, establishes a call to the Recipient through the Screener, and connects the Originator to the Recipient.
3. **Screener** - receives a call ultimately intended for the Recipient and transfers the calling party to the Recipient if appropriate.
4. **Recipient** - the party the Originator is ultimately connected to.

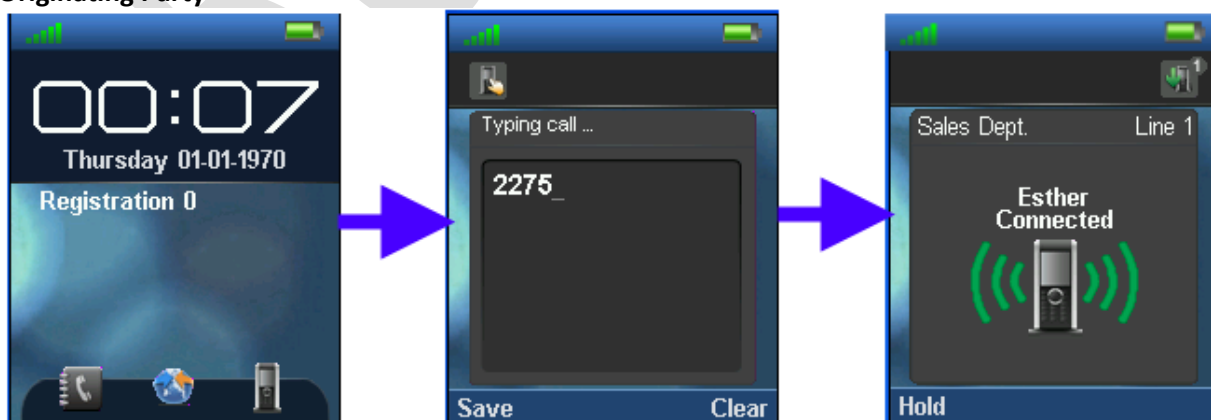
Call Transfer - Requirements

Any party in a call session is able to transfer any other party in that session at any point in that session. The Transferor and the Transferee are not removed from a session as part of a transfer transaction. This requirement is needed so e.g. ring-back on transfer failure will not be lost. The Transferor is aware of whether or not the transfer was successful

16.3.1 Initiating Calls

- Enter Number
- Press Green Button  to start dialling

Originating Party



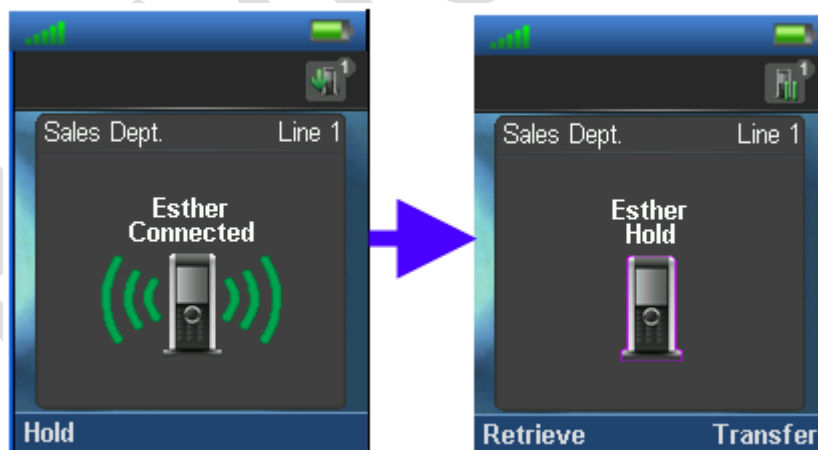
Destination Party

- The destination party must press the Green button available on its handset to accept the incoming call or reject to disallow the call.



16.3.2 Call Holding

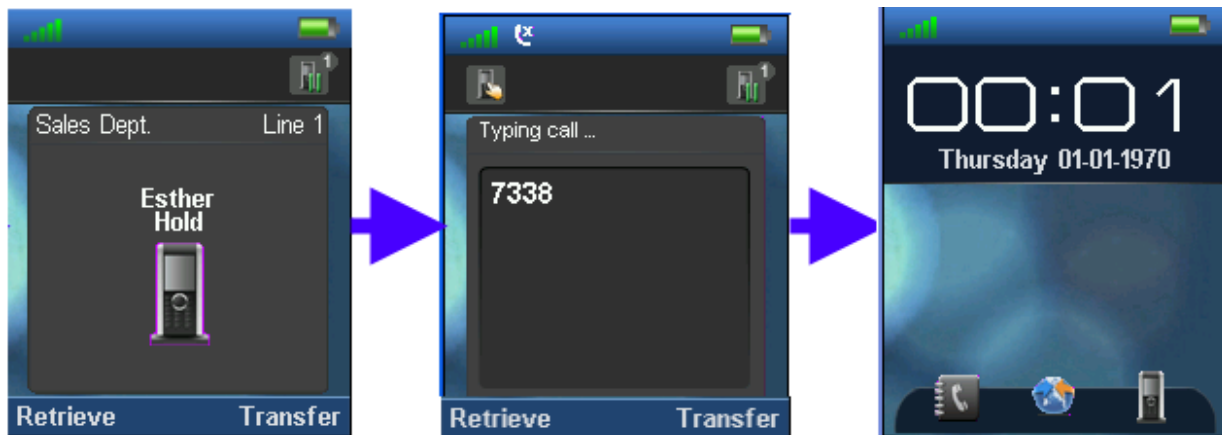
- Press the **Hold** option at the left while call session is in progress or "Connected",
- Press "Retrieve" option to re-connect the call placed on hold



16.3.3 Call Transfer (Blind)

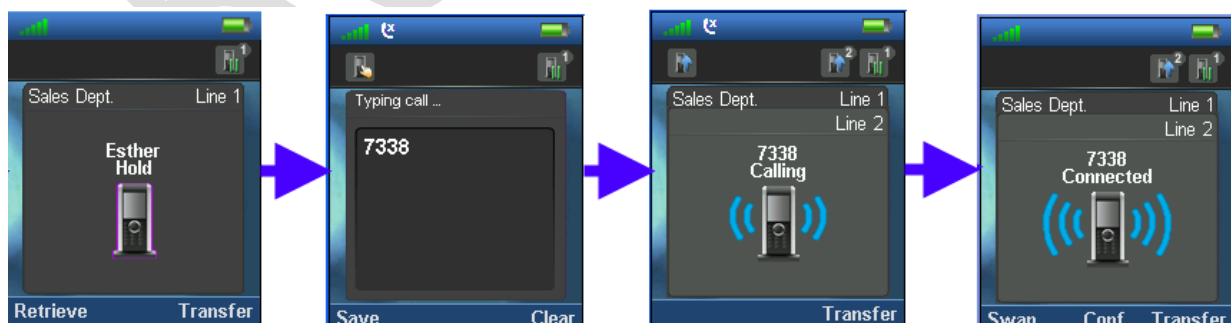
- While “Connected”, press the Hold option, to put the call session on hold (refer to section 16.3.3 “Connected” screen shots).
- Enter the transfer destination number
- Next, Press the “Transfer” option to transfer call session from Originator to the Target Transfer. The Facilitator handset performs transfer procedure and returns to Idle mode (On hook mode)

Facilitator



16.3.4 Call Bridging (Attended Transfer)

- While “Connected”, press the Hold option, to put the call session on hold (refer to section 16.3.3 “Connected” screen shots).
- Enter the transfer destination number and press Green button  to connect/establish call session between Facilitator and the destination party (i.e. Line 2).
- Next, Press the “Transfer” option to transfer call session from Originator (i.e. Line 1) to destination party i.e. “Line 2”
- Handset performs transfer procedure and returns to Idle mode (On hook mode) – i.e. the facilitator handset.



16.3.5 Call Conference (Conference)

- While “Connected”, press the Hold option, to put the call session on hold (refer to section 16.3.3 “Connected” screen shots).
- Enter the transfer destination number
- Press the Green button  to connect/establish call session between Facilitator and Line 2 i.e. the destination party.
- Next, Press the “Conf.” option to establish conference call session between all dialled parties i.e. Originator, Facilitator and Destination party.



17 Handset - Service Menu Management

We seek to describe how to use the “Service Menu” feature available only to vendors and developers of the handset.

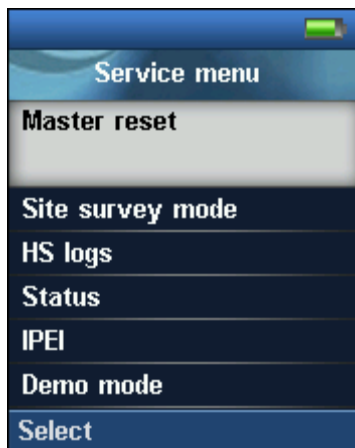
The document will also describe some options available in the Service Menu.

17.1 Service Menu – Site Survey Mode

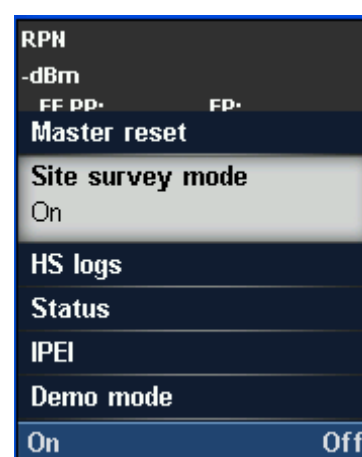
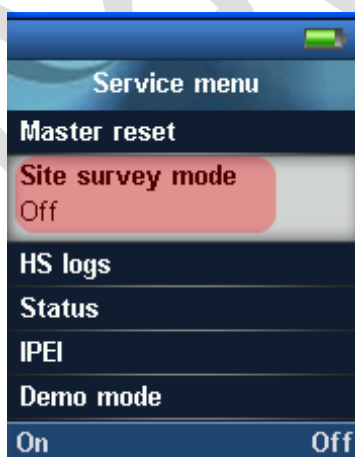
This is normally reserved and used to reveal features not used/seen by the end-user. By means of a special key sequence a special service menu can be accessed. This special menu enables some special feature like Master reset, Site survey mode, Handset logs, Status, IPEI and Demo mode.

To access the service menu, follow these steps:

- STEP 1** Click on Menu  from the Handset > Type ***SERVICE*** or ***7378423*** from the keypad to display the **Service Menu**



- STEP 2** On the **Service Menu** scroll down to the **Site survey mode** > Enable the **Site survey mode** to switch from **Off** to **On**.



This sets the handset in a state to iteratively scan other handsets around it and/or chained to the same base station(s). Handsets in site survey mode can display up to 5 other handsets with the strongest signal strength.

NOTE: If you set the handset to wideband mode, it will not possible to change back

17.2 Service Menu Parameter Definitions

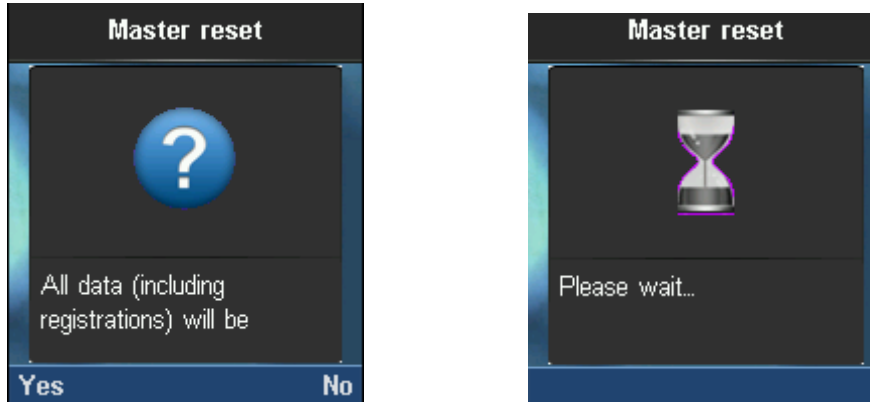
The Service Menu is not for end users – only installers and suppliers.

17.2.1 Master Reset

This feature allows the user to clear any pending errors or events and bring a Handset to normal condition and initial state in a controlled manner.

Valid inputs: Yes or No

Screen shots



17.2.2 Site Survey Mode

In Site Survey Mode the handset MMI shows the RFP (including slave RFP) to which the handset is locked to and the corresponding RSSI.

Valid Inputs: On or Off

Line1: RPN 28 20 03
Line2: -dBm 56 84 78
Line3: FE PP: 1 FP: 4

Parameter/Line	Description
RPN	The line contains the list of base stations identified by the handset or RPNs of the RFP-table entries in respect to the RSSI-values below. Up to 5 RPNs can be displayed. The Radio Fixed Part Number (RPN) is an 8-bit DECT cell identity allocated by the installer. The allocated RPN within a cluster must be geographically unique.
-dBm (Signal Strength)	This indicates the actual field strength information (RSSI) for the base station the current handset is locked to and additional RFPs stored in the RFP-table. RSSI unit is -dBm. The RSSI value of the RFP-table is updated in a 250ms cycle. This causes an update of any entry in a table with 3 RFPs every $3 * 250\text{ms} = 750\text{ms}$. If the RFP could not be synchronized for an RSSI-update, the RSSI value is decreased. This implies that an entry will be deleted after a while, if e.g. the dummy-bearer position has changed or the RFP is unreachable.
FE PP:XX FP:XX	Indicates the number of sync/CRC errors (frame-errors) within the last update cycle. This information is only valid for the existing link to the current handset located to the relevant base station. The PP value is the number of detected Sync/CRC error(s) within the last 100

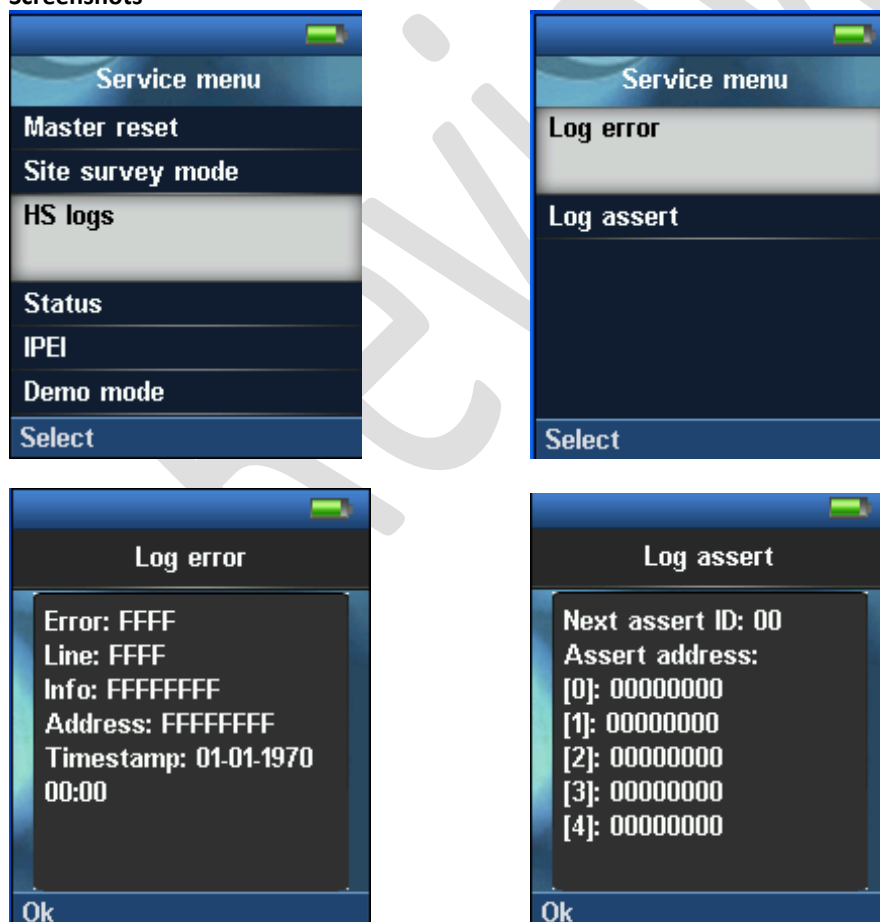
	receiving frames (per sec.). The FP value is the number of received Q1/Q2 bit information within the last 100 receiving frames (per sec.). This information is interpreted as Sync and CRC errors on the base station receiving side.

17.2.3 HS Logs

The HS log is a debugging feature that allows the user to retrieve low level interesting messages from the handset.

HS Logs	Description
Log error	These are debug error logs retrieved from the PP log file. The last log retrieved is formatted into: Error: This error code. Line: Location within the software code which triggered this error. Address: Register bank and/address from which error occurred.
Log Assert	This reports of the function/exception handler that run after an erroneous state in handset operation. Next assert ID: Immediate exception handler ID to be run when a specific error occurs. Assert address: Register bank and/address where an exception handler is executed as a result of the error which occurred.

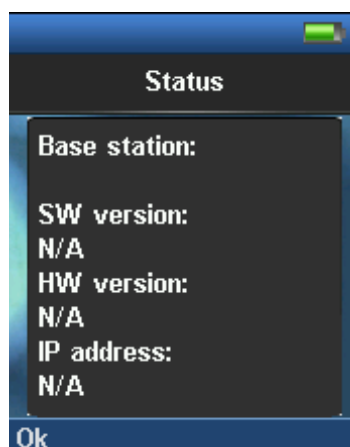
Screenshots



17.2.4 Status

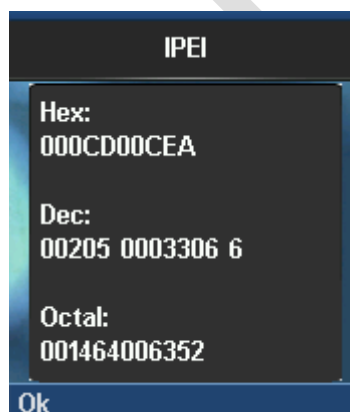
This provides the present condition of the handset and the base station it is location registered to. Some of the information available in this mode is described in the table below (this information is updated during location request update from the DECT system).

Parameter	Description
SW Version	Base station: Current firmware installed on the current Base station the Handset is location registered to. Handset: firmware presently installed in the handset. Format: Version Date Stamp (e.g.: 00.21 01-07-2010 00:00)
HW Version	Current hardware module used in base station and handset.
DECT Band	Operating frequency of system. DECT band includes UA, EU, LTAM, SA, N.A options.
IP Address	IP address of base station and handset
MAC Address	HW address of base station.
System Name	Name describing the SME network. Typically a string of 16 bytes.
Battery Level	Current handset battery energy position



17.2.5 IPEI

The IPEI (International Portable Equipment Identity) is a unique identification of portable part (handset) and DECT Repeater. The IPEI is formatted and displayed in HEX, OCT, and OCT nomenclatures.



17.2.6 Demo mode

The demo mode uses animations to show the user which functions the DECT phone offers (with/without connection to the SIP server).

Reviewed

Appendix

Reviewed

18 Appendix A

Handset



Base Station



Web interface

Home/Status

Extensions

Servers

Network

Management

Firmware Update

Time

Country

Security

Contact List

Multi cell

Settings

Debug Log

SIP Log

Logout

SME VoIP Configuration

Welcome

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

System Information:
Phone Type:
System Type:
RF Band:
Current local time:
Operation time:
RFPI-Address:
MAC-Address:
IP-Address:
Firmware-Version:
Firmware-URL:

Multi Cell Ready(Passive) Master
IPDECT HW ver 00
Generic SIP (RFC 3261)
EU
12/Nov/2010 13:40:56
00:34:34 (H:M:S)
116E606600; RPN:00
00087b077cd9
192.168.10.101
IPDECT/00.54//12-Nov-10 09:14
tftp://10.10.104.63/FwuFiles

SIP Identity Status on this Base Station:
123 Ext002@192.168.10.10:5080
185 Ext001@192.168.10.10:5080
143 Ext003@192.168.10.10:5080

Identity 1 Status:

OK

Identity 2 Status:

OK

Identity 3 Status:

OK

Press button to reboot.

Reboot

Copyright© 2010, RTX Products

Charge unit



Reviewed