Product Document

OpenMobility SIP Installation, Administration and Maintenance

Document ID: pm-0504

Aastra DeTeWe
Zeughofstr. 1
10997 Berlin, Germany

History

Version	Reason / Version	Date	Author
1 / 0	Initial release.	30.11.2006	H. Zander
1 / 2	Draft removed	30.11.2006	Tielmann

Additional Information:

Tool:	Microsoft Office 2000 SP3
Print Date:	30.11.2006

Table of contents

1 Overview

1.1 Purpose

This document describes the service interfaces of the OpenMobility Manager. In this version only the DECT relevant service issues are described.

1.2 Abbreviations and definitions

1.2.1 Abbreviations

AC	Authentication Code
ADPCM	Adaptive Differential Pulse Code Modulation
DECT	Digital Enhanced Cordless Telecommunication
DHCP	Dynamic Host Configuration Protocol
DSP	Digital Signal Processor
FCC	Federal Communications Commission
GAP	Generic Access Profile
IPEI	International Portable Equipment Identity
HTTP	Hyper Text Transfer Protocol
OMM	OpenMobility Manager
PARK	Portable Access Rights Key
PP	Portable Part (DECT handset)
SNMP	Simple Network Management Protocol
TFTP	Trivial File Transfer Protocol
RFP	Radio Fixed Part
RTCP	Real Time Control Protocol
RTP	Real Time Protocol
TFTP	Trivial File Transfer Protocol

1.2.2 Definitions

Asterisk **Asterisk**

Asterisk is a complete Open Source PBX in software. It runs on Linux, BSD and MacOSX and provides many features. Asterisk supports voice over IP in many protocols, and can interoperate with almost all standards-based telephony equipment.

DECT **Digital Enhanced Cordless Telecommunication**

- The standard (ETS 300 175) essentially specifies the air interface, known as the radio interface. Voice and data can both be transmitted via this interface.
- Its technical key characteristics are:
  - Frequency range: approx. 1,880 – 1,900 GHz (approximately 20 MHz bandwidth)
  - 10 carrier frequencies (1,728 MHz spacing) with 12

time slots each)

- Doubling the number of time slots (to 24) using the TDMA process
- Net data rate per channel of 32 kbps
  (for voice transmission using ADPCM)
- Voice coding using the ADPCM method
- Maximum transmission power of 10 mW

GAP

Generic Access Profile

- GAP is the abbreviation for Generic Access Profile
- The GAP standard (ETS 300 444) is based on the same technology as DECT, but is limited to the most important basic features. This standard was created in order to allow telephones of different vendors to be used on any type of DECT system. It thus represents the smallest common denominator of all manufacturer-specific variants of the DECT standard.
- An important limitation in the GAP standard is that external handover is not possible. For this reason connection handover is used, which is supported by GAP terminals.
- The operation of GAP-capable telephones is comparable to that of analogue terminals. For example, features can be called up via '*' and '#' procedures.

Handover

Handover

A handover is similar to roaming, but occurs during an ongoing call. A handover normally takes place “in the background”, without disrupting the call (seamless handover).

IPEI

International Portable Equipment Identity

- 13-digit identification code for PPs
- Example: 00019 0592015 3
  (the final digit is the checksum).
- The code is represented in decimal form.
- This code is globally unique.

PARK

Portable Access Rights Key

Access code for the Portable Part. This code determines whether a PP can access a particular DECT system. Used for unique selection of the system at enrolment.

Roaming

Roaming

While in motion, the PP performs ongoing measurements to determine which RFP is best received. The one that can be best received is defined as the active RFP. To prevent the PP from rapidly switching back and forth between two RFPs that can be almost equally well received, certain threshold values are in effect. (similar to a Schmitt trigger circuit)

1.3 References

/1/ RFC 1350, The TFTP Protocol, Revision 2, July 1992

/2/ RFC 1889, RTP: A Transport Protocol for Real-Time Applications, January 1996

/3/ RFC 2030, Simple Network Time Protocol (SNTP) Version 4 for IPv4, IPv6 and OSI, October 1996

/4/ RFC 2131, Dynamic Host Configuration Protocol, March 1997

/5/ RFC 2327, SDP: Session Description Protocol, April 1998

/6/ RFC 2474, Definition of the Differentiated Service Field (DS Field) in the IPv4 and IPv6 Headers, December 1998

/7/ RFC 2617, HTTP Authentication: Basic and Digest Access Authentication, June 1999

/8/ RFC 3164, The BSD Sys Log Protocol, August 2001

/9/ RFC 2833, RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals, May 2000

/10/ RFC 3261, Session Initiation Protocol (SIP), June 2002

/11/ RFC 3264, An Offer/Answer Model with Session Description Protocol (SDP), June 2002

/12/ RFC 3420, Internet Media Type message/sipfrag, November 2002

/13/ RFC 3515, The Session Initiation Protocol (SIP) Refer method, April 2003

/14/ RFC 3665, The Session Initiation Protocol (SIP) Basic Call Flow Examples, December 2003

/15/ RFC 3842, A Message Summary and Message Waiting Indication Event Package for the Session Initiation Protocol (SIP), August 2004

/16/ RFC 3891, The Session Initiation Protocol (SIP) “Replaces” Header, September 2004

/17/ RFC 3892, The Session Initiation Protocol (SIP) Referred-By Mechanism, September 2004

/18/ OpenMobility Diagnostic Tools

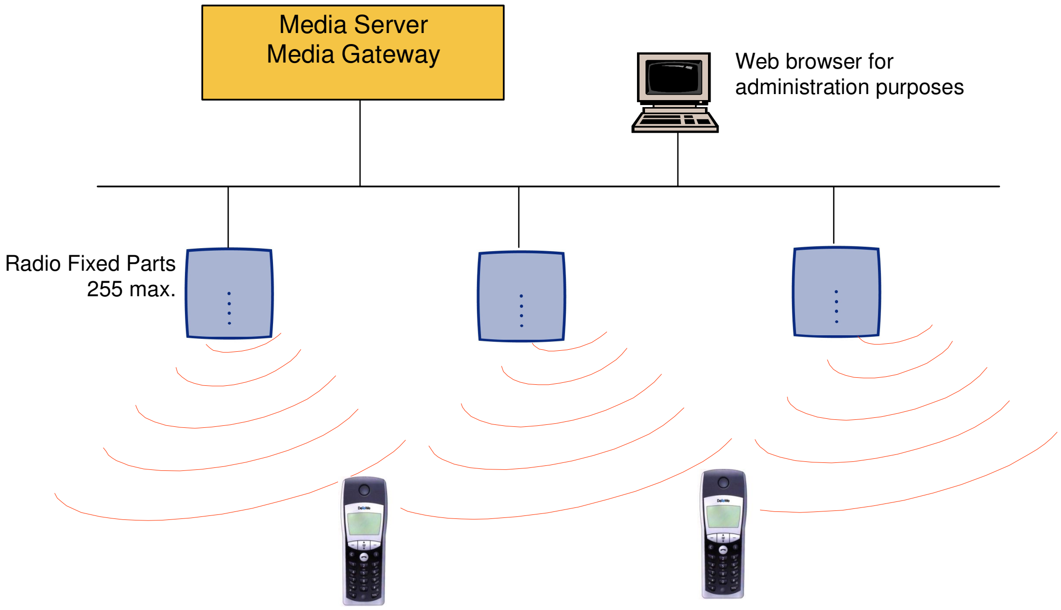
2 Introduction

2.1 About the IP DECT wireless solution

The DECT over IP system comprises the following components:

- DECT Radio Fixed Parts (RFP) being distributed over an IP network and offering DECT as a wireless interface.
- Media server / media gateway as telephony system platforms (e.g. Asterisk).
- Portable Parts (PP): Aastra Phone 142.
- OpenMobility Manager (OMM): Management interface for IP DECT wireless solution, which runs on one of the Radio Fixed Parts.

The following pictures give a graphical overview of the architecture of the IP DECT wireless solution:



The media server, media gateway, OMM and the RFPs communicate through the IP infrastructure. The RFPs and the Portable Parts communicate over air, where the DECT GAP protocol is used or DECT GAP with proprietary enhancements.

2.2 About the RFPs

In general all RFPs have the same hardware and software capabilities. But please mind the differences in regulatory domains which exist for North America and all other areas of the world . These domains lead to different RFP variants which use specific frequency bands and field strengths:

- RFP 32 IP or RFP 34 IP (EMEA)
  - Frequency Band 1.880 to 1.900 Mhz
  - 10 carrier frequencies
  - Transmit Power 24 dBm

- RFP 32 US or RFP 34 US (NA)
  - Frequency Band 1.920 to 1.930 Mhz
  - 5 carrier frequencies
  - Transmit Power 20 dBm

One of the RFPs within an IP DECT installation must be chosen to operate not in the RFP mode, only, but also in the OpenMobility Manager (OMM) mode. During installation you must set one of the RFPs to OMM mode. The others are set to RFP only mode.

RFP only mode

Within this mode the RFP converts IP protocol to DECT protocol and then transmits the traffic to and from the handsets over a DECT time slot. On air the RFP has 12 available time slots, 8 can have associated DSP resources for media streams, the remaining 4 time slots are used for e.g. control signalling between RFPs and the PPs.

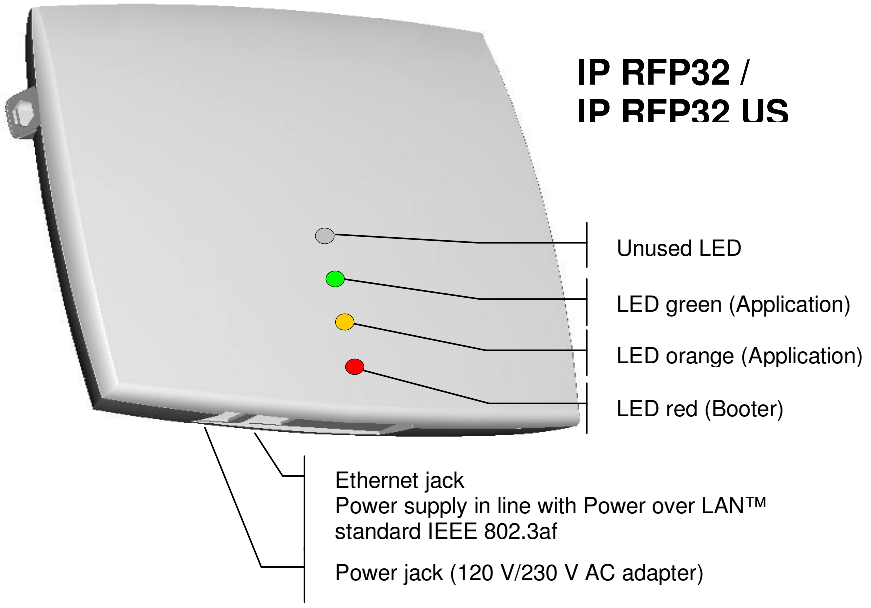
Groups of RFPs have to be built which are named clusters. Within a cluster RFPs are synchronized to enable a seamless handover, when a user crosses from one RFP’s zone of coverage to another. For synchronization it is not necessary for an RFP to communicate directly with all other RFPs in the system. Each RFP only needs to be able to communicate with the next RFP in the chain. But it is preferable for a RFP to see more than one RFP to guarantee synchronization in the event that one of the RFPs fails.

The 4 control signalling channels are also used to carry bearer signals that signal the handset to start the handover process. If the radio signal of another RFP is stronger than that of the current RFP, then the handset starts the handover process to the RFP that has the stronger signal as the user moves around the site.

OpenMobility Manager mode

In this mode a RFP functions as a regular RFP. Additionally it is responsible for SIP signalling between the IP DECT system and the telephony or media server. Further on it takes over the management part of the IP DECT solution. You designate a RFP as the OMM by assigning an IP address to the RFP within the DHCP scope (see 3). After a RFP is designated as the OMM, it starts the extra services on board (for example, the web service that supports the management interface).

Note: It is possible to deactivate the DECT part of a RFP. If the DECT interface is deactivated then the resources (CPU and memory) are available for the OMM.



2.3 OpenMobility Manager

The OpenMobility Manager (OMM) performs the following tasks:

- Signalling gateway (SIP <-> DECT).
- Media stream management.
- Managing sync-over-air functions between RFPs.
- Facilitating system configuration modifications.

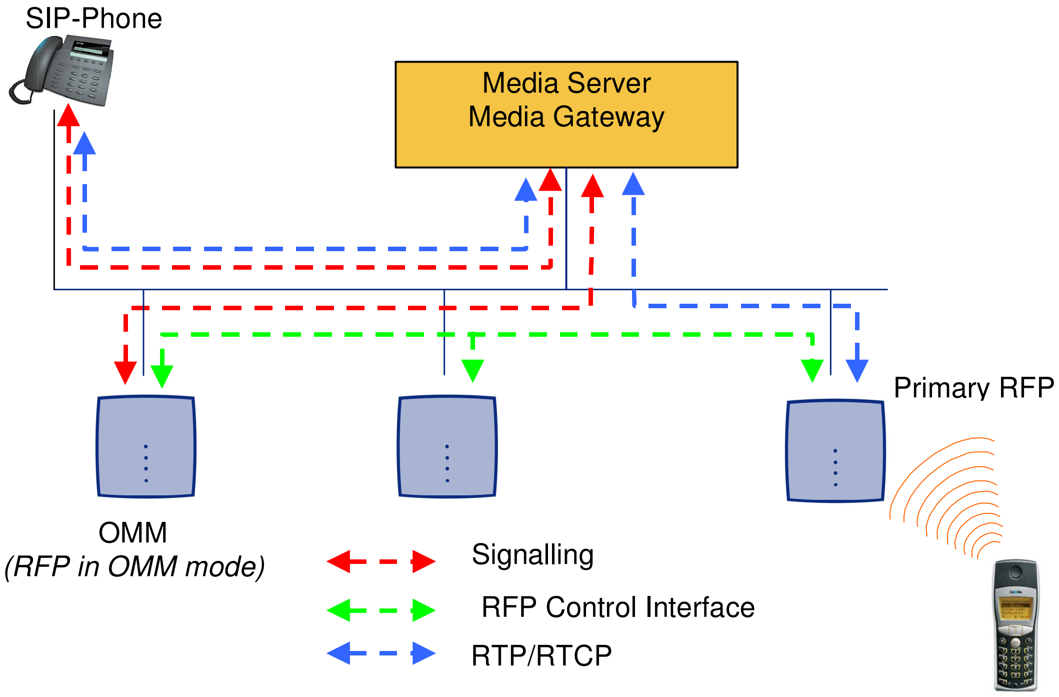
The OpenMobility Manager (OMM) may run on one of the RFPs or on a dedicated Linux server.

2.4 IP signalling and media stream

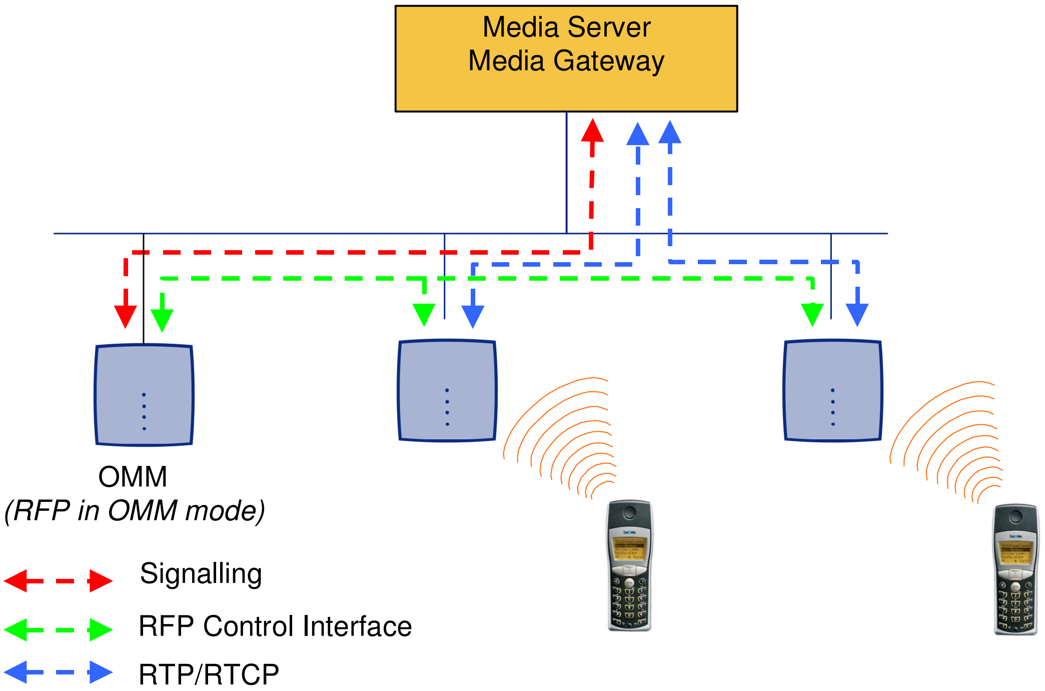
To establish a call between an IP Phone and a PP, the following IP streams must be established:

- A signalling channel to and from the SIP phone.
- A signalling channel to and from the OMM.
- A control interface between the OMM and the RFP that has a connection to the PP (known as the primary RFP).
- A Real Time Protocol (RTP) / Real Time Control Protocol (RTCP) connection between the SIP phone and the media gateway and then a RTP/RTCP connection between the media gateway and the RFP.

The following figure illustrates this scenario.



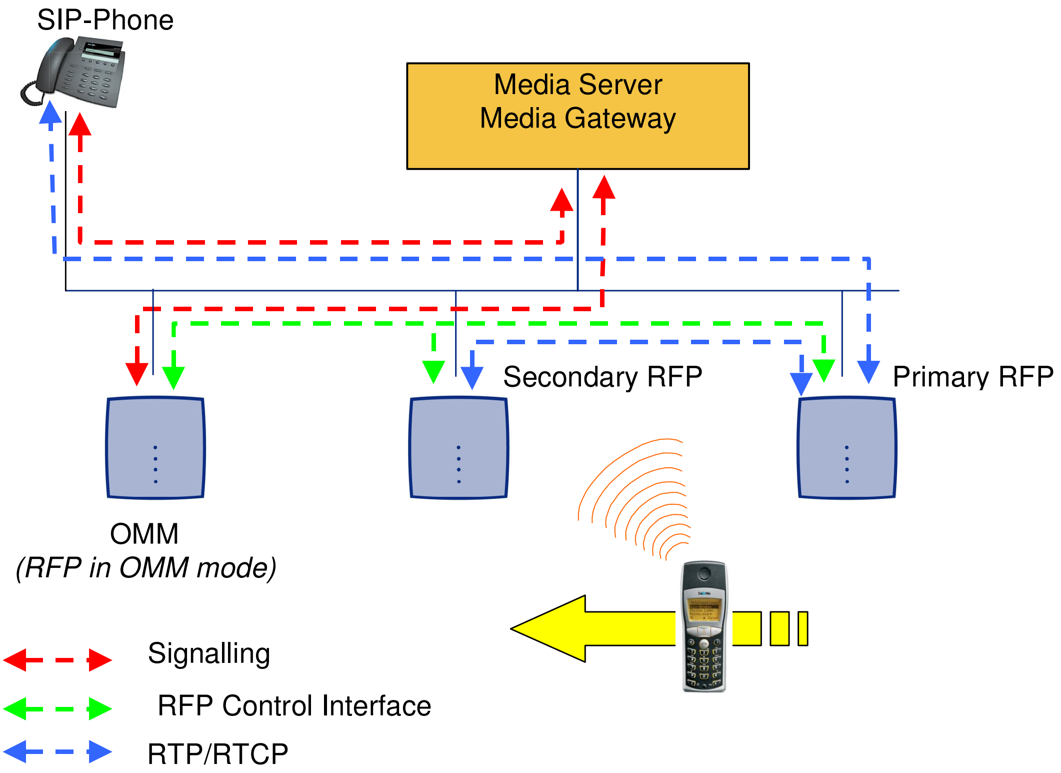
To establish a call between two PPs the same IP streams must be established like in the scenario before, except the IP phone is not involved. The following figure illustrates this scenario.



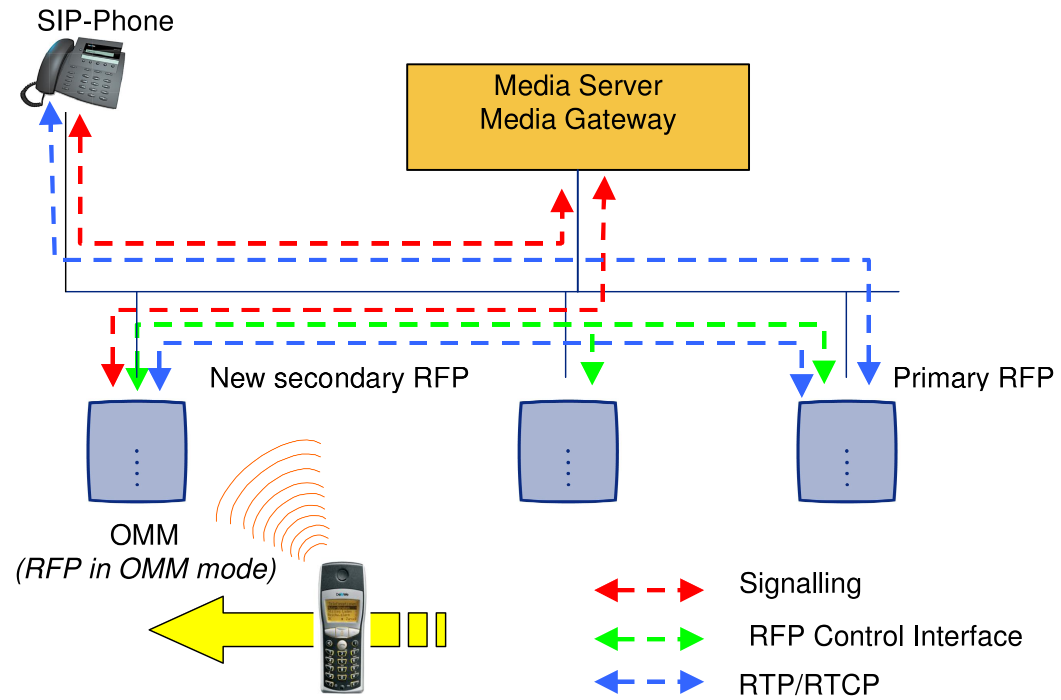
A call from one PP to another that resides on the same RFP will loop back within the RFP, if no media gateway is involved. So the call will not pass through to the Local Area Network (LAN). Although the voice packets will not impact LAN traffic, signal packets will.

It is also be possible to direct the media stream to connect directly the IP phone and the RFP, as shown in the following figures.

If the PP user is moving, the PP detects that another RFP has a better signal strength and, therefore, it starts the handover process. The media stream from the IP phone cannot move to the secondary RFP, so the primary RFP uses the LAN to direct the voice to the secondary RFP, as shown in the following figure.



As the PP user moves into the next RFP zone of coverage, the PP detects that the RFP has a better signal strength. Again the media stream from the SIP phone cannot move to the secondary RFP, so the primary RFP uses the LAN to direct the voice to the new secondary RFP.



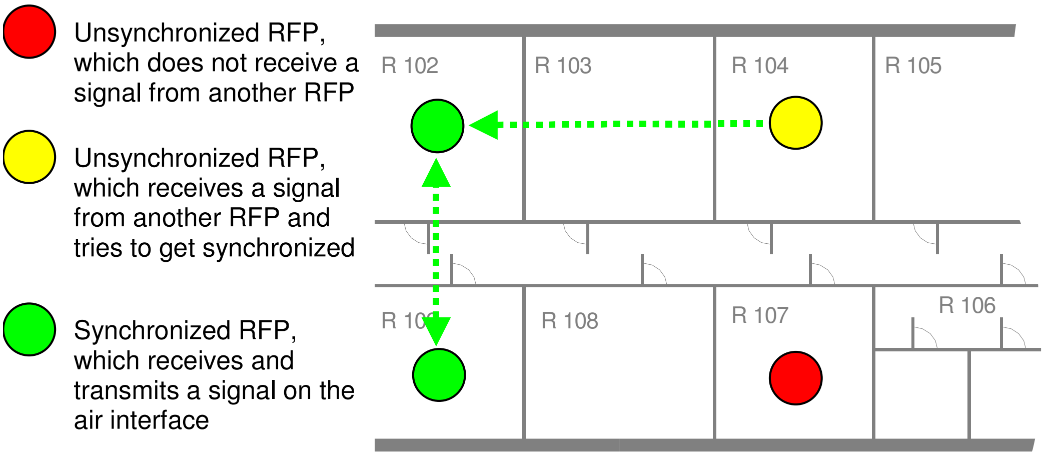
2.5 RFP Synchronization

To guarantee a seamless handover if a caller moves from one RFP zone of coverage to another RFP zone of coverage, an accurate synchronization of the RFPs is necessary.

The RFPs are synchronized over the air interface. During start up one RFP will be the first, which transmits a signal on the air. The other RFPs only receive the signal until their are synchronous. If a RFP gets in sync then it will transmit a signal on the air and will be the sync source for the next RFPs. Only RFPs which can receive each other will be synchronized.

For the RFP to sync to another RFP the signal strength cannot drop below –70 dBm. You must consider this requirement during the site survey.

The first active RFP will be chosen by the ADMM.

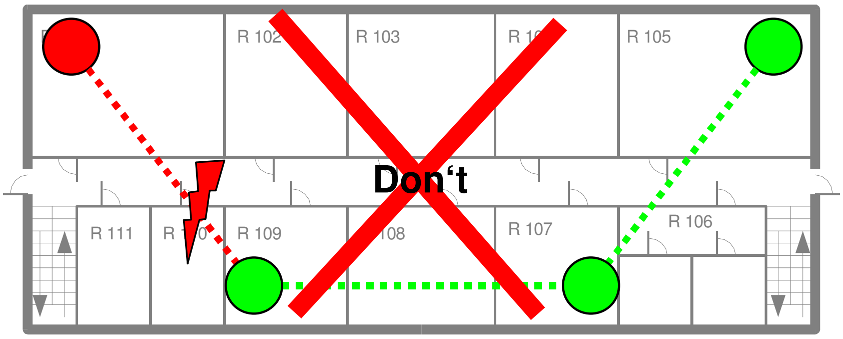

Unsynchronized RFP, which does not receive a signal from another RFP
Unsynchronized RFP, which receives a signal from another RFP and tries to get synchronized
Synchronized RFP, which receives and transmits a signal on the air interface
R 102
R 103
R 104
R 105
R 10
R 108
R 107
R 106

As long as a RFP is not in sync, no calls can be established using this RFP.

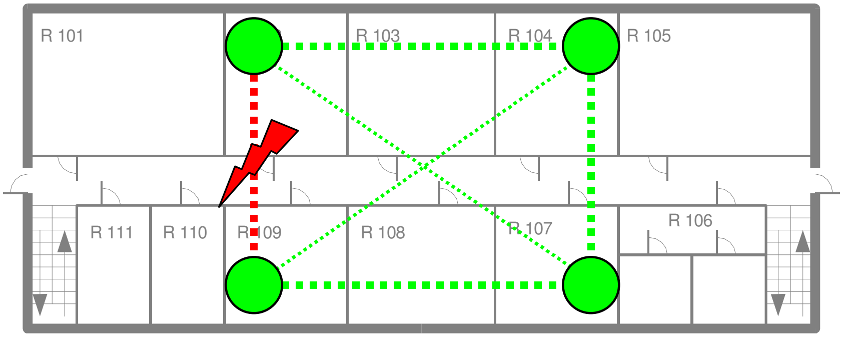
If a RFP loses the synchronization the RFP does not accept new calls (“busy bit”). There is a delay of maximum 3 minutes until the active calls on this RFP are finished. Then it tries to get synchronized again.

An IP DECT installation is more reliable if a RFP can receive the signal from more than only one RFP, because the other signals are also used for synchronization.

Unreliable Installation



Reliable Installation



The sync-over-air solution is very reliable, because all existing redundant paths are used for synchronization. Thus, hardware tolerances have only very little influence. No RFP has a key position.

Only unfavourable setups without redundant synchronization paths can cause problems.

Sometimes RFPs do not need to be synchronized, e.g. if they are in different buildings. These RFPs can be put into different clusters. RFPs in different clusters will not be synchronized with each other. Different clusters startup at the same time independently.

2.6 RFP channel capacity

The RFP has 12 available air time slots:

- 8 slots can have associated DSP resources for media streams.
- The remaining 4 slots are used for e.g. control signalling between RFPs and PPs.

If all 8 media stream channels are used IP DECT announces a “busy bit”. In that case the PPs determine whether another RFP has an appropriate signal strength. If so, the PP will handover to that RFP. Once the handover has been completed, the RFP will then lower its “busy bit”.

Whenever the busy state is announced a log entry is made to the system logs. If the announcement of busy raises in a specific area, a further RFP should be installed to double the number of media streams available for calls.

2.7 About the Portable Parts

Please mind the differences in regulatory domains which exist for North America and all other areas of the world . These domains lead to different PP variants which use specific frequency bands and field strengths:

- Aastra Phone 142 (EMEA)
  - Frequency Band 1.880 to 1.900 Mhz
  - 120 duplex channels
  - 10 mW (average output per active channel)

- Aastra Phone 142 US (NA)
  - Frequency Band 1.920 to 1.930 Mhz
  - 60 duplex channels
  - 5 mW (average output per active channel)

In addition to the Aastra Phone 142 also standard 3rd party DECT GAP phones function on the IP DECT solution. But the functionality may be limited by the characteristics of the 3rd party DECT phone.

2.8 About licensing

The OMM needs to be enabled with a license key, which depends on the MAC address of some RFPs in the DECT system. The license key needs to be entered / administered via the OMM web interface.

There are a sets of licenses with additional upgrade licenses:

- License for 1 to 2 RFPs
- License for more than 2 RFPs

As mentioned above the license key depends on the MAC addresses of some RFPs of the DECT system (License RFPs). Each RFP can be a License RFP independent from where the RFP is located. The number of RFP MAC addresses encoded in the license depends on the size of the DECT installation.

System size (# of RFPs)	**Number of RFP MAC addresses encoded in the license (License RFPs)**
1	1
2	2 (1, if a second RFP has been added to a single RFP system)
More than 2	3

Additional to the MAC addresses the PARK (Portable Access Rights Key), which identifies the DECT installation, is also part of the license. Because a DECT system can only be operated with a valid PARK, a DECT installation without a license will be inactive on the DECT side.

An IP DECT system is operational, if it is set up with a license and the RFPs, which are encoded in the license are part of the system so that the OMM can communicate with these License RFPs.

Depending on the size of the IP DECT system, it will still work if some License RFPs are out of service.

System size (# of RFPs)	**Number of License-RFPs**	**Number of License RFPs available at minimum**
1	1	1
2	2	1
More than 2	3	2

If the minimum number of License RFPs cannot be reached by the OMM or more RFPs are administered than licensed the DECT system will block the voice streams.

2.9 System capacities

There is only one OpenMobility Manager (OMM) in the system. The OMM capacities are:

- Up to 256 RFPs can be controlled.
- Up to 512 PPs are handled.

It is possible to deactivate the DECT part of a RFP. If the DECT interface is deactivated then the resources (CPU and memory) are available for the OMM only.

3 Installation and configuration

To establish and maintain an IP DECT installation, a network infrastructure is assumed, which comprises at least the following components:

- RFPs
- PPs
- media server (e.g. Asterisk)

The following services should be provided:

- TFTP
- DHCP
- Syslog daemon

3.1 OpenMobility start up

3.1.1 Start up of the RFPs

For booting a RFP there must at least a TFTP server on the attached network to load the application software.

The essential network settings can be alternatively

- given by a DHCP server at startup time.
- configured on the RFP with the tool OM Configurator. The settings made by the OM Configurator will be saved permanently in the internal flash memory.

The RFP gets the boot image file from a TFTP server. The used TFTP server needs to support /1/. A used DHCP server needs to support /4/.

The TFTP and DHCP server need not to reside on the same host.

3.1.1.1 Booting overview

Booting is performed in two steps:

1. Starting the boot process.
2. Starting the application.

Booter

The RFP has only a little standalone application built into the flash. This software realizes the so called net boot process.

On startup each IP DECT Base Station tries to determine its own IP address and other settings of the IP interface from the configuration settings in the internal flash memory. If no settings are available or these settings are disabled, the IP DECT Base Station tries to determine these settings via DHCP.

The RFP gets the application image file from the TFTP server.

Application

After starting the application image the IP DECT Base Station checks the local network settings in its internal flash memory once again. If no settings are available or if they are disabled it starts a DHCP client to determine the IP address of the ADMM and other startup settings.

3.1.2 Start up of the OpenMobility Manager

There is no difference in booting that RFP, which is chosen to be running in OMM mode from those which are in the RFP only mode.

The decision is driven by the OMM IP address, which is read

- within the local network settings, if active.
- via DHCP request.

The IP DECT Base Station which has the same IP address as the dedicated OMM IP address, is running as the OMM.

3.1.3 Booter

3.1.3.1 DHCP client

Within the initial boot process the DHCP client supports the following parameters:

• IP address	mandatory
• Netmask	mandatory
• Gateway	mandatory
• Boot file name	mandatory
• TFTP server	mandatory
• Public option 224: “OpenMobility”	mandatory

3.1.3.1.1 DHCP request

3.1.3.1.1.1 Vendor class identifier (code 60)

The DHCP client sends the vendor class identifier “**OpenMobility**”.

3.1.3.1.1.2 Parameter request list (code 55)

The DHCP client in the booter requests the following options in the parameter request list:

- **Subnet mask option (code 1)**
- **Router option (code 3)**
- **Public option 224 (code 224)**
- **Public option 225 (code 225)**
- **Public option 226 (code 226)**

3.1.3.1.2 DHCP offer

The DHCP client selects the DHCP server according to the following rules:

- the **public options** (**code 224**) has a value equal to the string "**OpenMobility**".

or

- the **file** field in the DHCP message has a sub string equal to "ip_rfp.cnt".

If none of the two rules above match the DHCP offer is ignored.

Information retrieved from the DHCP offer:

- The IP address to use is taken from the **yiaddr** field in the DHCP message.
- The IP netmask is taken from the **subnet mask option (code 1).**
- The default gateway is taken from the **router option (code 3).**
- The TFTP server IP address is taken from the **siaddr** filed in the DHCP message.
- The boot image filename is taken from the **file** field in the DHCP message, if this field is empty the default filename "iprfp.bin" is used.

3.1.3.1.3 Retries

If the DHCP client does not get an appropriate DHCP offer a new DHCP request is send after 1 second. After 3 DHCP requests are sent the DHCP client will sleep for 60 seconds.

During this time the booter will accept a local configuration with the OpenMobility Configurator (OMC).

3.1.3.2 TFTP client

The TFTP client will download the application image from the TFTP server. Both TFTP server and the name of the application image are supplied via the DHCP client. The application image is checksum protected.

3.1.4 Application

After successfully downloading and starting the application the RFP will determine the IP address of the OMM from DHCP.

The DHCP client is capable of receiving broadcast and unicast DHCP replies. Therefore the flags field is **`0x0000`**.

The DHCP request contains the well-known magic cookie `(0x63825363)` and the end option `(0xFF).`

The following parameters will be supported within this step:

Option / Field	Meaning	Mandatory
yiaddr	IP-Address of the IP-RFP	yes
siaddr	IP-Address of the TFTP server	yes
file	Path and name of the application image	yes

code 1	Subnet mask	yes
code 3	Default Gateway	yes
code 6	Domain Name Server	no
code 15	Domain Name	no
code 42	IP-Address of a NTP server	no
code 43	Vendor Specific Options	yes
public option 224	Must set to "OpenMobility".	yes

The *Vendor Specific Options* consist of:

Vendor Specific Option	Meaning	Mandatory
option 10	ommip: Used to select the IP-RFP who should reside the Open Mobility Manager (OMM)	yes
option 14	syslogip: IP-Address of a Syslog Daemon	no
option 15	syslogport: Port of a Syslog Daemon	no
option 17	country: Used to select the country in which the OMM reside. This enables country specific tones (busy tone, dial tone, ...)	no
option 18	ntpservname: Name of a NTP Server	no

Tones for the following countries are supported:

country code	country
1	Germany
2	Great Britain
3	Suisse
4	Spain
6	Italy
7	Russia
8	Belgium
9	Netherlands
10	Czechia
14	Finland
16	Poland
25	Taiwan
100	USA
101	France

3.1.4.1 Booter update

3.1.4.1.1 Automatic booter update

Each application SW comes with the latest released booter SW. The application SW will update the booter automatically as long as the major release number of the booter SW has not changed, e.g booter SW 2.1.2 will not be automatically updated by the booter SW 3.x.y, but the booter SW 3.0.0 will be automatically updated by the booter SW 3.1.0.

Details on how to check the booter SW version, see 4.1.

Details on how to update the booter manually, see 4.1.2.

3.1.4.1.2 Automatic booter update for major release changes

The update of booters with a major release number change will be performed automatically when the DHCP client in the application receives an DHCP offer with the public option 254 with a value “UPDATE”.

3.1.4.2 Selecting the right DHCP server

The DHCP client requests its own IP address using code 50. The DHCP client will select the DHCP server that offers the currently used IP address. Additionally the mandatory options must be offered otherwise the DHCP offer is ignored by the DHCP client.

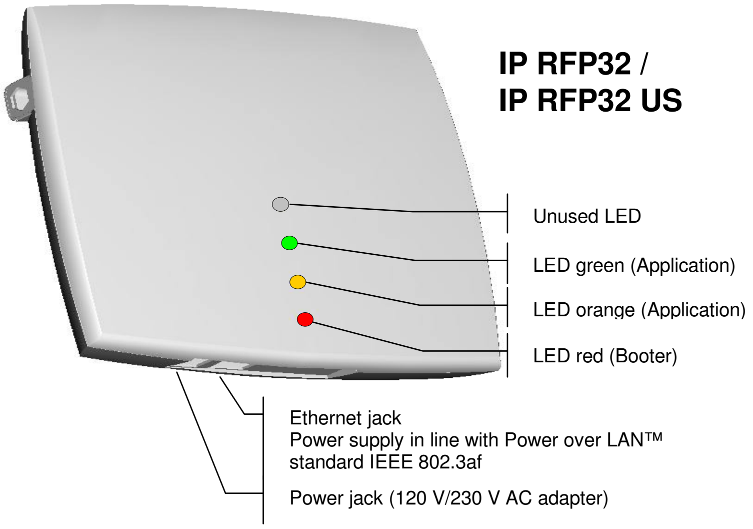
If no matching reply was received the DHCP client resends the request for 2 times after 1 second. Then the DHCP client will wait for 1 minute before resending 3 requests again.

If the DHCP client cannot accept an DHCP offer within 3 minutes the RFP is rebooted.

3.1.5 RFP LED status

The following diagram shows the LED status of a RFP according to the different states during start up.

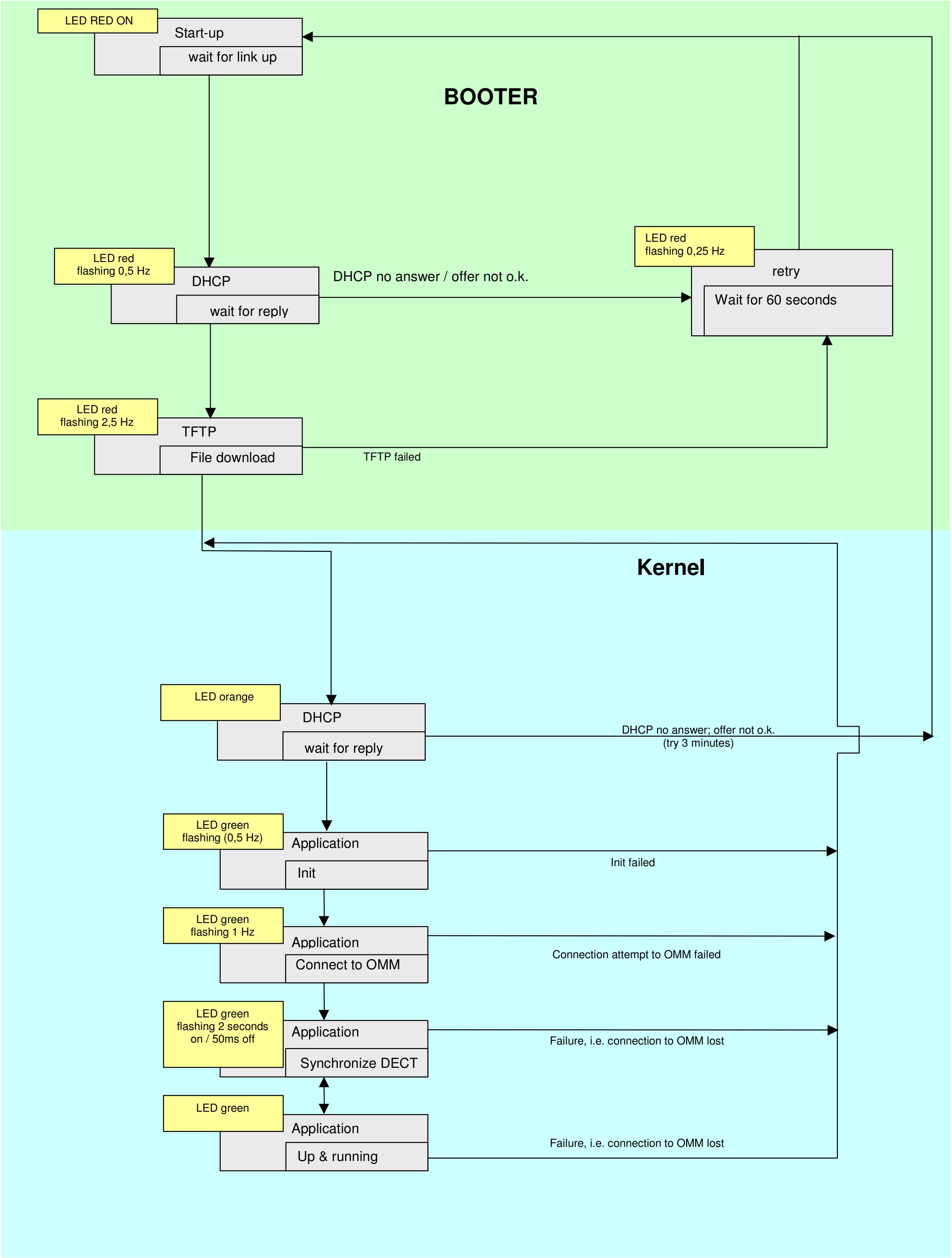
The RFP32 IP has three separate LEDs for red, orange and green to show the different states during start up.



State	LED state	Remarks
Booter (Start up)	Red on	Waiting for link up
Booter DHCP	Red flashing 0.5 Hz	Launching a DHCP request and waiting for an DHCP offer
Booter (TFTP)	Red flashing 2.5 Hz	Downloading the application image
Application (DHCP)	Orange on	Launching DHCP request and waiting for DHCP reply
Application (init)	Green flashing 0.5 Hz	RFP is initializing its internal components
Application (init)	Green flashing 1 Hz	RFP tries to connect to the OMM

State	LED state	Remarks
Application (init)	Green flashing (2 sec on, 0.5 sec off)	The DECT part of the RFP does not work (either not configured or not synchronized with other RFP's)
Application (init)	Green	RFP is up and running

3.1.6 State graph of the start up phases



3.2 Static local configuration of the IP DECT Base Station

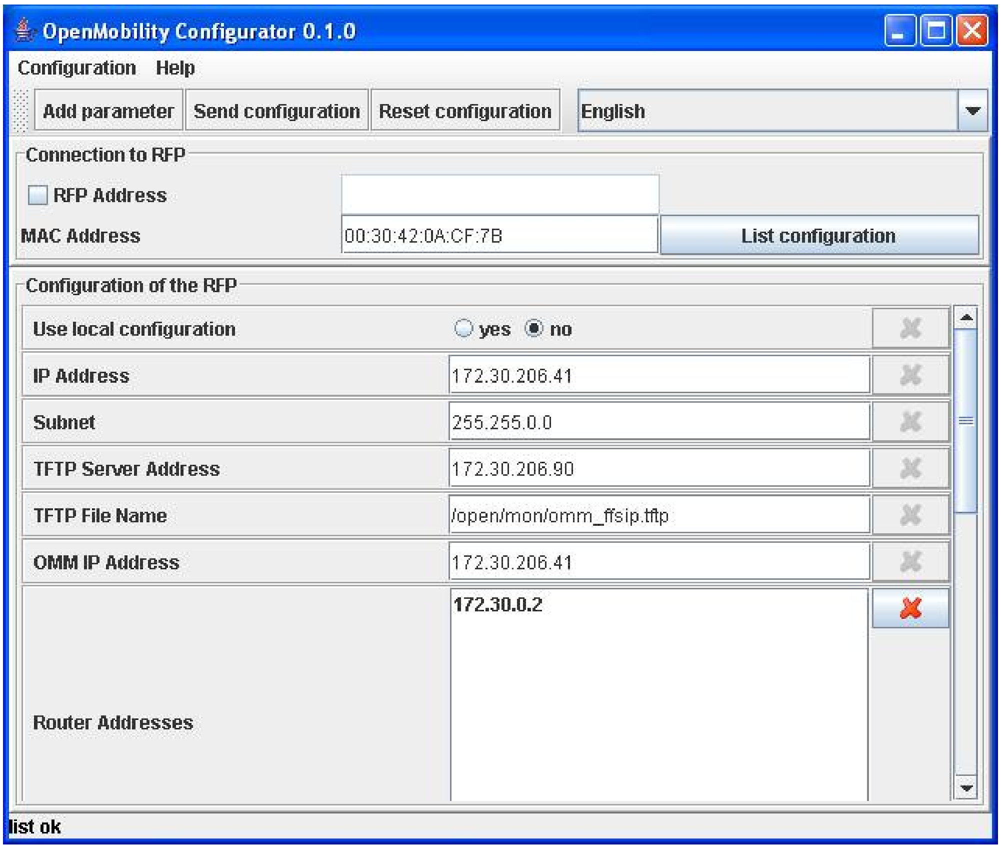
For a static local configuration you must use the java configuration tool OpenMobility Configurator (requires Java Runtime Environment version 1.4 or higher).

The settings, which are configured on the IP DECT Base Station with the tool OM Configurator, will be saved permanently in the internal flash memory of an IP DECT Base Station.

The parameters configurable via the OM Configurator comply with the DHCP option, please see section 3.1 for details.

If a local static configuration has been done, DHCP is not used anymore.

The following figure shows the OM Configurator.



Connection to RFP

□ RFP Address

MAC Address 00:30:42:0A:CF:7B

Configuration of the RFP

Use local configuration	○ yes ● no
IP Address	172.30.206.41
Subnet	255.255.0.0
TFTP Server Address	172.30.206.90
TFTP File Name	/open/mon/omm_ffsip.tftp
OMM IP Address	172.30.206.41
Router Addresses	172.30.0.2

list ok

To configure an IP DECT Base Station, at least the MAC address and all mandatory options (see table below) have to be set. If the IP DECT Base Station has an IP address enter this address in the IP address field. In this case you can reach the IP DECT Base Station from outside the local LAN segment.

To set additional parameters, press the “Add parameter” button and choose the desired parameter.

Press the “Send configuration” button to transmit the parameters to an IP DECT Base Station.

The configuration can only be set after powering up or at the retry phase (LED flashing 0,25 Hz) or in kernel mode, please see section 3.1.6 for details. The configurator tool waits 2 seconds and retries transmitting the data 3 times.

If you want to read the configuration parameters from an IP DECT Base Station set the MAC address and the IP address additionally and press the “List configuration” button. All parameters will be listed in the OM Configurator tool.

Press the “Reset configuration" button to clean all input fields and additional parameters.

3.3 Configuring the OpenMobility Manager

The OMM can be configured via HTTP. The OMM acts as a HTTP server which binds to port 80 by default. If executed in host mode the port can be configured via the command line interface.

The configuration data will be either read from the internal flash memory or from a local file. A local file is only used if specified on the command line on a PC host.

The configuration file is a human readable ASCII file. Changing the configuration file outside the OMM is not permitted.

The configuration file can be downloaded and uploaded via the web interface.

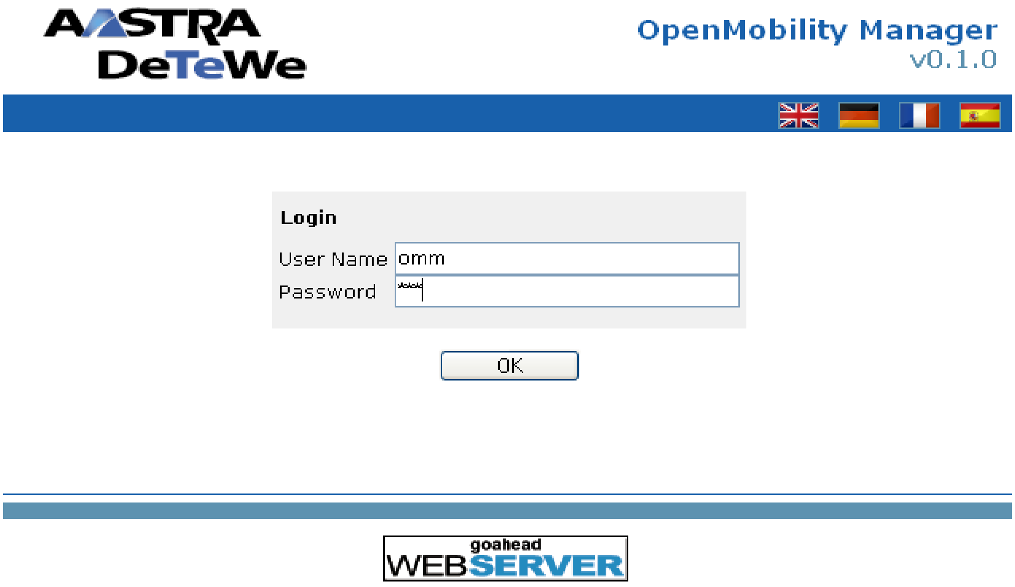
The service access is restricted to one active session at a time and is password protected.

The browser used for service access has to be at least Microsoft Internet Explorer 6.0 or Mozilla Firefox 1.0 and must have frame support, JavaScript and cookies enabled.

3.3.1 Service Login procedure

The OMM allows only one user at a time to configure the system. A user must authenticate with an user name and a password. Both strings are checked case sensitive.

Default login and password is “`omm`”.



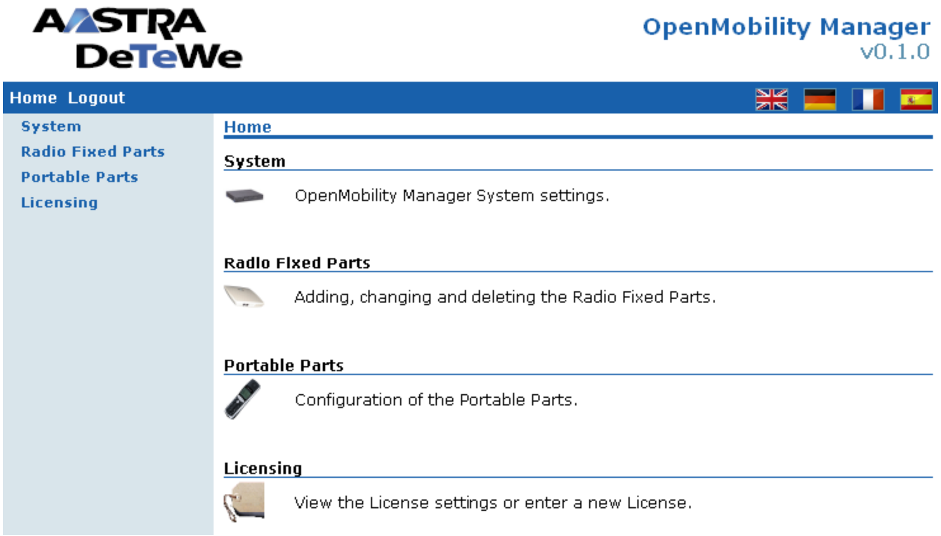
Login

User Name omm

Password ***

After login there are the following options available:

- Configuration of general IP DECT system parameters.
- Administration of the attached RFPs.
- Administration of the PPs.
- Administration of the licence options.



System

OpenMobility Manager System settings.

Radio Fixed Parts

Adding, changing and deleting the Radio Fixed Parts.

Portable Parts

Configuration of the Portable Parts.

Licensing

View the License settings or enter a new License.

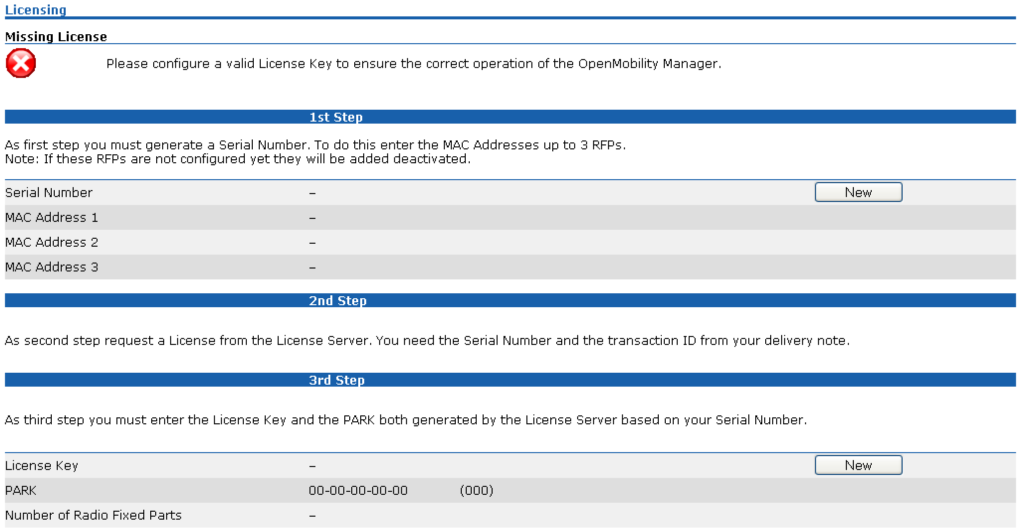
If no user action takes place the OMM logs out the user after 5 minutes.

To logout from the system click at “Logout”.

Note: If the browser is closed without logging out first the service access will be blocked for other clients for 5 minutes.

3.3.2 Licensing

Within the initial configuration of the IP DECT system, the license is missing and a warning occurs.



Licensing

Missing License

☒ Please configure a valid License Key to ensure the correct operation of the OpenMobility Manager.

1st Step

As first step you must generate a Serial Number. To do this enter the MAC Addresses up to 3 RFPs.
Note: If these RFPs are not configured yet they will be added deactivated.

Serial Number	–	New
MAC Address 1	–	
MAC Address 2	–	
MAC Address 3	–	

2nd Step

As second step request a License from the License Server. You need the Serial Number and the transaction ID from your delivery note.

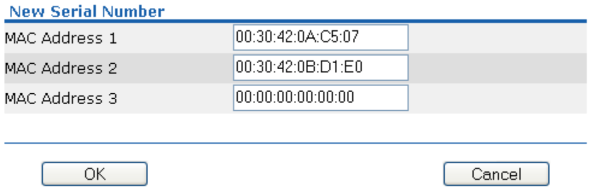
3rd Step

As third step you must enter the License Key and the PARK both generated by the License Server based on your Serial Number.

License Key	–	New
PARK	00-00-00-00-00 (000)	
Number of Radio Fixed Parts	–	

3.3.2.1 Definition of the License RFPs'

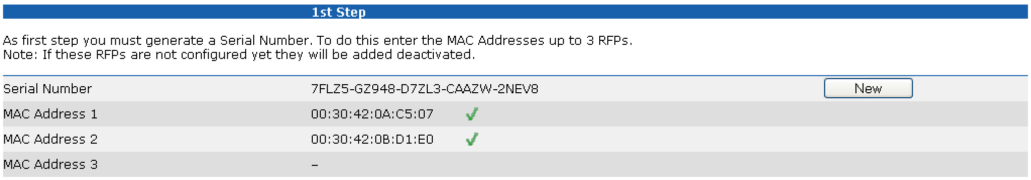
The License RFPs' have to be defined in that manner as described in chapter 2.8. Press the “New” button and add the MAC addresses of the License RFPs':



New Serial Number

MAC Address 1	00:30:42:0A:C5:07
MAC Address 2	00:30:42:0B:D1:E0
MAC Address 3	00:00:00:00:00:00

If that has been done please wait for the green tick(s) as shown in the next image.



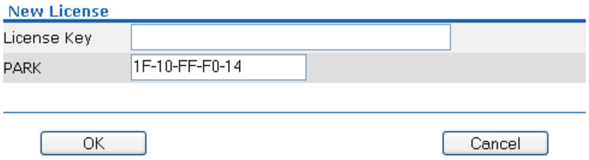
1st Step

As first step you must generate a Serial Number. To do this enter the MAC Addresses up to 3 RFPs.
Note: If these RFPs are not configured yet they will be added deactivated.

Serial Number	7FLZ5-GZ948-D7ZL3-CAAZW-2NEV8	New
MAC Address 1	00:30:42:0A:C5:07 ✓	
MAC Address 2	00:30:42:0B:D1:E0 ✓	
MAC Address 3	–	

3.3.2.2 Get and add the licence key and PARK number

The second step is to go to the Aastra - DeTeWe License web site and enter the serial number generated by the first step along with a TAN from your documentation. This will generate a license key that has to be entered in the 3rd step.



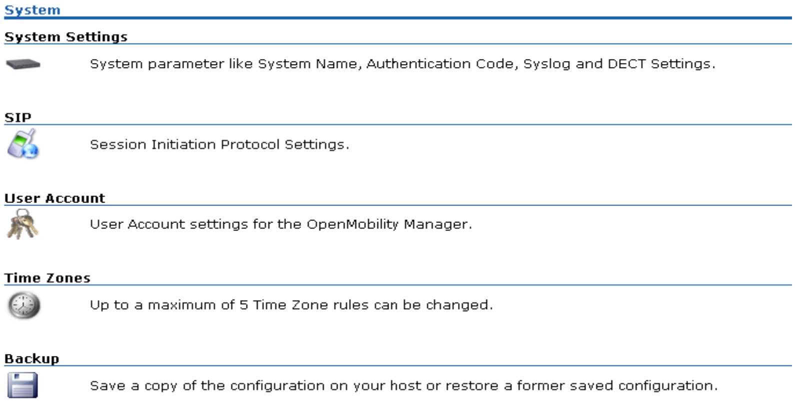
New License

License Key

PARK 1F-10-FF-F0-14

If the license is valid, the warning “Missing License” disappears and the OMM restarts.

3.3.3 System



System

System Settings

System parameter like System Name, Authentication Code, Syslog and DECT Settings.

SIP

Session Initiation Protocol Settings.

User Account

User Account settings for the OpenMobility Manager.

Time Zones

Up to a maximum of 5 Time Zone rules can be changed.

Backup

Save a copy of the configuration on your host or restore a former saved configuration.

3.3.3.1 System settings

The system settings cover global settings for the OpenMobility Manager like the system name or a system wide authentication code. The authentication code is used during initial PP subscription as a security option (see chapter 3.3.5).

Encryption and regulatory domain are described in the chapters 3.3.3.1.2 and 3.3.3.1.3.

For monitoring the DECT system behaviour of the OpenMobility Manager a separate application will be delivered. This tool needs an access to the OpenMobility Manager which is disabled by default and can be enabled on the system page.

To allow the prioritisation of Voice Packets and/or Signalling Packets (SIP) inside the used network the IP parameter ToS (Type of Service) could be configured here.

The OpenMobility Manager and the RFPs are capable of propagating syslog messages conforming to /8/. This feature together with the IP address of a host collecting these messages can be configured.

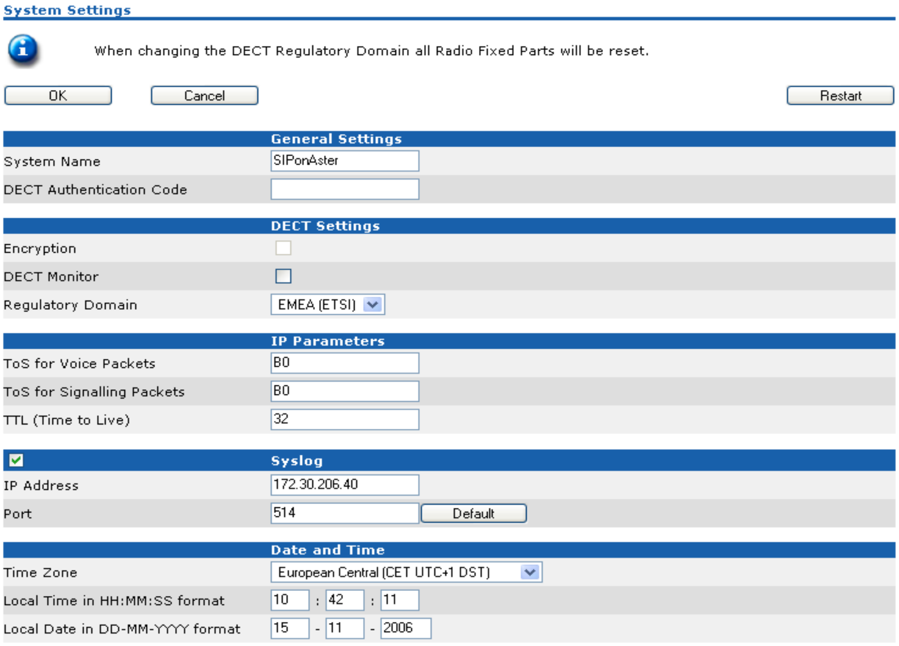
If SNTP is not used, date and time can be configured at the OMM. This has to be done to provide date and time to the Aastra Phone 142.

The time zone, which is shown on this web page, has been configured at the IP region section of the web service.

Please note, that in the case that SNTP is not used, the date and time has to be configured after every restart of the IP DECT Base Station, where the OpenMobility Manager is running.

The date and time will be provided by the OpenMobility Manager to the Aastra Phone 142 if the Aastra Phone 142 initiates a DECT location registration. This will be done in the following cases:

- Subscribing at the OMM
- Entering the network again after the DECT signal was lost
- Power on
- Silent charging feature is active at the phone and the phone is taken out of the charger
- After a specific time to update date and time



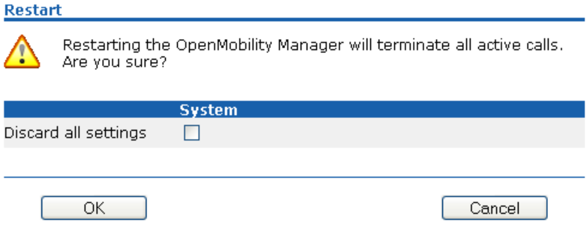
System Settings

When changing the DECT Regulatory Domain all Radio Fixed Parts will be reset.

General Settings	
System Name	SIPonAster
DECT Authentication Code	
DECT Settings	
Encryption	□
DECT Monitor	□
Regulatory Domain	EMEA (ETSI)
IP Parameters	
ToS for Voice Packets	B0
ToS for Signalling Packets	B0
TTL (Time to Live)	32
☑ **Syslog**	
IP Address	172.30.206.40
Port	514 Default
Date and Time	
Time Zone	European Central (CET UTC+1 DST)
Local Time in HH:MM:SS format	10 : 42 : 11
Local Date in DD-MM-YYYY format	15 - 11 - 2006

3.3.3.1.1 Restarting the OMM

To restart the OMM select “System Settings” from the navigation tree and then select ‘Restart’. There is also the option to reset the configuration data.

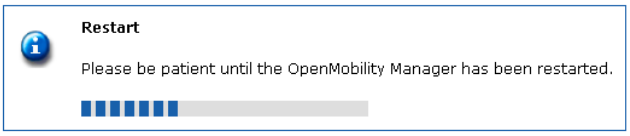


Restart

Restarting the OpenMobility Manager will terminate all active calls.
Are you sure?

System	
Discard all settings	□

A reset web page is loaded then displaying a progress bar and the login web page is loaded automatically if the OMM is reachable again.



Restart

Please be patient until the OpenMobility Manager has been restarted.

3.3.3.1.2 Encryption

Encryption is only available if RFP32/34 IP (not RFP 31/33 IP) are used.

Therefore it can only be enabled on the “System Settings” web page if no RFP31/33 IP has been connected to the OMM.

If encryption is enabled and an RFP31/33 IP connects to the OMM, its DECT air interface will not be activated. The user always has the possibility to disable encryption. In this case all connected RFP31/33 IP are restarted.

Note: The PPs have to support DECT encryption which is not a mandatory feature.

3.3.3.1.3 Regulatory domain

To define where the IP DECT is used the parameter regulatory domain has to be configured. Existing installations are updated to the default value “EMEA (ETSI)”. To setup an FCC compliant installation the value has to be set to “US (FCC/CI)”.

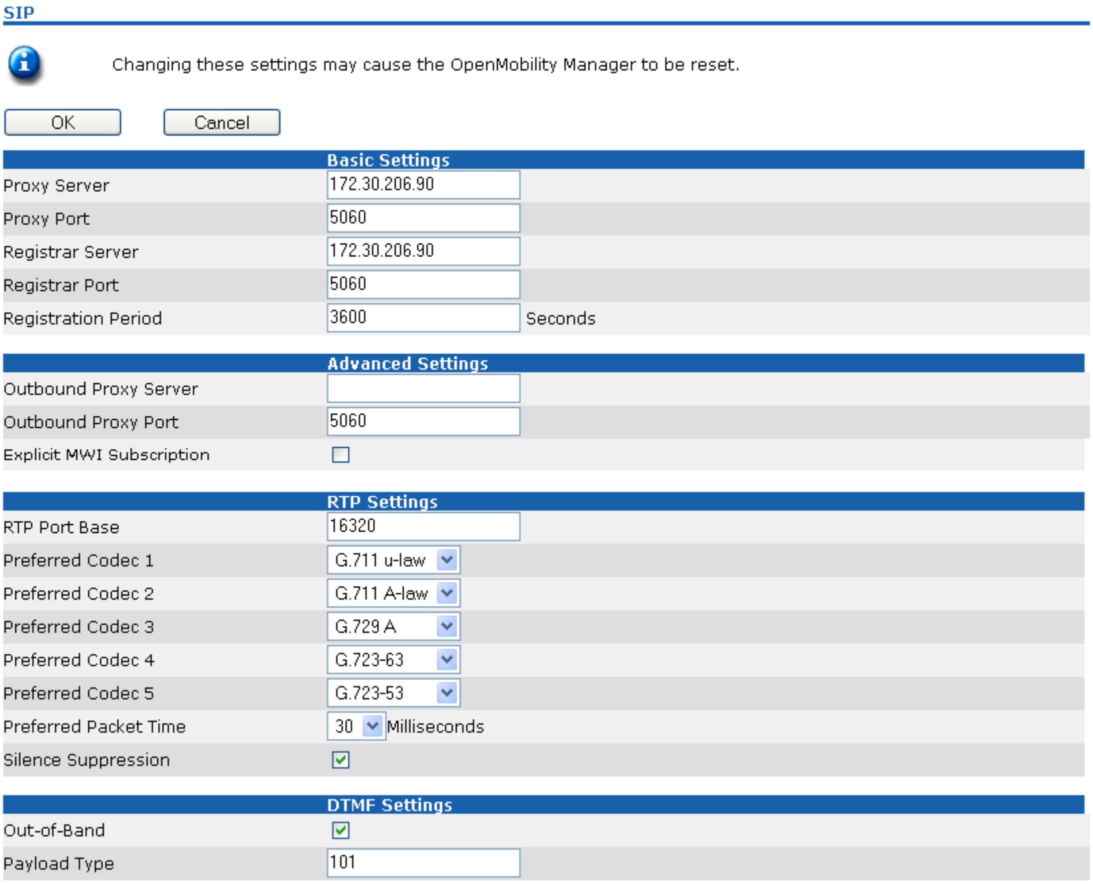
ETSI compliant RFPs are inactive and can not be activated if the regulatory domain is set to “US (FCC/CI)” and vice versa.

3.3.3.2 SIP

The SIP settings cover all global settings matching the SIP signalling and the RTP voice streams.

- **Proxy Server**
  IP address or name of the SIP proxy server.
- **Proxy Port**
  SIP proxy server’s port number. Default is 5060.
- **Registrar Server**
  IP address or name of the SIP registrar. Enables the PPs to be registered with a Registrar.
- **Registrar Port**
  SIP Registrar’s port number. Default is 5060.
- **Registration Period**
  The requested registration period, in seconds from the registrar.
- **Outbound Proxy**
  Address of the outbound proxy server. All SIP messages originating from the OMM are sent to this server. For example, if you have a Session Border Controller in your network, then you would normally set its address here.
- **Outbound Proxy Port**
  The proxy port on the proxy server to which the OMM sends all SIP messages.

- **Explicit MWI Subscription**
  Some Media Server such as the Asterisk support Message Waiting Indication (MWI) based on /15/. A MWI icon will be presented on a Aastra Phone 142 if the user has received a voice message on his voice box which is supported by the Media Server. If Explicit MWI Subscription is enabled the OMM sends explicit for each PP a MWI Subscription message to the Proxy or Outbound Proxy Server.
- **RTP Port Base**
  Each RFP needs a continuous port area of 68 UDP ports for RTP voice streaming. The RTP Port Base is the start port number of that area. Default is 16320.
- **Preferred Codec 1 – 5**
  Specifies a customized codec preference list which allows you to use the preferred Codecs. The *Codec 1* has the highest and *Codec 5* the lowest priority.
- **Silence Suppression**
  Allows to configure whether Silence Suppression is preferred or not.
- **DTMF Out-of-Band**
  The OMM supports DTMF based on /9/.
- **DTMF Payload Type**
  If Out-of-Band is enabled the *Payload Type* specify the payload type which is used for sending DTMF events based on /9/.



SIP

Changing these settings may cause the OpenMobility Manager to be reset.

Basic Settings		
Proxy Server	172.30.206.90	
Proxy Port	5060	
Registrar Server	172.30.206.90	
Registrar Port	5060	
Registration Period	3600	Seconds

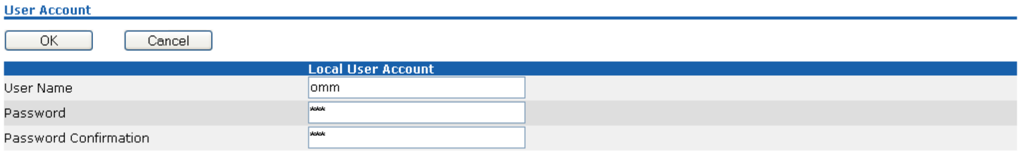
Advanced Settings	
Outbound Proxy Server	
Outbound Proxy Port	5060
Explicit MWI Subscription	□

RTP Settings		
RTP Port Base	16320	
Preferred Codec 1	G.711 u-law	
Preferred Codec 2	G.711 A-law	
Preferred Codec 3	G.729 A	
Preferred Codec 4	G.723-63	
Preferred Codec 5	G.723-53	
Preferred Packet Time	30	Milliseconds
Silence Suppression	☑	

DTMF Settings	
Out-of-Band	☑
Payload Type	101

3.3.3.3 User account

After initial installation or after removing the configuration file the OpenMobility service is accessible via a build-in user account with user “omm” and password “omm”. These settings which are case sensitive can be changed on the “User Account” web page.



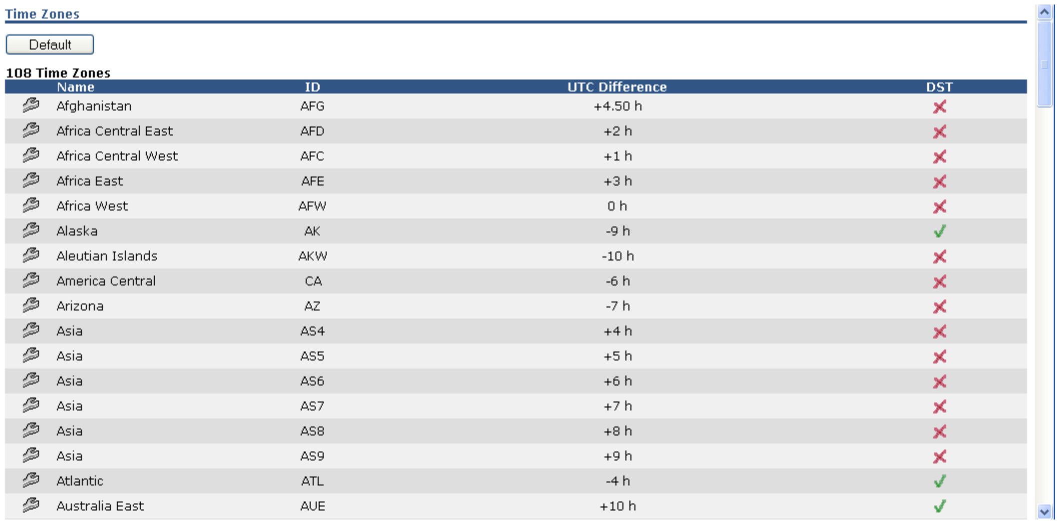
Local User Account	
User Name	omm
Password	***
Password Confirmation	***

3.3.3.4 Time zones

A time and date resynchronization of the Aastra Phone 142 devices is described in chapter 3.3.3.1.

In the time zone section the OpenMobility Manager provides all available time zones. They are set with their known daylight savings time rules adjusted to the Universal Coordinated Time (UTC) per default. The difference to the UTC time is shown in the “UTC Difference” column. In case of a configured daylight savings time rule this is also marked for each time zone.

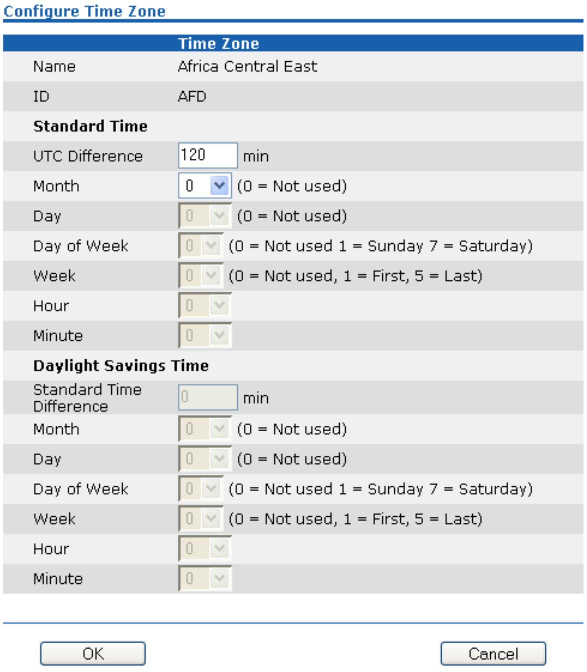
There is a possibility to change the time zone rules for maximal five time zones. Changed rules are marked with a bold time zone name in the table. The changes are saved in the configuration file and are restored after each OpenMobility Manager startup. The “Default” button sets all time zones back to the default values and deletes the changed time zone rules in the configuration file.



108 Time Zones

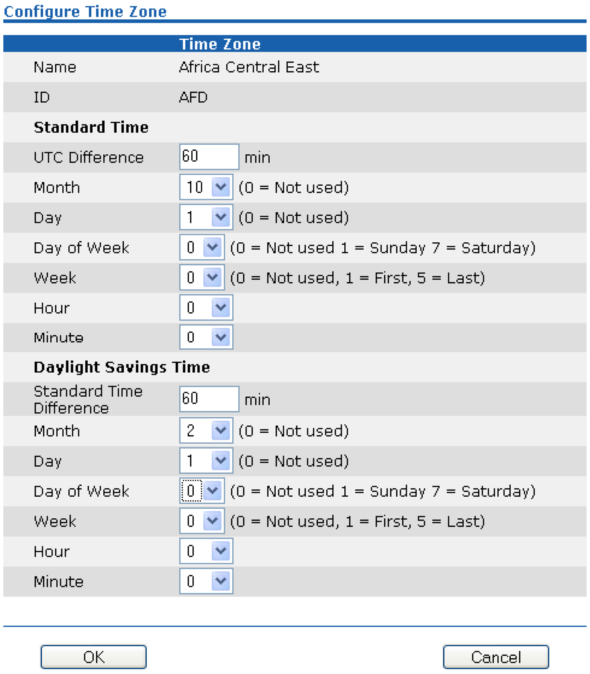
Name	ID	UTC Difference	DST
Afghanistan	AFG	+4.50 h	✗
Africa Central East	AFD	+2 h	✗
Africa Central West	AFC	+1 h	✗
Africa East	AFE	+3 h	✗
Africa West	AFW	0 h	✗
Alaska	AK	-9 h	✓
Aleutian Islands	AKW	-10 h	✗
America Central	CA	-6 h	✗
Arizona	AZ	-7 h	✗
Asia	AS4	+4 h	✗
Asia	AS5	+5 h	✗
Asia	AS6	+6 h	✗
Asia	AS7	+7 h	✗
Asia	AS8	+8 h	✗
Asia	AS9	+9 h	✗
Atlantic	ATL	-4 h	✓
Australia East	AUE	+10 h	✓

With the “Configure Time Zone” dialog the standard time and the daylight savings time (DST) of a time zone can be changed. If the time zone has no DST only the UTC difference can be configured. For the DST both points of time (begin of standard time and begin of daylight savings time) have to be specified exactly. Therefore a certain day in the month or a certain week day in a month can be used. See the following screen shots as an example:



Configure Time Zone

	Time Zone
Name	Africa Central East
ID	AFD
Standard Time	
UTC Difference	120 min
Month	0 (0 = Not used)
Day	0 (0 = Not used)
Day of Week	0 (0 = Not used 1 = Sunday 7 = Saturday)
Week	0 (0 = Not used, 1 = First, 5 = Last)
Hour	0
Minute	0
Daylight Savings Time	
Standard Time Difference	0 min
Month	0 (0 = Not used)
Day	0 (0 = Not used)
Day of Week	0 (0 = Not used 1 = Sunday 7 = Saturday)
Week	0 (0 = Not used, 1 = First, 5 = Last)
Hour	0
Minute	0

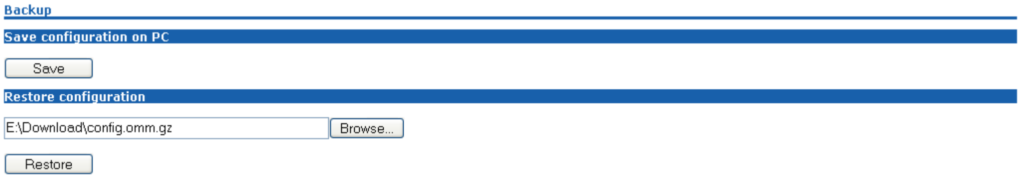


Configure Time Zone

	Time Zone
Name	Africa Central East
ID	AFD
Standard Time	
UTC Difference	60 min
Month	10 (0 = Not used)
Day	1 (0 = Not used)
Day of Week	0 (0 = Not used 1 = Sunday 7 = Saturday)
Week	0 (0 = Not used, 1 = First, 5 = Last)
Hour	0
Minute	0
Daylight Savings Time	
Standard Time Difference	60 min
Month	2 (0 = Not used)
Day	1 (0 = Not used)
Day of Week	0 (0 = Not used 1 = Sunday 7 = Saturday)
Week	0 (0 = Not used, 1 = First, 5 = Last)
Hour	0
Minute	0

3.3.3.5 Backup

The web service interface allows to save a copy of the current configuration on the local host (host where the browser application is executed) as well as to restore an older configuration.



Backup

Save configuration on PC

Restore configuration

E:\Download\config.omm.gz

Restoring a previously saved configuration will lead to a reset of the OMM to take effect.

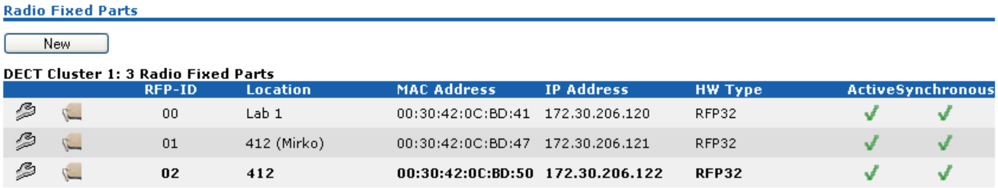
3.3.4 RFP configuration

All configured RFPs are listed in tables grouped to clusters by its topographic relations. The RFPs are sorted by their Ethernet addresses.

To ensure correct handover of a PP during a call, all involved RFPs must deliver the same clock signal to the PP. This is achieved by placing the RFPs so close to each other, that every RFP recognizes at least one other RFP through its radio interface.

There are conditions where this is not possible, for instance with RFPs at remote locations. In this case the RFPs shall be grouped to different clusters. The OpenMobility Manager will not try to synchronize RFPs over cluster borders.

All used clusters are displayed in the navigation bar on the left side and the OMM RFP is marked with a bold font.

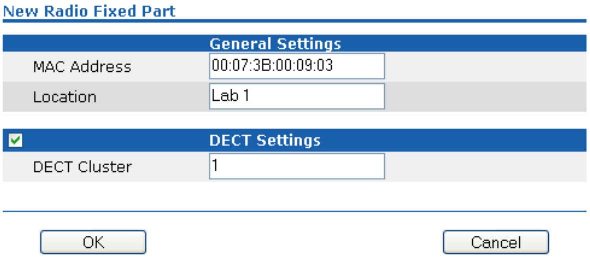


DECT Cluster 1: 3 Radio Fixed Parts

RFP-ID	Location	MAC Address	IP Address	HW Type	Active	Synchronous
00	Lab 1	00:30:42:0C:BD:41	172.30.206.120	RFP32	✓	✓
01	412 (Mirko)	00:30:42:0C:BD:47	172.30.206.121	RFP32	✓	✓
02	**412**	**00:30:42:0C:BD:50**	**172.30.206.122**	**RFP32**	✓	✓

When the RFPs are connecting the OMM they submit their HW type. This type is displayed on the RFP list web page.

New RFPs can be added to the system by pressing the “New” button. A popup window appears providing the configuration of a new RFP.



General Settings

MAC Address: 00:07:3B:00:09:03

Location: Lab 1

☑ DECT Settings

DECT Cluster: 1

Each RFP is identified by its MAC address (6 bytes hex format, colon separated). The Ethernet address is unique and can be found on the back of the chassis.

For easier administration each RFP can be associated with a location string. The location string can hold up to 20 characters.

The same popup window could be opened for an existing RFP by pressing the tool icon 🔧 of the appropriate RFP.

An RFP could be deleted by pressing the trash can icon 🗑. A similar popup window asks for confirmation showing the current configuration of this RFP.

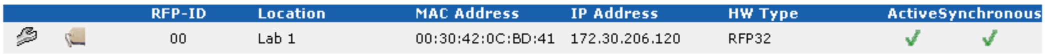
3.3.4.1 DECT configuration

The DECT functionality for each RFP can be switched on/off. If DECT is active the RFP can be added to a cluster.

3.3.4.2 States of a RFP

For each RFP the state of the DECT subsystem is displayed. The states are:

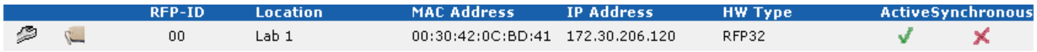
Synchronous



		RFP-ID	Location	MAC Address	IP Address	HW Type	Active	Synchronous
🔧	📁	00	Lab 1	00:30:42:0C:BD:41	172.30.206.120	RFP32	✓	✓

The RFP is up and running. The RFP recognizes and is recognized by other RFPs in its cluster through its air interface and delivers a synchronous clock signal to the PPs.

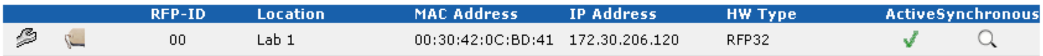
Asynchronous but active



		RFP-ID	Location	MAC Address	IP Address	HW Type	Active	Synchronous
🔧	📁	00	Lab 1	00:30:42:0C:BD:41	172.30.206.120	RFP32	✓	✗

The RFP has not been able to synchronize to its neighbours yet. No DECT communication is possible. But nevertheless the RFP has already been able to connect to the OMM. This phase should usually last only for a few seconds after starting up the RFP or the OMM. If this state lasts longer this is an indication for a hardware or network failure.

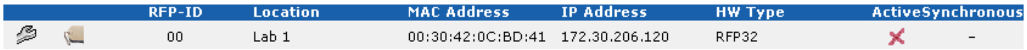
Searching



		RFP-ID	Location	MAC Address	IP Address	HW Type	Active	Synchronous
🔧	📁	00	Lab 1	00:30:42:0C:BD:41	172.30.206.120	RFP32	✓	🔍

The RFP has lost synchronization to its neighbours. No DECT communication is possible. This phase should usually last only for a few seconds after starting up the RFP or the OMM. If this state lasts longer or is re-entered after being in a synchronous state this is an indication for a bad location of the RFP.

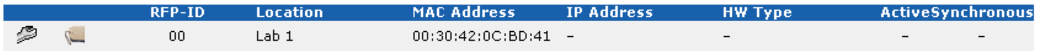
Inactive



		RFP-ID	Location	MAC Address	IP Address	HW Type	Active	Synchronous
🔧	📁	00	Lab 1	00:30:42:0C:BD:41	172.30.206.120	RFP32	✗	-

The RFP has connected to the OMM but the air interface has not been switched on yet. For any RFP with activated DECT functionality this phase should last only for a few seconds after starting up the RFP. If this state lasts longer this may indicate an hardware failure.

Not connected

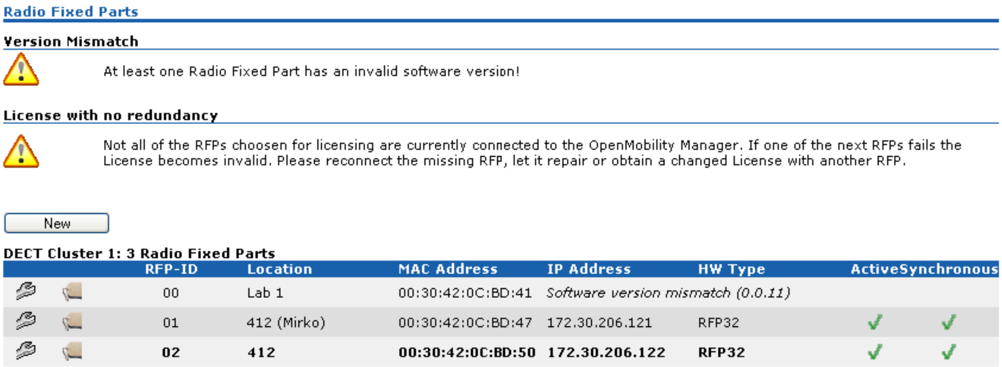


		RFP-ID	Location	MAC Address	IP Address	HW Type	Active	Synchronous
🔧	📁	00	Lab 1	00:30:42:0C:BD:41	-	-	-	-

The RFP was configured but has not connected to the OMM yet. Therefore the IP address column is empty.

3.3.4.3 OMM / RFP SW version check

When the RFPs are connecting the OMM they submit their SW version. If this version differs from the OMM SW version the RFP connection attempt is rejected. This could happen when using several DHCP servers with different OpenMobility SW versions. In this case the RFP is marked with an error message. Moreover a global error message is displayed on the RFP list web page if at least one version mismatch has been found.



Radio Fixed Parts

Version Mismatch

At least one Radio Fixed Part has an invalid software version!

License with no redundancy

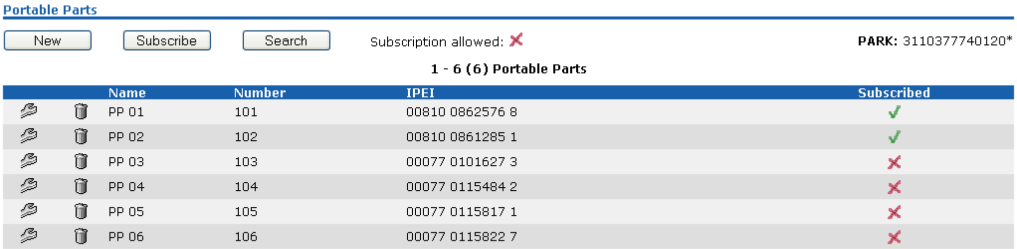
Not all of the RFPs choosen for licensing are currently connected to the OpenMobility Manager. If one of the next RFPs fails the License becomes invalid. Please reconnect the missing RFP, let it repair or obtain a changed License with another RFP.

DECT Cluster 1: 3 Radio Fixed Parts

RFP-ID	Location	MAC Address	IP Address	HW Type	Active	Synchronous
00	Lab 1	00:30:42:0C:BD:41	*Software version mismatch (0.0.11)*			
01	412 (Mirko)	00:30:42:0C:BD:47	172.30.206.121	RFP32	✓	✓
02	**412**	**00:30:42:0C:BD:50**	**172.30.206.122**	**RFP32**	✓	✓

3.3.5 Configuration of Portable Parts

At the Portable Parts web page all configured DECT handsets are sorted by their number. To keep the list concise, the complete list is split up into sub lists containing up to 100 handsets. The user can move back and forth in steps of 100 handsets. Because the browser function can not be used to search for a certain handset in all sub lists, a search function is available, which allows to find a handset by a given number or IPEI.



Portable Parts

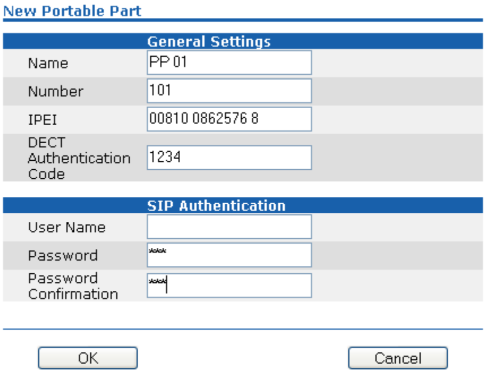
Subscription allowed: ✗

PARK: 3110377740120*

1 - 6 (6) Portable Parts

Name	Number	IPEI	Subscribed
PP 01	101	00810 0862576 8	✓
PP 02	102	00810 0861285 1	✓
PP 03	103	00077 0101627 3	✗
PP 04	104	00077 0115484 2	✗
PP 05	105	00077 0115817 1	✗
PP 06	106	00077 0115822 7	✗

A new PP can be added to the system by pressing the “New” button. The following popup window appears allowing the configuration of a new PP.



New Portable Part

General Settings

Name	PP 01
Number	101
IPEI	00810 0862576 8
DECT Authentication Code	1234

SIP Authentication

User Name	
Password	***
Password Confirmation	***

The name and authentication code fields are optional settings. The number represents the SIP user ID and the name represents the SIP display name. The DECT authentication code is used during initial DECT subscription as a security option and can be set here for each PP separately. If it is not configured the global authentication code on the “System Settings” web page is used (see chapter 3.3.3.1).

The SIP Authentication User Name is optional. It represents the name which will be used during SIP authentications. If no name is given the number will be used instead. The password will be used during SIP authentications.

A similar popup window appears when configuring an existing PP by pressing the tool icon 🔧. The only difference is the delete subscription checkbox. If this option is selected, the PP will be unsubscribed.

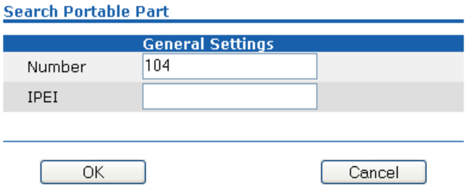
Note: The authentication code can only be changed if the PP is not subscribed. The PP name can be changed, but this will not take effect until the PP is subscribed again.

Deleting of a PP can be done by pressing the trash can icon 🗑. A popup window appears and asks for confirmation.

After adding a PP to the OMM the PP must be subscribed. This is done by pressing the “Subscribe” button. The OMM will allow a subscription of configured but not subscribed PPs during the next hour.

During the subscription process the system wide PARK and the authentication code either configured for the PP or system wide must be entered in the PP form fields. The PARK is displayed at the PP configuration page in the top right corner.

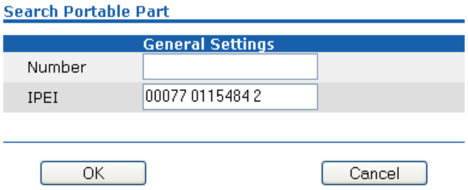
If the user wants to find a certain handset then the search function can be used. A click on the “Search” button provides the following pop-up window.



Search Portable Part

General Settings

Number	104
IPEI	



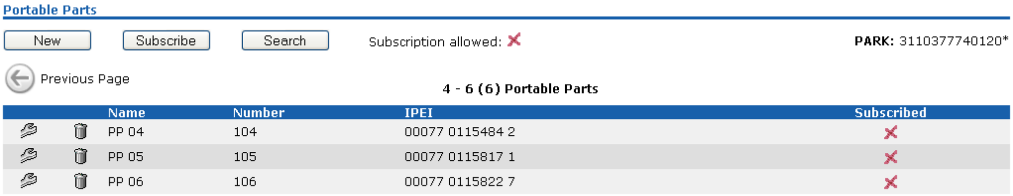
Search Portable Part

General Settings

Number	
IPEI	00077 0115484 2

The user can enter the handsets’ number or IPEI. At least one parameter has to be set. The entered number or IPEI has to match exactly with a handset’s number or IPEI. If number and IPEI are given then a handset has to exist in the OMM’s database whose number and IPEI match both otherwise the search fails.

If a handset with the specified number and/or IPEI was found then a list is displayed which has this handset as the first entry. The search function can also be used to get to the right sub list in one step.



Portable Parts

Subscription allowed: ✗

PARK: 3110377740120*

4 - 6 (6) Portable Parts

		Name	Number	IPEI	Subscribed
✎	🗑	PP 04	104	00077 0115484 2	✗
✎	🗑	PP 05	105	00077 0115817 1	✗
✎	🗑	PP 06	106	00077 0115822 7	✗

4 Maintenance

4.1 Booter

The booter may be handled via the DHCP option 254 “UPDATE” (see chapter 3.1.4.1) automatically. In any case you may have direct control to the booter SW, if you use a telnet user session. A complete description of the usage of the user shell, you can find in /18/.

4.1.1 Checking the RFP booter version

You can display the version information of the RFP booter using the telnet interface of an RFP. Check the booter version to determine whether an update is required to overcome any user issues or to enhance the functionality.

1. Start a telnet session using the IP address of the RFP.
2. Enter login “`iprfp`” and password “`ommsip/987`”.
3. Enter `flash`.

The display will show the software and the hardware level of the RFP.

```
> flash
version of initial booter : 2.0.12
Version of booter 1       : 3.2.2
Version of booter 2       : 3.2.2
Hardware Revision         : 51
MAC address               : 00:30:42:08:31:A4
>
```

4.1.2 Manual update of the RFP booter

You can update the RFP booter manually if there is no opportunity to have an autonomic update. Please check the booter version to determine whether an update is required to overcome any user issues or to enhance the functionality.

1. Start a telnet session using the IP address of the RFP.
2. Enter login “`iprfp`” and password “`ommsip/987`”.
3. Enter `flash_update`.
4. Enter `flash_update` a second time because of the two booter images.

4.2 Site survey measurement equipment

If an IP DECT installation has to be planned, a sufficient distribution of the RFPs is necessary, which fulfills the requirements for reliable synchronization and connectivity to the Portable Parts. The site survey kit may help you. It comprises:

- Scaled layout diagram of the building/premises.
- One measuring RFP with its own power supply.
- A tripod and a battery for the RFP.

- Two reference PPs with chargers.
- Battery chargers.
- A measuring handset, which can monitor other makers DECT radio sources.

4.3 Checking the Aastra Phone 142 firmware version

You can display the version information of the Aastra Phone 142 with a few keystrokes. Check the firmware version to determine whether an update is required to overcome any user issues.

1. Press the “**Menu**” soft key
2. Select “**System**” (only to highlight)
3. Press “**OK**”.
4. Select “**Version Number”**
5. Press “**OK**”.

The display will show the software and the hardware version of the Aastra Phone 142.

4.4 Diagnostic

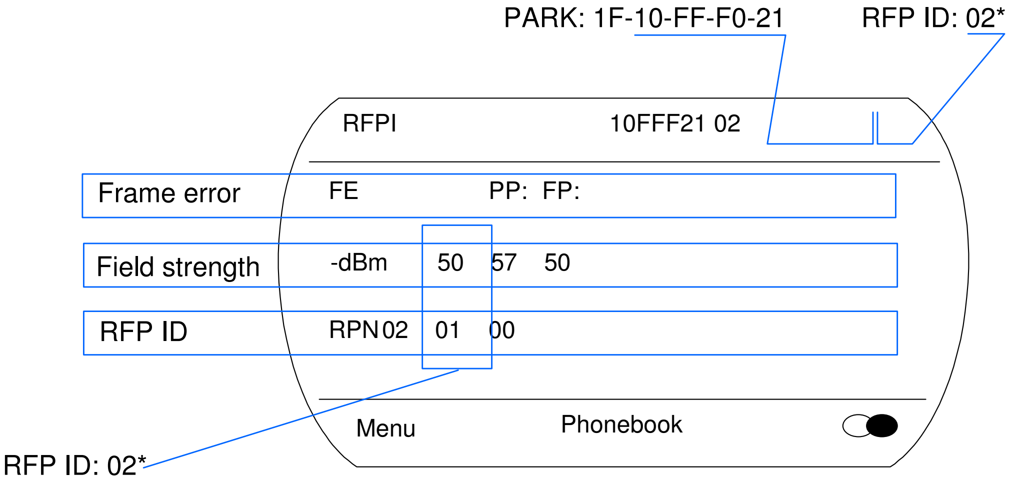
4.4.1 Aastra Phone 142 site survey mode

You can set the Aastra Phone 142 in “site survey mode” with a few keystrokes. In this mode the phone will display the RFPs and the actual field strength of the receiving signal in dBM.

1) Press the “**Menu**” soft key
2) Enter the following key sequence “**R***76#**”
3) Select “**Site Survey**”
4) Press “**OK**”.

To leave the site survey mode switch the phone off and on again.

The following display is shown on the Aastra Phone 142:



*The ID of RFP to which the PP is currently associated to.

In this example the PP is currently connected to the RFP with the number 02. The RFP 01 and 00 are also visible. The number “10FFF221 02” on the upper right side refers to the PARK 1F-10-F2-21 of the IP DECT system and to the RFP to which the phone is currently connected to.

4.4.2 Aastra Phone 142 auto call test mode

You can set the Aastra Phone 142 to “auto call test mode” with a few keystrokes. In this mode the phone will call a specified number cyclically. You can use this feature to generate traffic for test purposes. This mode is also active if the phone is an the charger.

1) Press the “**Menu**” soft key
2) Enter the following key sequence “**R***76#**”
3) Select “**Auto Call Test**”
4) Press “**OK**”.
5) Enter the phone number to call.
6) Press “**OK**”.
7) Enter a number of seconds between two calls.
8) Press “**OK**”.
9) Enter a number of seconds a call shall be active.
10) Press “**OK**”. The test will be started automatically.

To stop the test, switch the phone off and on again.

4.4.3 Aastra Phone 142 auto answer test mode

You can set the Aastra Phone 142 to “auto answer test mode” with a few keystrokes. In this mode the phone will answer incoming calls automatically. You can use this feature together this phones in the “auto call test mode” for test purposes. This mode is also active if the phone is an the charger.

1) Press the “**Menu**” soft key
2) Enter the following key sequence “**R***76#**”
3) Select “**Auto Answer**”
4) Press “**OK**”.
5) Enter a number of seconds the phone shall ring before it will answer the call.
6) Press “**OK**”.
7) Enter a number of seconds a call shall be active.
8) Press “**OK**”. The test will be started automatically.

To stop the test switch the phone off and on again.

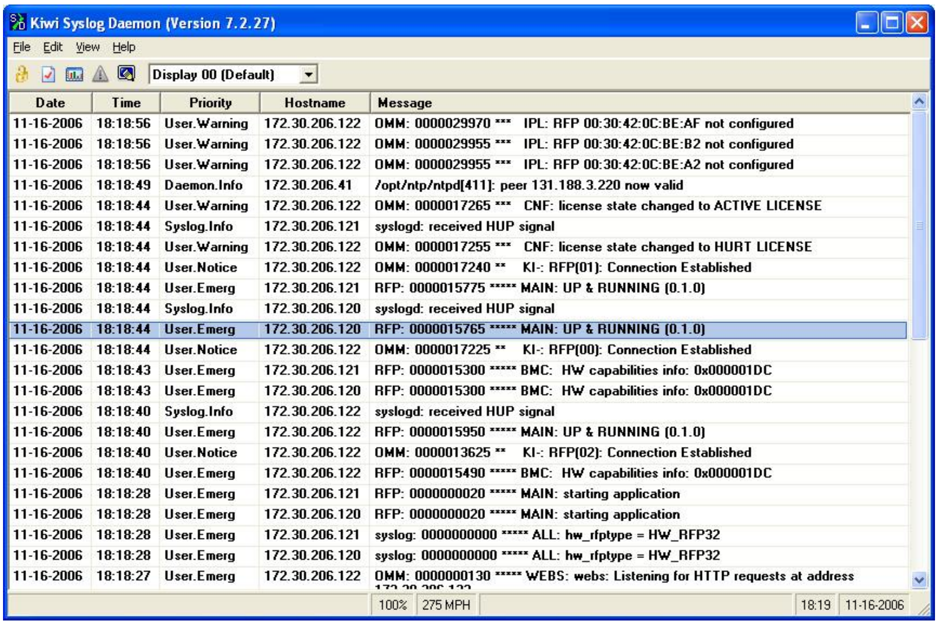
4.4.4 Syslog

The OpenMobility Manager and the RFPs are capable of propagating syslog messages conforming to /8/. This feature together with the IP address of a host collecting these messages can be configured.

Syslog has to be enabled by

- DHCP using the public options 227 and 228.
- Setting the syslog daemon server and port via the web interface.

To set up the syslog via DHCP or OM Configurator has the advantage, that syslogs are available in earlier states of the RFP start up.



Date	Time	Priority	Hostname	Message
11-16-2006	18:18:56	User.Warning	172.30.206.122	OMM: 0000029970 *** IPL: RFP 00:30:42:0C:BE:AF not configured
11-16-2006	18:18:56	User.Warning	172.30.206.122	OMM: 0000029955 *** IPL: RFP 00:30:42:0C:BE:B2 not configured
11-16-2006	18:18:56	User.Warning	172.30.206.122	OMM: 0000029955 *** IPL: RFP 00:30:42:0C:BE:A2 not configured
11-16-2006	18:18:49	Daemon.Info	172.30.206.41	/opt/ntp/ntpd[411]: peer 131.188.3.220 now valid
11-16-2006	18:18:44	User.Warning	172.30.206.122	OMM: 0000017265 *** CNF: license state changed to ACTIVE LICENSE
11-16-2006	18:18:44	Syslog.Info	172.30.206.121	syslogd: received HUP signal
11-16-2006	18:18:44	User.Warning	172.30.206.122	OMM: 0000017255 *** CNF: license state changed to HURT LICENSE
11-16-2006	18:18:44	User.Notice	172.30.206.122	OMM: 0000017240 ** KI-: RFP(01): Connection Established
11-16-2006	18:18:44	User.Emerg	172.30.206.121	RFP: 0000015775 ***** MAIN: UP & RUNNING (0.1.0)
11-16-2006	18:18:44	Syslog.Info	172.30.206.120	syslogd: received HUP signal
11-16-2006	18:18:44	User.Emerg	172.30.206.120	RFP: 0000015765 ***** MAIN: UP & RUNNING (0.1.0)
11-16-2006	18:18:44	User.Notice	172.30.206.122	OMM: 0000017225 ** KI-: RFP(00): Connection Established
11-16-2006	18:18:43	User.Emerg	172.30.206.121	RFP: 0000015300 ***** BMC: HW capabilities info: 0x000001DC
11-16-2006	18:18:43	User.Emerg	172.30.206.120	RFP: 0000015300 ***** BMC: HW capabilities info: 0x000001DC
11-16-2006	18:18:40	Syslog.Info	172.30.206.122	syslogd: received HUP signal
11-16-2006	18:18:40	User.Emerg	172.30.206.122	RFP: 0000015950 ***** MAIN: UP & RUNNING (0.1.0)
11-16-2006	18:18:40	User.Notice	172.30.206.122	OMM: 0000013625 ** KI-: RFP(02): Connection Established
11-16-2006	18:18:40	User.Emerg	172.30.206.122	RFP: 0000015490 ***** BMC: HW capabilities info: 0x000001DC
11-16-2006	18:18:28	User.Emerg	172.30.206.121	RFP: 0000000020 ***** MAIN: starting application
11-16-2006	18:18:28	User.Emerg	172.30.206.120	RFP: 0000000020 ***** MAIN: starting application
11-16-2006	18:18:28	User.Emerg	172.30.206.121	syslog: 0000000000 ***** ALL: hw_rfptype = HW_RFP32
11-16-2006	18:18:28	User.Emerg	172.30.206.120	syslog: 0000000000 ***** ALL: hw_rfptype = HW_RFP32
11-16-2006	18:18:27	User.Emerg	172.30.206.122	OMM: 0000000130 ***** WEBS: webs: Listening for HTTP requests at address

The level of syslog messages in the default state allows the user, to have control over the general system state and major failures. If it is wished to increase the level for diagnostic reasons, this can be done via the telnet user shell by increasing the spy level of each subsystem (see chapter 4.4.5).

You can also read syslogs if you type the command `logread` within the telnet user shell.

4.4.5 Telnet user shell

Each RFP (OMM included) offers a lot of commands within the telnet shell. Most of them are useful for diagnostics and may help experts to resolve failures.

Note: Some commands can harm the systems operation.

4.4.5.1 Login

The procedure is:

- Open a telnet session to the RFP.
- Enter user “`iprfp`” and password “`ommsip/987`”.

```
Welcome to IP RFP OpenMobility SIP Version x.y.z
Mon Nov 13 12:34:06 CEST 2006
Release

(BUILD 0)
172.30.106.41 login: iprfp
Password:

Welcome to the system usershell!

172.030.206.41 > help
```

4.4.5.2 Command overview

Type `help` to get a command overview:

```
arp                 -     show arp table
console_off         -     disable console on local terminal
console_on          -     enable console on local terminal
dmesg               -     print the kernel ring buffer
flash               -     show flash info
flash_update        -     update the booter
interface                 show interface configuration
ip_rfpconsole       -     console to the rfp application
link                -     show link state
logread             -     show message log
mem                       show memory usage
ommconsole          -     console to the omm application
ps                  -     show process table
ping                -     ping <ipaddress>
reboot              -     restarts the system
route               -     show routing table
uptime              -     show system uptime
exit                      exit shell
```

4.4.5.3 RFP console commands

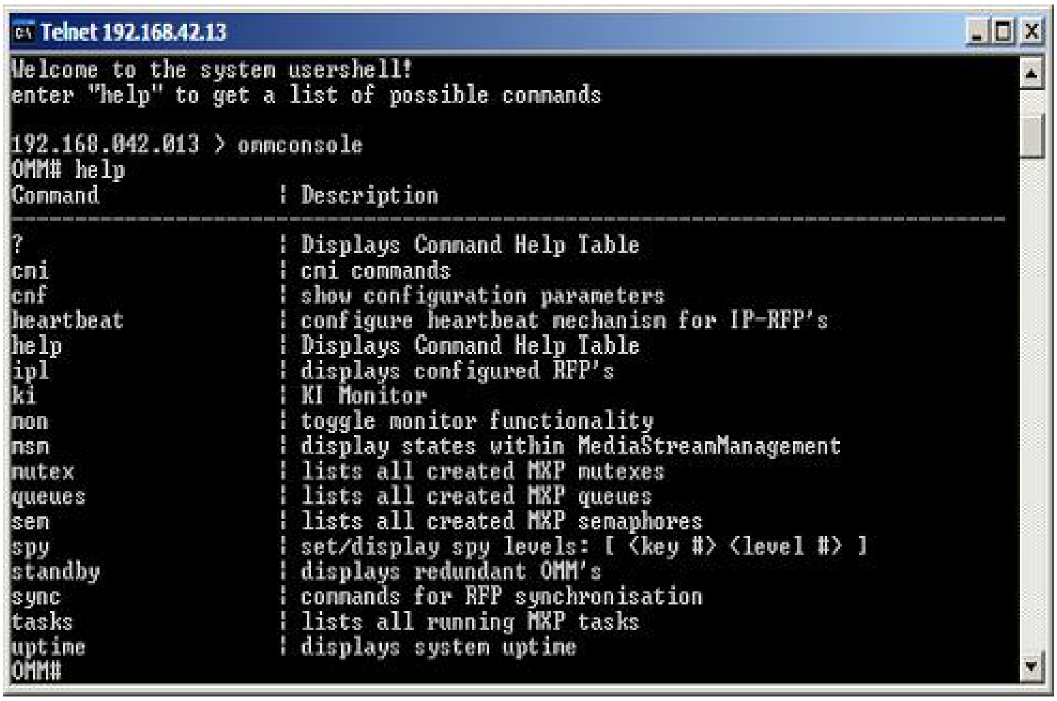
If you type `ip_rfpconsole` you are able to use the following commands on each RFP:

```
IP RFP console commands:
heap                 - shows heap buffer statistics
help                 - Displays Command Help Table
lec                  - adjust linear echo canceler parameters
media                - display state of media channels
mutex                - lists all created MXP mutexes
queues               - lists all created MXP queues
reset                - resets the IPRFP application
rsx                  - allows RSX connection to BMC via TCP
sem                  - lists all created MXP semaphores
spy                  - set/display spy levels: [ <key #> <level #> ]
tasks                - lists all running MXP tasks
voice                - displays the state of voice handling
exit                 - leave the RFP console
```

Note: The `spy` command enables you to increase the level of syslog messages. These should be used only by trained support personnel, because the `spy` command can harm the systems operation.

4.4.5.4 OMM console commands

If you type `ommconsole` and you have opened the session on the OMM RFP you are able to use the following OMM related commands:



```
Welcome to the system usershell!
enter "help" to get a list of possible commands

192.168.042.013 > ommconsole
OMM# help
Command              | Description
---------------------------------------------------------------------
?                    | Displays Command Help Table
cmi                  | cmi commands
cnf                  | show configuration parameters
heartbeat            | configure heartbeat mechanism for IP-RFP's
help                 | Displays Command Help Table
ipl                  | displays configured RFP's
ki                   | KI Monitor
mon                  | toggle monitor functionality
msm                  | display states within MediaStreamManagement
mutex                | lists all created MXP mutexes
queues               | lists all created MXP queues
sem                  | lists all created MXP semaphores
spy                  | set/display spy levels: [ <key #> <level #> ]
standby              | displays redundant OMM's
sync                 | commands for RFP synchronisation
tasks                | lists all running MXP tasks
uptime               | displays system uptime
OMM#
```

Note: The `spy` command enables you to increase the level of syslog messages especially for subsystems of the OMM. These should be used only by trained support personnel, because the `spy` command can harm the systems operation.

4.4.6 DECT monitor of the OpenMobility system

For a better error detection in the OpenMobility system the DECT monitor can be used. The DECT monitor is an MS Windows based standalone application. It provides the possibility to give a real time overview of the current RFP and PP states in the DECT OpenMobility system.

The following features are provided by the DECT monitor:

- Reading out of the DECT configuration of a OpenMobility system.
- Configuration can be stored in an ASCII file.
- Display of DECT transactions RFP-PP in clear tabular form, with highlighting of handover situations. Real-time display.
- Display of further events concerning the status or actions of RFPs and PPs of the OpenMobility system.
- All events can also be recorded in a log file.
- Display of the synchronization relations between the RFPs.
- Monitoring of systems with up to 255 RFPs and 1023 PPs.
- Reading out and display of RFP statistics data, either for a single RFP or for all RFPs.
- Display of DECT central data of the OpenMobility system.

The DECT Monitor application can only be used if the DECT Monitor flag in the OMM web service on the system settings configuration page is enabled.

The DECT monitor application is used together with the OpenMobility system.

When the application is started, the user is requested to enter the IP address of the RFP or server running the OpenMobility Manager (OMM) software. This address is different from the IP address of the PABX the OMM is connected to!

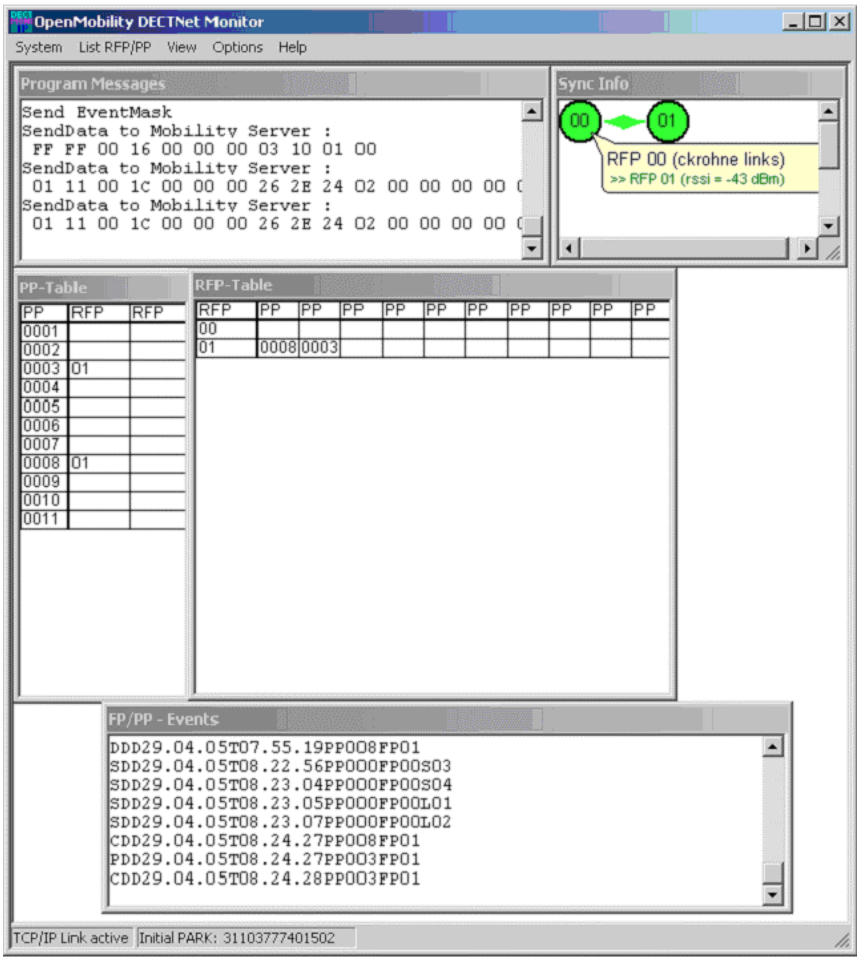
There can be several reasons for an unsuccessful link establishment:

- Operation of DECT Monitor is not enabled inside the OMM. Use the web service to enable the DECT Monitor operation.
- IP address is not correct. It has to be the address of the RFP or server the OMM is running on, not the address of the PABX!
- A link routed through the PABX is not supported. In case of a remote service on a PABX via dial-in the OMM can not be accessed from the DECT Monitor.

The application displays the IP address which has been used last time.

When the application is started a link to the OpenMobility system is automatically established and the application window shows all user configured child windows and tables.

When all links have been established, the DECT data of the system is automatically read out and entered in the tables “RFP-Table” and “PP-Table”. This procedure is called “Config Request”.



```
Send EventMask
SendData to Mobilitv Server :
 FF FF 00 16 00 00 00 03 10 01 00
SendData to Mobilitv Server :
 01 11 00 1c 00 00 00 26 2E 24 02 00 00 00 00
SendData to Mobilitv Server :
 01 11 00 1c 00 00 00 26 2E 24 02 00 00 00 00
```

PP	RFP	RFP
0001		
0002		
0003	01	
0004		
0005		
0006		
0007		
0008	01	
0009		
0010		
0011		

RFP	PP	PP	PP	PP	PP	PP	PP	PP	PP	PP
00										
01	0008	0003								

```
DDD29.04.05T07.55.19PP008FP01
SDD29.04.05T08.22.56PP000FP00S03
SDD29.04.05T08.23.04PP000FP00S04
SDD29.04.05T08.23.05PP000FP00L01
SDD29.04.05T08.23.07PP000FP00L02
CDD29.04.05T08.24.27PP008FP01
PDD29.04.05T08.24.27PP003FP01
CDD29.04.05T08.24.28PP003FP01
```

TCP/IP Link active | Initial PARK: 31103777401502

Next, the defined trace options (event mask) are sent to the OMM. The options which are sent to the OMM are always those which were active the last time the application was exited.

If the trace option “Transaction establish/release” is activated, the OMM will deliver all existing transactions.

Following this, the OMM system delivers the desired trace data. The user can either communicate with the application interactively (see below) or he can simply activate a log file in which to record the data.

Following this initialization, the user can carry out the following modifications:

- The trace settings can be modified using the menu item “Options-Event Mask”. Transmissions to the OMM take place after confirming the settings with “OK’”.
- A “Config Request” can be sent again to the OMM.
- A log file can be activated.
- By means of various dialogues, the configuration data of the PPs, RFPs and control modules can be displayed and stored in ASCII files.

The following information is displayed in the tables dynamically:

- Transactions between PP and PABX system. These are displayed in both tables. Simple transactions are displayed in black on a white background; during handover, both transactions involved are displayed in white on a red background.
- The location registration and detach events are displayed in the tables for approximately 1 – 2 sec after their occurrence (light green background), if possible. There is no display in the RFP table if there is no column free for display. If the event has already been displayed, it can be overwritten at any time. The events are not displayed if they occur during an on-going transaction. Irrelevant of whether the events are displayed in the tables, they are always entered in the ‘FP/PP-Events' window and in the log file (provided that this is open).

The following colour scheme is used for the RFP table display:

RFP grey-blue	RFP is not active (not connected or disturbance)
RFP black	RFP is active

The data of a RFP are displayed in a dialogue box after clicking on the respective RFP field in the RFP table. The statistics data of the RFP can be called up from this dialogue box.

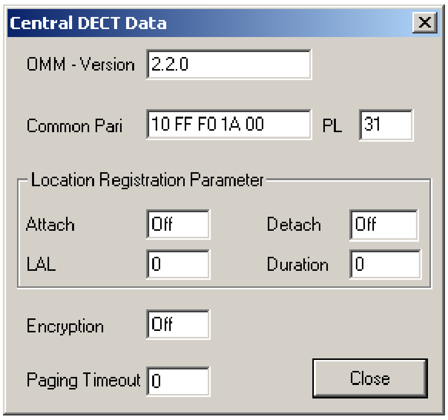
The following colour scheme is used for the PP table display:

PP black:	PP is enrolled. It is assumed that the PP can be reached.
PP blue:	PP can presumably not be reached. Detach was received or when an attempt was made to reach a PP, the PP did not answer.
PP grey/blue:	PP not enrolled.

The PP data is displayed in a dialogue box after clicking on the corresponding PP field in the RFP table.

The “Sync Info” child window contains all RFPs and shows their synchronization and relation states to each other. Selecting the RFPs with the right mouse button the user can change visibility views and can even force a resynchronization of a RFP.

There are several optional sub windows selectable. They are all listed below and give some more information about the OpenMobility systems. Mostly they are statistics and for internal use only.



Central DECT Data

OMM - Version: 2.2.0

Common Pari: 10 FF F0 1A 00 PL: 31

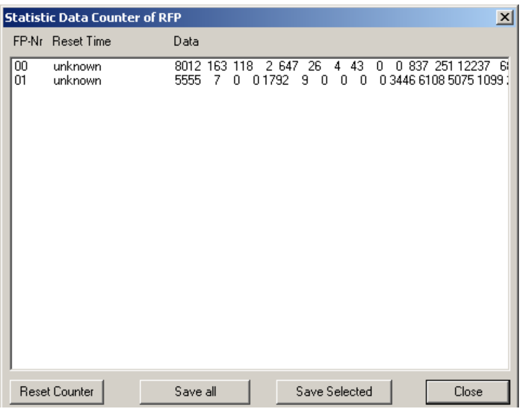
Location Registration Parameter

Attach: Off Detach: Off

LAL: 0 Duration: 0

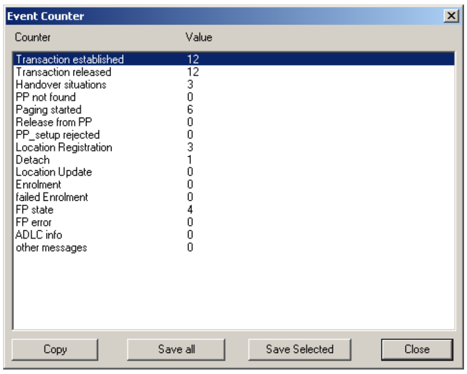
Encryption: Off

Paging Timeout: 0



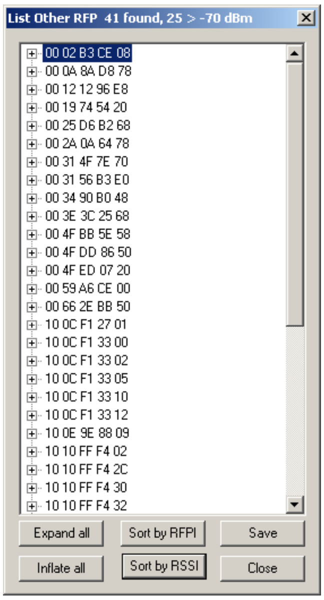
Statistic Data Counter of RFP

```
FP-Nr  Reset Time       Data
00     unknown          8012  163  118   2  647  26   4  43   0    0  837  251 12237  6
01     unknown          5555    7    0   0 1792   9   0   0   0    0 3446 6108  5075 1099
```



Event Counter

Counter	Value
Transaction established	12
Transaction released	12
Handover situations	3
PP not found	0
Paging started	6
Release from PP	0
PP_setup rejected	0
Location Registration	3
Detach	1
Location Update	0
Enrolment	0
failed Enrolment	0
FP state	4
FP error	0
ADLC info	0
other messages	0



List Other RFP 41 found, 25 > -70 dBm

```
00 02 B3 CE 08
00 0A 8A D8 78
00 12 12 96 E8
00 19 74 54 20
00 25 D6 B2 68
00 2A 0A 64 78
00 31 4F 7E 70
00 31 56 B3 E0
00 34 90 B0 48
00 3E 3C 25 68
00 4F BB 5E 58
00 4F DD 86 50
00 4F ED 07 20
00 59 A6 CE 00
00 66 2E BB 50
10 0C F1 27 01
10 0C F1 33 00
10 0C F1 33 02
10 0C F1 33 05
10 0C F1 33 10
10 0C F1 33 12
10 0E 9E 88 09
10 10 FF F4 02
10 10 FF F4 2C
10 10 FF F4 30
10 10 FF F4 32
```

5 Appendix

5.1 Communications Regulation Information for Aastra Phone 142 US

FCC Notices (U.S. Only)

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

Modifications not expressly approved by this company could void the user's authority to operate the equipment.

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

. Reorient or relocate the receiving antenna.

. Increase the separation between the equipment and receiver.

. Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.

. Consult the dealer or an experienced radio/TV technician for help.

Health and Safety Information

Exposure to Radio Frequency (RF) Signals:

The wireless phone is a radio transmitter and receiver. It is designed and manufactured not to exceed the emission limits for exposure to radio frequency (RF) energy set by the Federal Communications Commission (FCC) of the U.S. Government. These limits are part of comprehensive guidelines and establish permitted levels of RF energy for the general population. The guidelines are based on the safety standards previously set by both U.S. and international standards bodies. These standards include a substantial safety margin designed to assure the safety of all persons, regardless of age and health.

This device and its antenna must not be co-located or operating in conjunction with any other antenna or transmitter.

This EUT has been shown to be capable of compliance for localized specific absorption rate (SAR) for uncontrolled environment/general population exposure limits specified in ANSI/IEEE Std. C95.1-1992 and had been tested in accordance with the measurement procedures specified in FCC/OET Bulletin 65 Supplement C (2001) and IEEE 1528-2003.

Industry Canada (Canada only)

Operation of this device is subject to the following two conditions: (1) this device may not cause interference, and (2) this device must accept any interference, including interference that may cause undesired operation of the device.

Privacy of communications may not be ensured when using this telephone.

Exposure to Radio Frequency (RF) Signals:

The wireless phone is a radio transmitter and receiver. It is designed and manufactured not to exceed the emission limit for exposure to radio frequency (RF) energy set by the Ministry of Health (Canada), Safety Code 6. These limits are part of comprehensive guidelines and established permitted levels of RF energy for the general population. These guidelines are based on the safety standards previously set by international standard bodies. These standards include a substantial safety margin designed to assure the safety of all persons, regardless of age and health.

This device and its antenna must not be co-located or operating in conjunction with any other antenna or transmitter.

This device has been shown to be capable of compliance for localized specific absorption rate (SAR) for uncontrolled environment / general public exposure limits specific in ANSI/IEEE C95.1-1992 and had been tested in accordance with the measurement procedures specified in IEEE 1528-2003.

5.2 Communications Regulation Information for RFP 32 US or RFP 34 US (NA)

FCC Notices (U.S. Only)

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

Modifications not expressly approved by this company could void the user's authority to operate the equipment.

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

. Reorient or relocate the receiving antenna.

. Increase the separation between the equipment and receiver.

. Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.

. Consult the dealer or an experienced radio/TV technician for help.

Exposure to Radio Frequency (RF) Signals:

The wireless phone is a radio transmitter and receiver. It is designed and manufactured not to exceed the emission limits for exposure to radio frequency (RF) energy set by the Federal Communications Commission (FCC) of the U.S. Government. These limits are part of comprehensive guidelines and establish permitted levels of RF energy for the general population. The guidelines are based on the safety standards previously set by both U.S. and international standards bodies. These standards include a substantial safety margin designed to assure the safety of all persons, regardless of age and health.

This device and its antenna must not be co-located or operating in conjunction with any other antenna or transmitter.

The radiating element of the base station should be installed during operating at a separation distance greater than 20 cm between user and device. The device comply with the requirements for routine evaluation limits ”

Industry Canada (Canada only)

Operation of this device is subject to the following two conditions: (1) this device may not cause interference, and (2) this device must accept any interference, including interference that may cause undesired operation of the device.

Privacy of communications may not be ensured when using this telephone.

Exposure to Radio Frequency (RF) Signals:

The wireless phone is a radio transmitter and receiver. It is designed and manfactured not to exceed the emission limit for exposure to radio frequency (RF) energy set by the Ministry of Health (Canada), Safety Code 6. These limits are part of comprehensive guidelines and established permitted levels of RF energy for the general population. These guidelines are based on the safety standards previously set by international standard bodies. These standards include a substantial safety margin designed to assure the safety of all persons, regardless of age and health.

This device and its antenna must not be co-located or operating in conjunction with any other antenna or transmitter.

The radiating element of the base station should be installed during operating at a separation distance greater than 20 cm between user and device. The device comply with the requirements for routine evaluation limits.