

UNIVERGE SV8100

IP DECT Installation Guide

NEC Corporation of America reserves the right to change the specifications, functions, or features at any time without notice.

NEC Corporation of America has prepared this document for use by its employees and customers. The information contained herein is the property of NEC Corporation of America and shall not be reproduced without prior written approval of NEC Corporation of America.

Dterm, NEAX and UNIVERGE are registered trademarks of NEC Corporation and Electra Elite is a registered trademark of NEC America, Inc.

Copyright 2014

**NEC Corporation of America
6535 N. State Highway 161
Irving, TX 75039-2402**

Communications Technology Group

TABLE OF CONTENTS

Chapter 1

Section 1	Important.....	1-1
Section 2	Product Disposal Information (EN).....	1-1
Section 3	Third Party Software	1-2
3.1	SRTP	1-3
3.2	TLS	1-3

Chapter 2

Section 1	Description.....	2-1
Section 2	Installing the NEC IP/Digital Manager	2-1
2.1	Installing the IP/Digital Manager	2-1
2.2	Configure the Call Manager for Licensing	2-8
2.2.1	License Manager Client (LMC)	2-8
2.2.2	License Manager System (LMS)	2-10
2.2.3	USB Dongle	2-11

Chapter 3

Section 1	General Description	3-1
Section 2	RFP- PP Communication	3-4
Section 3	Beacon Signal.....	3-6

3.1	General.....	3-6
3.2	Beacon Signal and PP.....	3-6
Section 4	Call Handling Procedures between PP and RFP.....	3-7
4.1	Setting Up a Call.....	3-7
4.2	Paging and Answering a Call	3-7
4.3	Encryption.....	3-7
Section 5	Cluster Arrangement.....	3-7
5.1	General.....	3-7
5.2	RFP Behavior in a Cluster	3-8
5.3	PP Behavior in a Cluster	3-8
Section 6	Handover.....	3-9
Section 7	Call Quality Control.....	3-9
Section 8	Subscription and De-Subscription	3-10
Section 9	Secondary Access Right Identifier (SARI)	3-12

Chapter 4

Section 1	System Architecture	4-1
1.1	DAP	4-2
1.2	DAP Controller/Manager	4-2
1.3	SIP Proxy.....	4-3
1.4	SIP Registrar	4-3
1.5	VLAN Router	4-3
1.6	PC with WEB Browser.....	4-3
Section 2	Handset Subscription/Registration	4-4
Section 3	Automatic Distribution When DAP Down	4-6

Section 4	Handset Registration in SIP Registrar	4-7
Section 5	Handover Mechanism	4-7
Section 6	Is DAP Manager Required?	4-10
Section 7	Radio Synchronization	4-12
7.1	How it Works	4-12
7.2	Synchronization Hierarchy.....	4-13
7.3	Coverage and Signal Strength Calculation.....	4-15
Section 8	IP Port Number Assignments.....	4-16
Section 9	DAP Characteristics.....	4-16
9.1	General.....	4-16
9.2	Common Characteristics	4-17
9.3	AP200 Characteristics (not available anymore)	4-18
9.4	AP200S (not available anymore).....	4-18
9.5	AP200E (not available anymore).....	4-18
9.6	AP300.....	4-18
9.7	AP300E	4-19
9.8	AP400.....	4-19
9.9	AP400G	4-19
9.10	AP400E	4-19
9.11	AP400C	4-19
9.12	AP400S	4-19
Section 10	AP200/AP200S Power Provision.....	4-19
Section 11	AP300/AP400 Power Provision	4-20
Section 12	More than 256 DAPS	4-20
Section 13	RPN Number Ranges per Branch Office	4-20

Chapter 5

Section 1	General	5-1
Section 2	Functional Licenses	5-1
Section 3	Project Based Licenses	5-2
Section 4	System Assurance License	5-3
Section 5	From Release 5 to Release 6	5-3
Section 6	DMLS Licenses	5-4
Section 7	Where to Enter and Where to Find the License Data?	5-4

Chapter 6

Section 1	Typical Configurations	6-1
Section 2	Simple Configuration	6-1
	2.1 Network Configuration	6-1
	2.2 Settings in DAP Configurator	6-2
Section 3	Branch Office Solution	6-3
	3.1 Network Configuration	6-3
	3.2 Settings in DAP Configurator	6-5
Section 4	Routed Head Quarter	6-5
	4.1 Network Configuration	6-5
	4.2 Settings in DAP Configurator	6-7
Section 5	Routed Head Quarter with Branch Offices	6-8
	5.1 Network Configuration	6-8
	5.2 Settings in the DAP Configurator	6-9
Section 6	Routed Head Quarter with Branch Offices	6-10

6.1	Network Configuration	6-10
6.2	Settings in the DAP Configurator	6-11

Chapter 7

Section 1	General	7-1
Section 2	DAP Power Provision	7-1
Section 3	DHCP and TFTP Requirements	7-2
3.1	DHCP Server	7-2
3.2	TFTP Server	7-3
3.3	Operation without DHCP or TFTP Server	7-3
3.4	Using other DHCP and/or TFTP Servers	7-4

Chapter 8

Section 1	Hardware Requirements	8-1
Section 2	Software Requirements	8-1
2.1	Operating System	8-1
2.2	IIS and Internet Explorer	8-2
2.3	.NET Framework	8-2
2.4	DHCP Server and TFTP Server	8-2
Section 3	Virtualization	8-3
Section 4	Marathon Fault Tolerancy	8-3

Chapter 9

Section 1	PreConditions	9-1
Section 2	Installing the DAP Controller Release 6	9-1

Chapter 10

Section 1	General.....	10-1
Section 2	Using the DAP Configurator.....	10-1
2.1	Setting Up the Configuration	10-1
Section 3	System Control Section.....	10-5
3.1	General.....	10-5
3.2	System Status Window.....	10-6
Section 4	Single Site / Multi Site.....	10-8
4.1	Switching between Single Site and Multi Site.....	10-8

Chapter 11

Section 1	Settings Buttons.....	11-1
Section 2	General Settings.....	11-1
Section 3	IP Settings.....	11-3
3.1	The Window.....	11-3
3.2	IP Settings, Tab "DAPs IP Configuration"	11-3
3.3	IP Settings, tab "DAP Controller IP Configuration"	11-4
3.4	IP Settings, tab "Proxy IP Configuration"	11-6
3.4.1	Multiple SIP Proxies Settings.....	11-8
3.5	IP Settings, Tab "CDA IP Configuration"	11-8
Section 4	Network Settings 11-9	
4.1	Network Settings, Tab "Network Card Settings".....	11-9
4.2	Network Settings, Tab "DHCP Settings"	11-11
4.3	Network Settings, Tab "TFTP Settings"	11-12
4.4	Network Settings, Tab "Leased IP Addresses"	11-14

4.5	Network Settings, Tab "QoS Settings"	11-15
4.6	Network Settings, Tab "Boot options".....	11-16
Section 5	System Configuration	11-17
5.1	Simple Configuration	11-18
5.2	Multiple Subnets.....	11-18
5.3	Routed Head Quarter	11-21
Section 6	SIP Settings	11-22
6.1	SIP Settings, Tab "General Settings"	11-22
6.2	SIP Settings, Tab "Configuration Settings".....	11-23
6.3	SIP Settings, Tab "Authentication Settings"	11-26
Section 7	DECT Settings	11-28
7.1	DECT Settings, Tab "DECT Settings"	11-28
7.2	DECT Settings, Tab "Handset Settings".....	11-29
7.3	DECT Settings, Tab "DAP Settings".....	11-31
7.4	DECT Settings, Tab "Synchronization Settings"	11-32
Section 8	PBX Settings.....	11-32
8.1	PBX Settings, Tab "Handset Sharing"	11-32
8.2	PBX Settings, Tab "Three party conference Settings"	11-33
Section 9	Performance / E-mail Settings	11-34
9.1	Performance / E-mail Settings, Tab "PCR Settings"	11-34
9.2	Performance / E-mail Settings, Tab "Alarm Settings".....	11-36
9.3	Performance / E-mail Settings, Tab "Archive Settings"	11-37
9.4	Performance / E-mail Settings, Tab "E-mail Settings".....	11-39
9.5	Performance / E-mail Settings, Tab "Miscellaneous Settings"	11-40
9.6	Customer Information	11-41

9.7	Save System and Start System	11-42
9.8	Finishing Advice.....	11-42
9.9	License Handling	11-42
9.9.1	Install a New License File	11-42
9.9.2	Reading out the Licenses	11-43
9.9.3	License Information Window.....	11-44

Chapter 12

Section 1	General	12-1
1.1	Voice Redundancy.....	12-1
1.2	Roaming Redundancy	12-1
1.3	Messaging Redundancy	12-2

Chapter 13

Section 1	General	13-1
Section 2	DAP Controller Redundancy in Messaging Configuration.....	13-2
Section 3	DAP Controller Redundancy - How does it work	13-6
Section 4	Local DAP Controllers	13-8
Section 5	Secondary DAP Controller in Branch Office location.....	13-9
Section 6	How to Set Up	13-10
6.1	Setting up the Redundant Configuration.....	13-10
Section 7	DECT Management.....	13-12
Section 8	How to Create an Archive	13-12
Section 9	Actual Status Indication.....	13-12

Chapter 14

Section 1	Implementation.....	14-1
Section 2	Selection Mechanisms.....	14-2
Section 3	Examples.....	14-3
3.1	Example "Fail Over"	14-3
3.2	Example "Alternating"	14-4
3.3	Example "Load Balancing"	14-6
3.4	Example "Using Different Domains"	14-7

Chapter 15

Section 1	General.....	15-1
Section 2	Prepare files for TFTP Upload to DAPs.....	15-1
2.1	Copying Files to the TFTP Directory	15-1

Chapter 16

Section 1	Opening the DAP Manager WEB Interface.....	16-1
------------------	---	-------------

Chapter 17

Section 1	What it Is	17-1
1.1	Portable Sharing and the DAP Manager	17-2

Chapter A

Chapter B

Section 1	Overview of Differences	B-1
------------------	--------------------------------------	------------

1.1	Main Differences	B-1
1.2	Mechanical Differences	B-2
1.3	Outdoor Cabinet Differences	B-3

Chapter C

Section 1	Overview of Differences.....	C-1
1.1	Main Differences	C-1

Chapter D

Section 1	General	D-1
Section 2	Main Characteristics	D-1
Section 3	Call Handling.....	D-2
Section 4	Configurable Items in IP DECT SIP	D-3
Section 5	TLS AND SRTP SUPPORT	D-5
5.1	General	D-5
5.2	TLS	D-5
5.3	SRTP	D-6
5.4	Configurable Items in IP DECT.....	D-6

Chapter E

Section 1	General	E-1
Section 2	Types of Messages.....	E-3
Section 3	Broadcast Messaging	E-3
3.1	General	E-3
3.2	Additional Broadcast Type Messages	E-4

	3.3	How about Normal, Urgent, Emergency Messages	E-5
Section 4		SIP Messaging and DASGIF Messaging (IP DECT Rel. 5.00_401 or higher).....	E-6

Chapter F

Section 1		Generic Information	F-1
Section 2		Software Requirements	F-2
Section 3		How to Set it Up.....	F-2
	3.1	IP DECT SIP With Branch Offices.....	F-2
	3.1.1	Setting up IP DECT SIP Mobility with Branch Offices	F-2
	3.2	IP DECT SIP With Branch Offices and Traditional DECT	F-3
	3.2.1	Setting up Traditional DECT to Work with IP DECT SIP	F-3

Chapter G

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF FIGURES AND TABLES

Figure 2-1	D ^{term} VSR Call Manager – Welcome Screen	2-2
Figure 2-2	D ^{term} VSR Call Manager – License Agreement Screen	2-3
Figure 2-3	D ^{term} VSR Call Manager – Choose Destination Location Screen	2-4
Figure 2-4	D ^{term} VSR Call Manager – Select License System Screen	2-5
Figure 2-5	D ^{term} VSR Call Manager – Ready to Install the Program Screen	2-6
Figure 2-6	D ^{term} VSR Call Manager – Wizard Complete Screen	2-7
Figure 2-7	D ^{term} VSR Call Manager – Play History Tab	2-8
Figure 2-8	D ^{term} VSR Call Manager – Select License Manager Client (LMC)	2-9
Figure 2-9	D ^{term} VSR Call Manager – Select License Manager System (LMS)	2-10
Figure 2-10	USB Key Error – Call Manager	2-11
Figure 2-11	D ^{term} VSR Call Manager – Select USB Dongle	2-12
Figure 3-1	DECT System Parts (General)	3-2
Figure 3-2	DECT System Parts in an IP Solution as Add-on to a PBX	3-3
Figure 3-3	Carriers and Timeslots in the DECT Air Interface	3-5
Figure 3-4	Each time slot can use any of the 10 Carrier Frequencies	3-5
Figure 3-5	Cluster Arrangement	3-8
Figure 3-6	UAK Relation between the IPUI and the PARI	3-11
Figure 3-7	Using SARI in three DECT Systems	3-13
Figure 4-1	Business Mobility IP DECT - System Configuration	4-1
Figure 4-2	Phases in the Subscription Process	4-4
Figure 4-3	Subscription Locations	4-6
Figure 4-4	Call Connection Before Handover	4-8

Figure 4-5	Handover Action Started	4-9
Figure 4-6	Handover Taken Place, New Connection Active	4-10
Figure 4-7	Simple Business Mobility IP DECT configuration without DAP Manager	4-11
Figure 4-8	Radio Synchronization	4-13
Figure 4-9	Synchronization Structure	4-14
Figure 4-10	Signal Strength Considerations	4-16
Figure 6-1	Example of Simple IP DECT Network Configuration	6-2
Figure 6-2	Setup for Simple Configuration Example	6-3
Figure 6-3	Example of an IP DECT Configuration with a Branch Office	6-4
Figure 6-4	Branch Office Configurator Example	6-5
Figure 6-5	Example of an IP DECT Routed Head Quarter Configuration	6-6
Figure 6-6	Branch Office Configuration Example	6-7
Figure 6-7	Example of an IP DECT Routed Head Quarter Configuration with Branch Office	6-8
Figure 6-8	Routed Head Quarter with Branch Office Configuration	6-9
Figure 6-9	Example of an IP DECT Routed Head Quarter Configuration with a Routed Branch Office	6-10
Figure 6-10	Routed Head Quarter with Routed Branch Office Setup Configuration Example	6-12
Figure 7-1	Layout Ethernet Connector RJ45 on the DAP	7-2
Figure 9-1	System Configuration Check	9-2
Figure 9-2	Install Prerequisites	9-3
Figure 9-3	Install Shield Wizard	9-4
Figure 9-4	Choose System Type	9-5
Figure 9-5	Choose Setup Type	9-6
Figure 9-6	Ready to Install	9-7

Figure 9-7	Installation Complete	9-8
Figure 10-1	Starting DAP Configurator	10-2
Figure 10-2	Select License File	10-3
Figure 10-3	System Control	10-4
Figure 10-4	System Status Window	10-7
Figure 10-5	Reboot DAPS	10-8
Figure 10-6	DAP Configurator Icon	10-9
Figure 10-7	About Configurator	10-9
Figure 11-1	General Settings	11-2
Figure 11-2	IP Settings	11-3
Figure 11-3	DAP Controller IP Configuration 1	11-4
Figure 11-4	DAP Controller IP Configuration 2	11-5
Figure 11-5	DAP Controller IP Configuration 3	11-6
Figure 11-6	Proxy IP Configuration	11-7
Figure 11-7	CDA IP Configuration	11-9
Figure 11-8	Network Card Settings	11-10
Figure 11-9	DHCP Settings	11-11
Figure 11-10	TFTP Settings	11-13
Figure 11-11	Leased IP Addresses	11-14
Figure 11-12	QoS Settings	11-15
Figure 11-13	Boot Options	11-16
Figure 11-14	System Configuration	11-17
Figure 11-15	System Configuration Options	11-18
Figure 11-16	Multiple Subnets	11-19
Figure 11-17	Routed Head Quarter	11-21

Figure 11-18 SIP Settings - General Settings	11-23
Figure 11-19 SIP Settings - Configuration Settings	11-24
Figure 11-20 SIP Settings - Authentication Settings	11-27
Figure 11-21 DECT Settings	11-28
Figure 11-22 DECT Settings - Handset Settings	11-30
Figure 11-23 DECT Settings - DAP Settings	11-31
Figure 11-24 PBX Settings - Handset Sharing	11-33
Figure 11-25 PBX Settings - Three Party Conference Settings	11-34
Figure 11-26 Performance Email Settings - PCR	11-35
Figure 11-27 Performance/E-mail Settings - Alarm Settings	11-36
Figure 11-28 Alarm Notification	11-37
Figure 11-29 Performance/E-mail Settings - Archive Settings	11-38
Figure 11-30 Performance/E-mail Settings - E-mail Settings	11-39
Figure 11-31 Performance/E-mail Settings - Miscellaneous Settings	11-40
Figure 11-32 Customer Information	11-41
Figure 11-33 Import License	11-43
Figure 11-34 License	11-43
Figure 11-35 License Information Window	11-44
Table 11-1 License Items	11-45
Figure 13-1 DAP Controller Redundancy Configuration	13-2
Figure 13-2 Example of a Redundant IP DECT configuration with Messaging	13-3
Figure 13-3 Messaging when Primary DAP Controller Active	13-4
Figure 13-4 Messaging when primary DAP Controller down	13-5
Figure 13-5 Message from handset when Primary DAP Controller is active	13-6
Figure 13-6 DAP Controller Redundancy	13-7

Figure 13-7	Example of DAP Controller Redundancy with two Central DAP Controllers and two Local DAP Controller	13-9
Figure 13-8	Example of DAP Controller Redundancy with Secondary DAP Controller in the Branch Office	13-10
Figure 13-9	Redundant DAP Controller	13-11
Figure 13-10	Display Redundant Mode	13-13
Figure 14-1	Example of Proxy settings required for the "Fail Over" example	14-3
Figure 14-2	Example of Return to Primary Setting for "Fail Over" Example	14-4
Figure 14-3	Example of Proxy Settings Required for the "Alternating" Example	14-5
Figure 14-4	Return to Primary Setting for "Alternating" Example	14-5
Figure 14-5	Example of Proxy Settings Required for the "Load Balancing" Example	14-6
Figure 14-6	Example of Return to Primary Setting for "Load Balancing" Example	14-7
Figure 14-7	Proxy Settings Required for the "Using Different Domains" Example	14-8
Figure 14-8	Return to Primary Setting for "Using Different Domains" Example	14-9
Table 1	Overview of TFTP Servers	15-2
Table B-1	Main Differences between AP200 and AP300	B-1
Table B-2	Mechanical Differences AP200 - AP300	B-2
Table B-3	Outdoor Cabinet Differences AP200 - AP300	B-3
Table C-1	Differences between AP300 and AP400	C-1
Table D-1	Supported SIP Features	D-2
Table D-2	Configurable Items in SIP IP DECT	D-4
Figure E-1	Message Path in IP DECT - Messaging Server Configuration	E-2
Figure E-2	Outbound Messaging from Handset	E-7
Table D-1	Default ports used in Business Mobility IP DECT	G-1

THIS PAGE INTENTIONALLY LEFT BLANK

Preface

This manual is valid for Business Mobility IP DECT Software Release 6.0.

SECTION 1 IMPORTANT

This manual gives information for setting up a Business Mobility IP DECT system. However, the Business Mobility IP DECT is normally part of an IP network. The success of the installation depends on the structure and components in the IP network. Make sure that you have sufficient knowledge of the customers IP network.

The Business Mobility IP DECT is also a wireless data communication system. This requires knowledge of radio signal propagation. The radio signal propagation in Business Mobility IP DECT requires a different approach than for the traditional DECT systems. The success of the installation also depends on the radio signal propagation. Make sure that you have sufficient knowledge about this subject as well.

It is strongly advised to follow the Business Mobility IP DECT CE training. Please contact your IP DECT supplier.

No legal rights can be obtained from information in this manual.

SECTION 2 PRODUCT DISPOSAL INFORMATION (EN)

For countries in the European union:

The symbol depicted here has been affixed to your product in order to inform you that electrical and electronic products should not be disposed of as municipal waste.



Electrical and electronic products including the cables, plugs and accessories should be disposed of separately in order to allow proper treatment, recovery and recycling. These products should be brought to a designated facility where the best available treatment, recovery and recycling techniques is available. Separate disposal has significant advantages: valuable materials can be re-used and it prevents the dispersion of unwanted substances into the municipal waste stream. This contributes to the protection of human health and the environment.

Please be informed that a fine may be imposed for illegal disposal of electrical and electronic products via the general municipal waste stream.

In order to facilitate separate disposal and environmentally sound recycling arrangements have been made for local collection and recycling. In case your electrical and electronic products need to be disposed of please refer to your supplier or the contractual agreements that your company has made upon acquisition of these products.

At www.nec-unified.com/weee you can find information about separate disposal and environmentally sound recycling.

For countries outside the European union:

Disposal of electrical and electronic products in countries outside the European Union should be done in line with the local regulations. If no arrangement has been made with your supplier, please contact the local authorities for further information.

SECTION 3 THIRD PARTY SOFTWARE

Within the SRTP and TLS, open libraries are applied. The following text is applicable for these open libraries:

3.1 SRTP

For SRTP version 1.4.4 is applied. The following license text is applicable to the SRTP library:

Copyright (c) 2001-2005 Cisco Systems, Inc. - All rights reserved.

- Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:
- Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer
- Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
- Neither the name of the Cisco Systems, Inc. nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

3.2 TLS

For TLS version openssl-0.9.8e of the OpenSSL library is incorporated. The following license text is applicable to the OpenSSL Library:

OpenSSL License:

Copyright (c) 1998-2007 The OpenSSL Project. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgment: "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (<http://www.openssl.org/>)"
4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact openssl-core@openssl.org.
5. Products derived from this software may not be called "OpenSSL" nor may "OpenSSL" appear in their names without prior written permission of the OpenSSL Project.
6. Redistributions of any form whatsoever must retain the following acknowledgment: "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (<http://www.openssl.org/>)"

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT ``AS IS" AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).

Original SSLeay License Copyright (C) 1995-1998 Eric Young (eay@cryptsoft.com). All rights reserved.

This package is an SSL implementation written by Eric Young (eay@cryptsoft.com). The implementation was written so as to conform with Netscapes SSL.

This library is free for commercial and non-commercial use as long as the following conditions are adhere to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code.

The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (tjh@cryptsoft.com).

Copyright remains Eric Young's, and as such any Copyright notices in the code are not to be removed. If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used. This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgement: "This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)" The word 'cryptographic' can be left out if the routines from the library being used are not cryptographic related :-).
4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement: "This product includes software written by Tim Hudson (tjh@cryptsoft.com)"

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The licence and distribution terms for any publicly available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution licence [including the GNU Public Licence].

UNIVERGE SV8100 IP DECT Installation Guide


SECTION 1 DESCRIPTION

The **NEC IP/Digital Manager** provides advanced visibility, access, retrieval, and playback tools for the NEC BackOffice administrators. It also provides an intuitive interface for establishing shortcuts to any number of storage folders and allows the supervisor to search across all storage folders for specific call information such as User, Time/Date, Length of Call, etc. The application can be used to access and manage recordings whether created by the single port, the 4-Port Digital Logging Unit or IP. **IP/Digital Manager** is built on the robust Microsoft.net frame-work and manipulates large volumes of recordings. It is a workhorse that delivers truly feature rich productivity tools in a familiar, ergonomic and easy to use MS Office style interface.

IP/Digital Manager allows the manager or supervisor to quickly and easily gain access to important calls.

SECTION 2 INSTALLING THE NEC IP/DIGITAL MANAGER

2.1 Installing the IP/Digital Manager

 *Administrative privileges required for installation.*

1. Insert the Manager CD in the computer CD ROM drive or navigate to the location where you have saved your application download.

2. Double-click on the **Setup.exe** icon, the Dterm VSR Call Manager Welcome screen displays, [Figure 2-1 D^{term}VSR Call Manager – Welcome Screen](#).

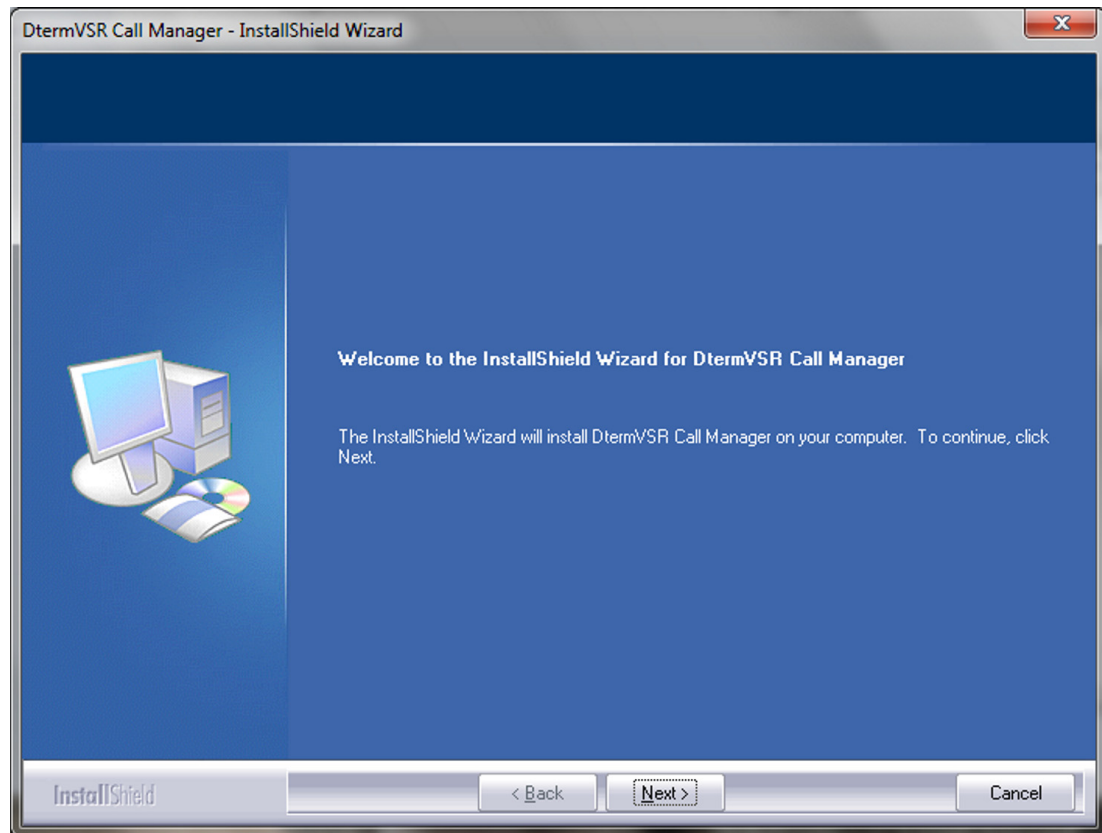


Figure 2-1 D^{term}VSR Call Manager – Welcome Screen

3. Click **Next**, the License Agreement screen opens, [Figure 2-2 D^{term}VSR Call Manager – License Agreement Screen](#).

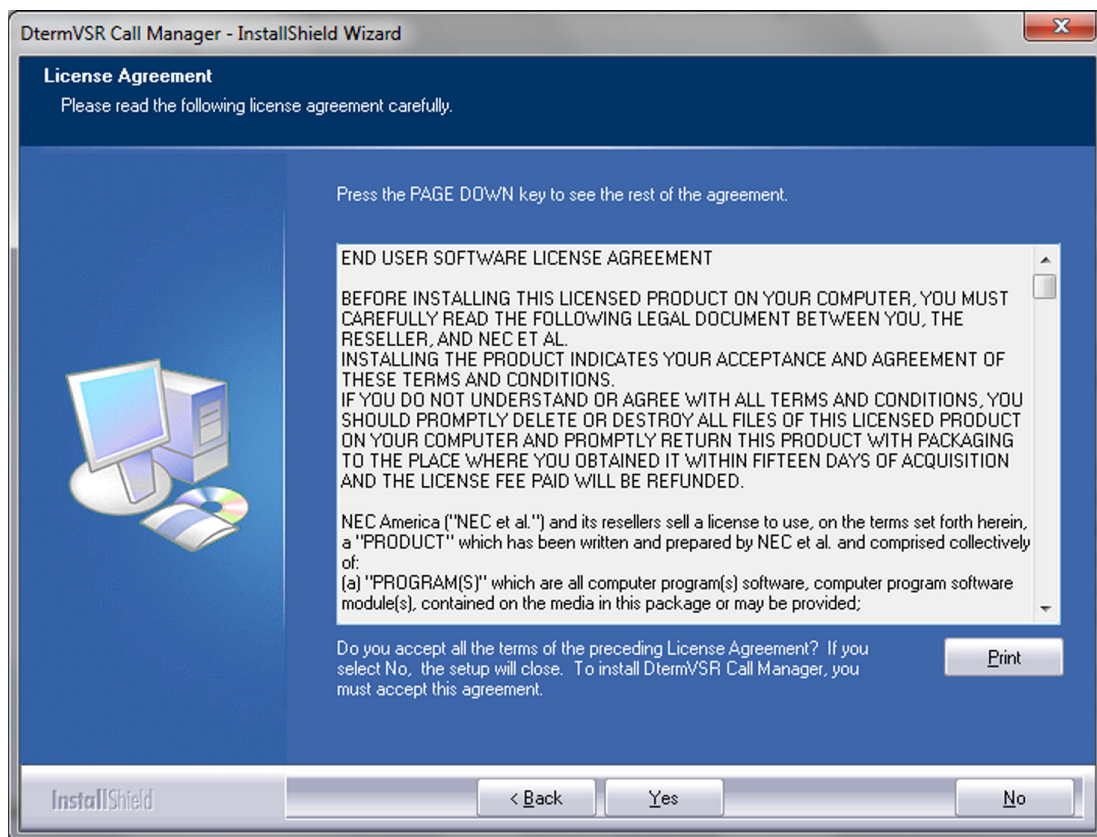


Figure 2-2 D^{term}VSR Call Manager – License Agreement Screen

4. Select **Yes**, the Choose Destination Location screen opens, [Figure 2-3 D^{term}VSR Call Manager – Choose Destination Location Screen](#).

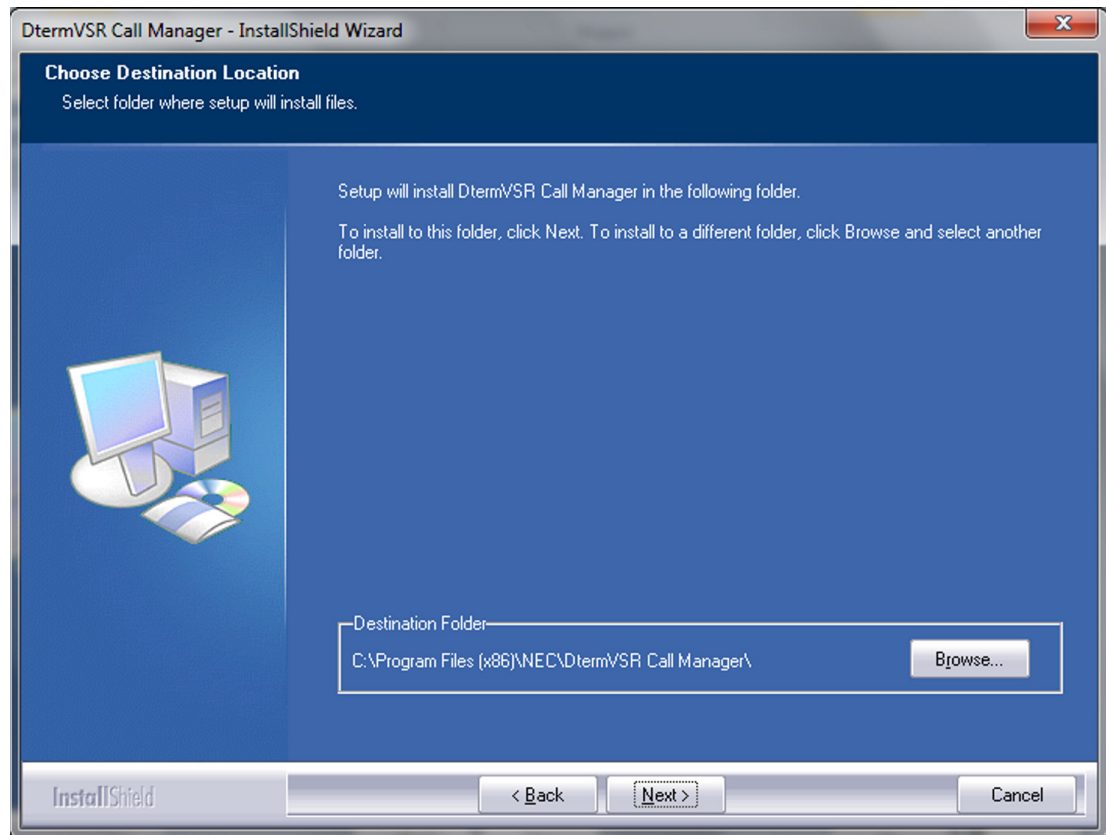


Figure 2-3 D^{term}VSR Call Manager – Choose Destination Location Screen

5. Click **Next**, the Select License System screen displays, [Figure 2-4 D^{term}VSR Call Manager – Select License System Screen](#).

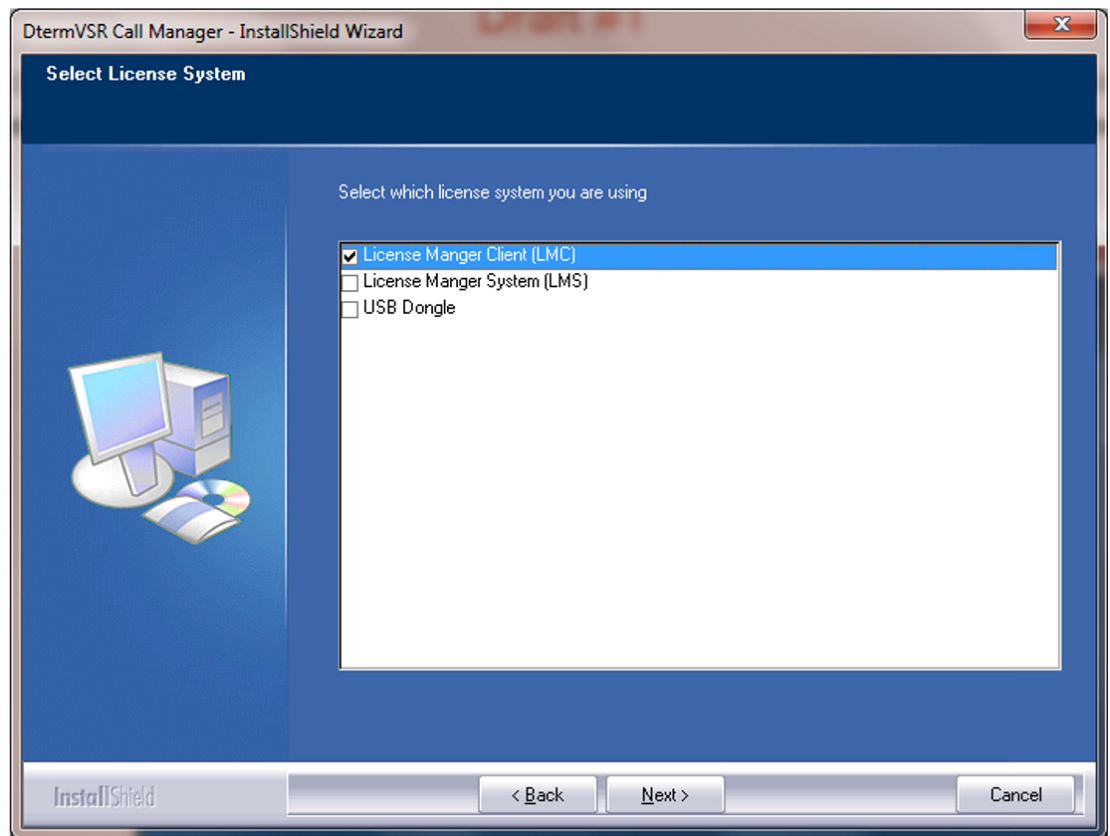



Figure 2-4 D^{term}VSR Call Manager – Select License System Screen

6. Select one license system:

License Manager Client (LMC) – SV8300

 License will be loaded to the LMC.

License Manager System (LMS) – SV8100

USB Dongle – Installing with a dongle key

7. Click **Next**, the Ready to Install the Program screen displays, [Figure 2-5 D^{term}VSR Call Manager – Ready to Install the Program Screen](#).

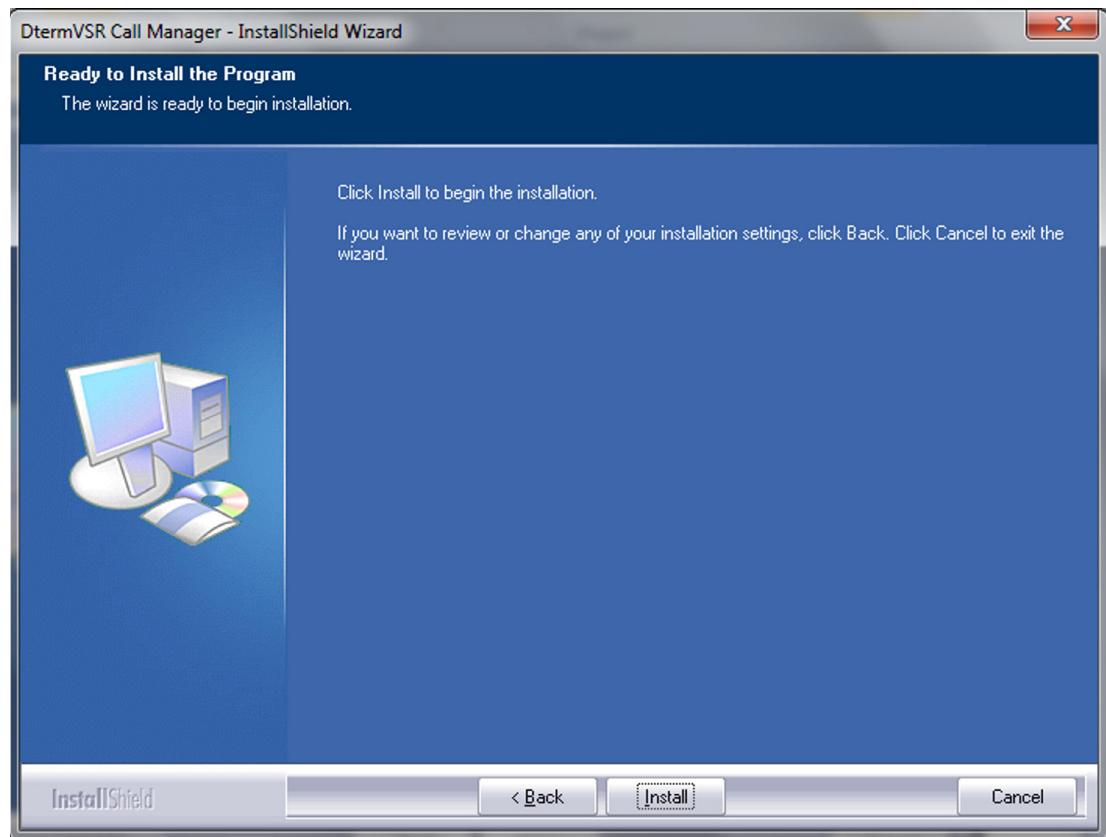


Figure 2-5 D^{term}VSR Call Manager – Ready to Install the Program Screen

8. Click **Install**, a screen displaying installation progress displays. When installation completes, a Wizard Complete screen opens, [Figure 2-6 D^{term}VSR Call Manager – Wizard Complete Screen](#).

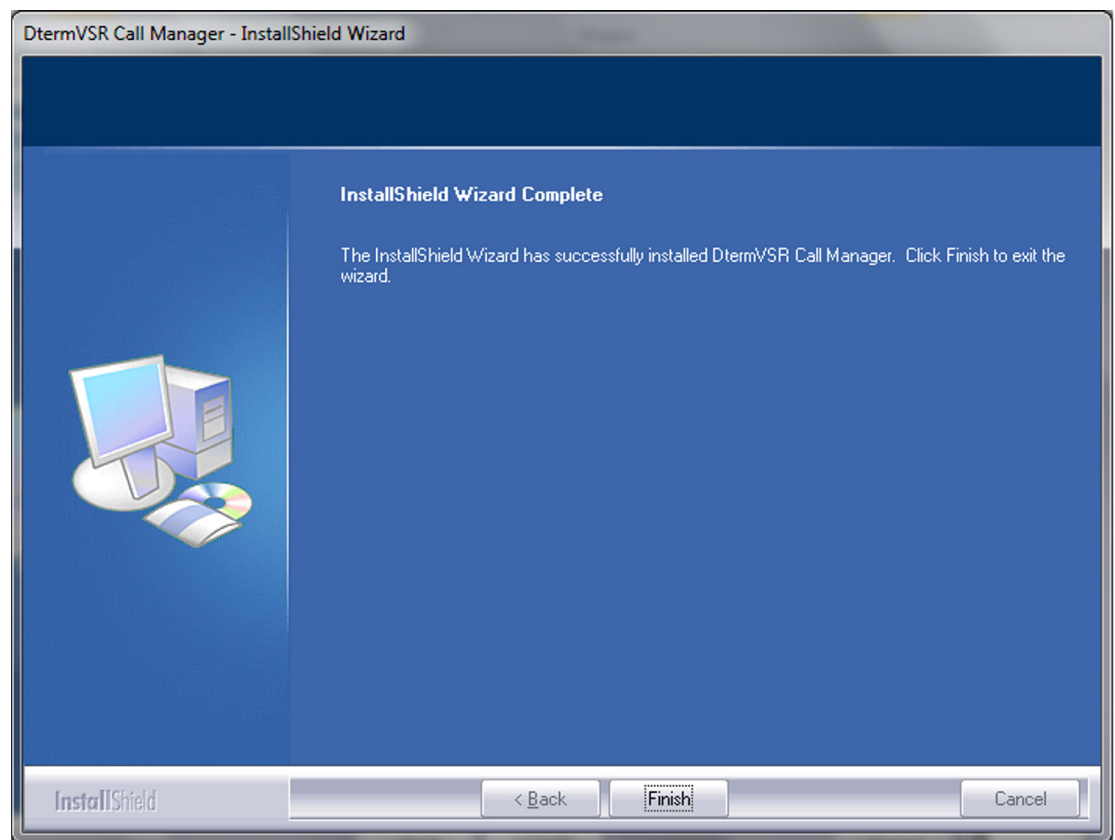


Figure 2-6 D^{term}VSR Call Manager – Wizard Complete Screen

9. Click **Finish**. Following initial installation, the Dterm VSR Call Manager screen opens displaying the Play History tab, [Figure 2-7 D^{term}VSR Call Manager – Play History Tab](#).

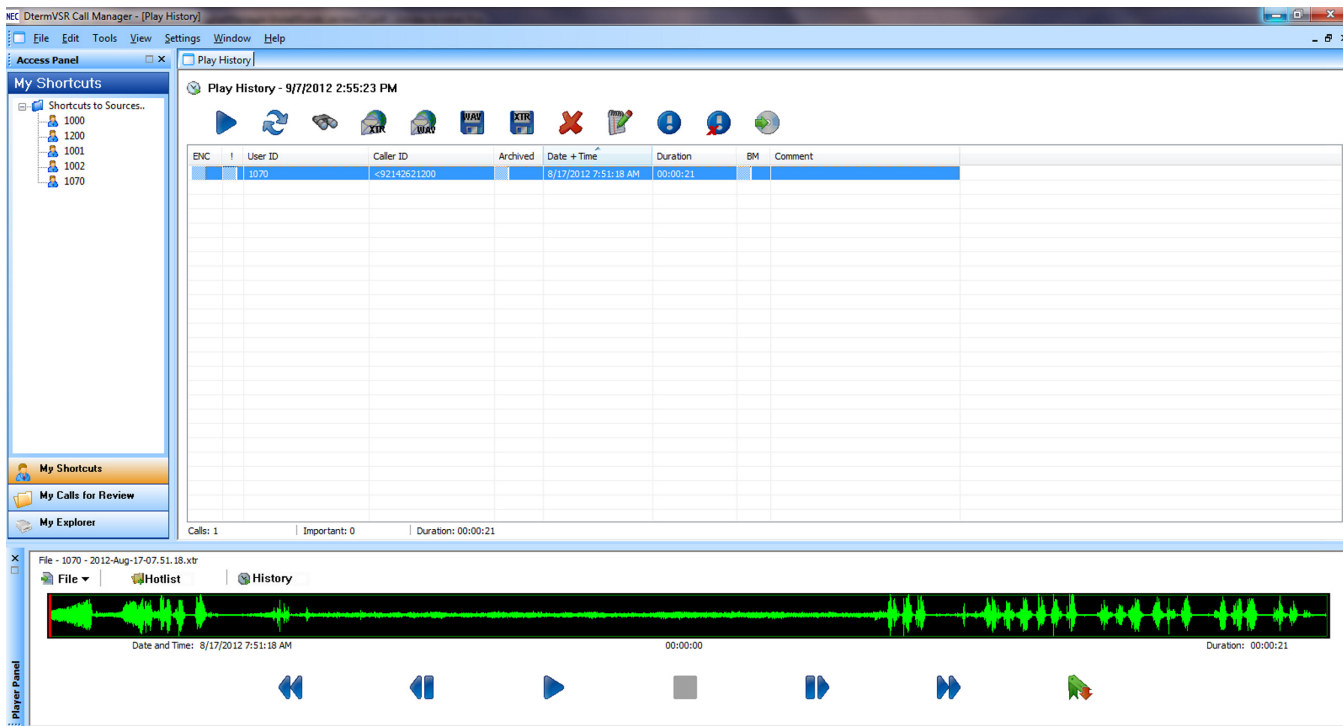


Figure 2-7 D^{term}VSR Call Manager – Play History Tab

2.2 Configure the Call Manager for Licensing

Three methods of Manager licensing are supported, depending on the system type and or if a dongle is used. Select **LMC** if installing on an SV8300, select **LMS** for the SV8100. Select **Dongle** if a dongle key was provided.

2.2.1 License Manager Client (LMC)

This method requires the license to be loaded on the SV8300 and the call logging application configured to retrieve license information from the PBX.

1. From Settings, select **License Server**. See [Figure 2-8 D^{term}VSR Call Manager – Select License Manager Client \(LMC\)](#).

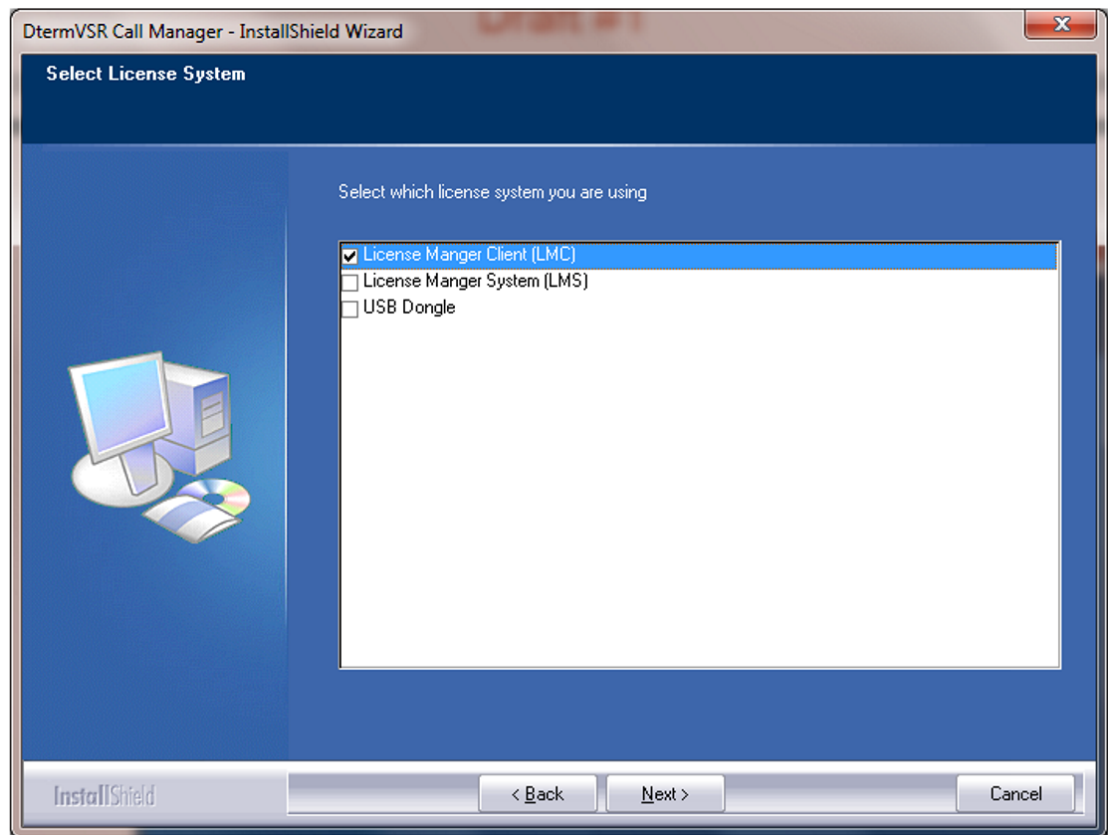


Figure 2-8 D^{term}VSR Call Manager – Select License Manager Client (LMC)

2. Select **License Manager Client (LMC)**.
3. Click **Next**, the Ready to Install the Program screen displays.
4. Click **Install**.
5. A screen displaying installation progress appears. When complete, select **Finish**.

2.2.2 License Manager System (LMS)

This method requires the license to be loaded on the SV8100 and the call logging application configured to retrieve license information from the PBX.

1. From Settings select **License Server**. See [Figure 2-9 D^{term}VSR Call Manager – Select License Manager System \(LMS\)](#).

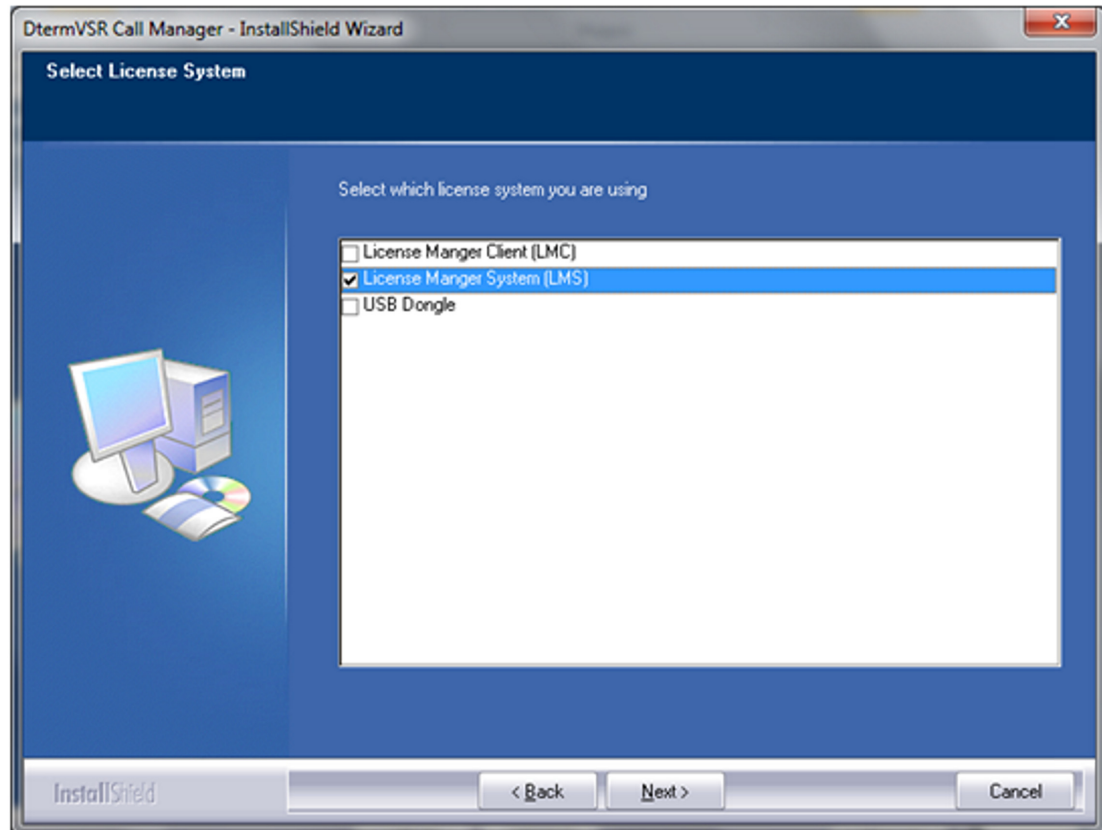


Figure 2-9 D^{term}VSR Call Manager – Select License Manager System (LMS)

2. Select **License Manager System (LMS)**.
3. Click **Next**, the Ready to Install the Program screen displays.
4. Click **Install**.
5. A screen displaying installation progress appears. When complete, select **Finish**.

6. If the Manager cannot find a license dongle, [Figure 2-10 USB Key Error – Call Manager](#) displays.

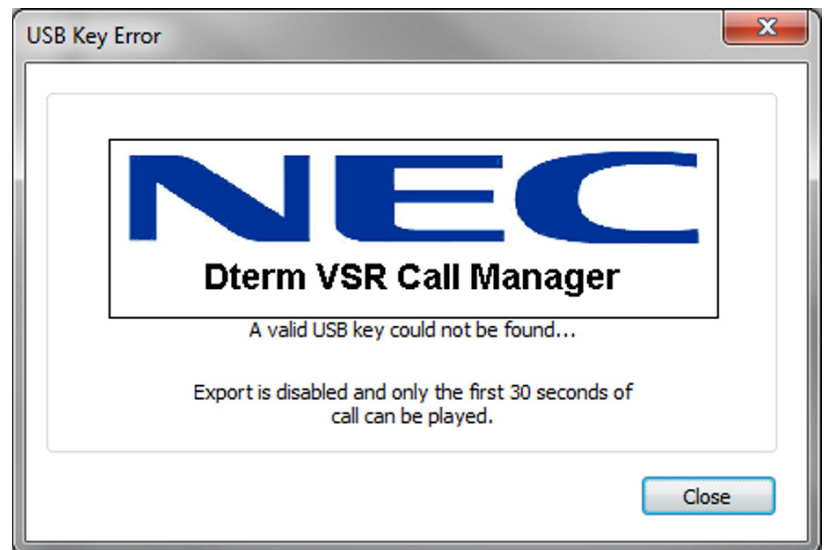


Figure 2-10 USB Key Error – Call Manager

7. Click on the **Close** button. Call Manager application launches.
8. From the main menu select **Settings > License Server**.
9. Enter the **IP address of your PBX or LMC**, then click **OK**.
10. Shut down the application.
11. Double-click on the **Dterm VSR Call Manager** icon.

2.2.3 USB Dongle

This method requires the use of a NEC IP/Digital application security key (USB dongle shipped with the application) and inserted when the Manager is running.



- *The Application Security Key is associated with your Software license.*
- *The Application Security Key is non-transferable and cannot be replaced if lost.*
- *If the key becomes damaged within the warranty period, you must return your key to support for verification and replacement if the nature of the damage qualifies.*

1. Select **USB Dongle**. See [Figure 2-11 D^{term}VSR Call Manager – Select USB Dongle](#).

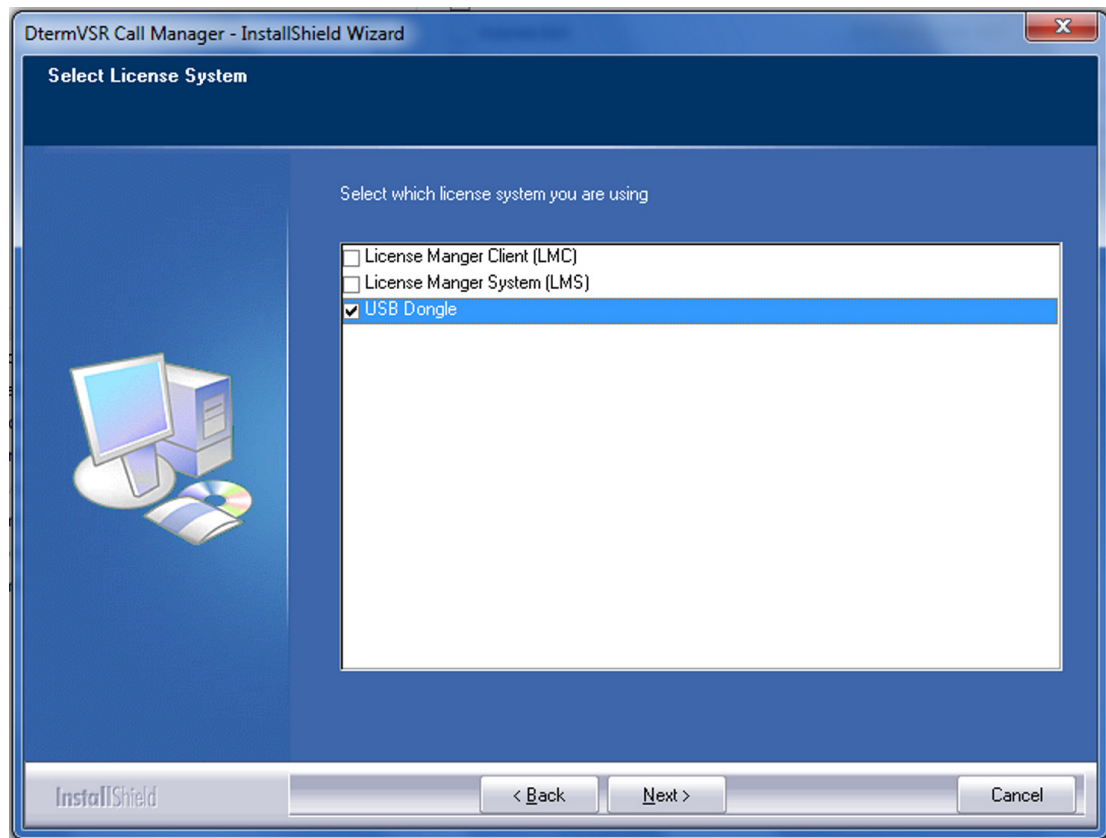


Figure 2-11 D^{term}VSR Call Manager – Select USB Dongle

2. Insert the USB dongle into an available USB port on the PC.
3. **Found New Hardware** displays, then Hardware successfully installed.
 - If Windows does not locate the driver, browse to the CD or download from NEC site. Drivers are located on the CD in the Driver folder.*
4. Click **Next**.
5. The Call Manager application launches.

DECT System Characteristics

SECTION 1 GENERAL DESCRIPTION

The DECT System allows mobile users to use the switched telecommunication facilities provided by a SIP Proxy system. Such a mobile user can make or receive calls by using a cordless handset. Many call handling facilities of the SIP Proxy are available on the cordless handset. As the cordless connection is a digital connection, other services will also be possible in the future.

The Digital Enhanced Cordless Telecommunication (DECT) interface has been developed by the European Telecommunication Standards Institute (ETSI).

Mobile users carry a portable handset which uses a radio transceiver to communicate with the DECT System. In this manual the DECT system is the Business Mobility IP DECT system connected to the SIP Proxy via a IP Ethernet connection. The radio transceivers are placed within the working area so that a portable handset/telephone is always within radio coverage area of at least one such transceiver.

The portable telephone is called a Portable Part (PP) according to the DECT standard. However, in this manual the portable telephone is also referred to as handset. It also contains a transceiver.

A radio transceiver in the DECT System is called the Radio Fixed Part (RFP) according to the DECT Standard. The RFP is also referred to as a base station. However, in the Business Mobility IP DECT configuration, the RFP is comprises more than just a transceiver, and is therefore called: DAP (DECT Access Point).

[Figure 3-1 DECT System Parts \(General\)](#) shows a general DECT system setup. [Figure 3-2 DECT System Parts in an IP Solution as Add-on to a PBX](#) shows a general IP DECT Solution. It shows the basic system setup for the Business Mobility IP DECT system.

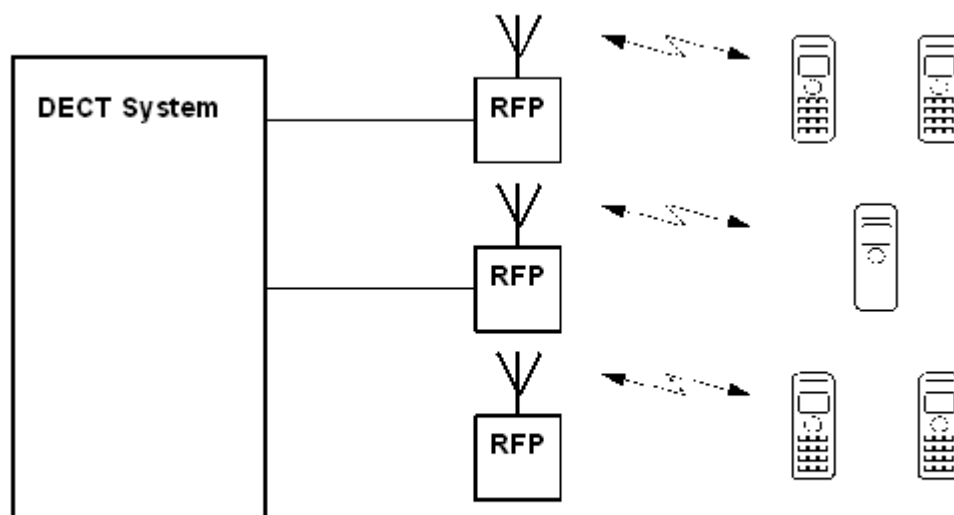
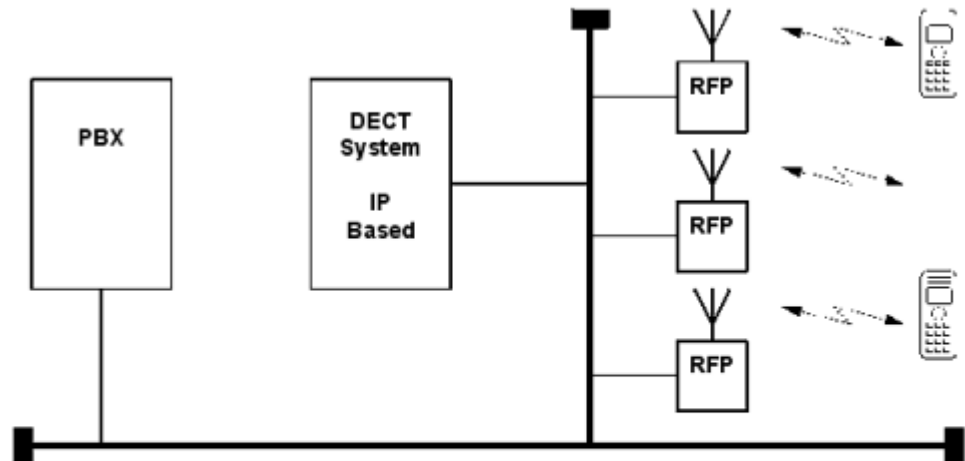


Figure 3-1 DECT System Parts (General)



Note: This figure shows a general system setup.
If applied to NEC IP DECT configuration, the:

DECT System IP Based = DAP Controller
PBX= PBX type that is supported by NEC IP DECT
RFP = DAP (DECT Access Point)

Figure 3-2 DECT System Parts in an IP Solution as Add-on to a PBX

The radio area covered by a single RFP (DAP) is called a cell. The RFPs (DAPs) are located so that the cells overlap slightly and the PP can remain in contact with the DECT system when moving from one cell to another. A group of cells belonging to one DECT system is called a cluster. According to the DECT standard, the maximum number of simultaneous calls per RFP can be 12. (The DAP in the Business Mobility IP DECT supports up to 12 simultaneous calls, depending on the licenses.)

The number of RFPs (DAPs) needed to cover a certain area (within which the mobile telephone users might roam) depends on many factors such as:

- ☐ The size of the area
- ☐ The nature of the area
 - ☐ The number and the size of buildings in the area
 - ☐ The radio propagation characteristics of the building(s)
 - ☐ Materials used for walls, floors, elevator shafts, reinforced glass, doors etc.
 - ☐ Strong magnetic fields in the area (e.g. as result of welding equipment, radar, etc.)

- ☐ The amount of telephone users in an area, and how often they make or receive calls

The speech signal through the air will be encrypted, if the portable handset allows it, to ensure the privacy of the conversation. This encryption is done fully automatically, without the intervention of a technician.

SECTION 2 RFP- PP COMMUNICATION

The radio link between the RFP and a PP can carry information on any one of ten carrier frequencies and in one out of twelve pairs of time slots (12 in each direction). The ten carrier frequencies are separated by 1728 kHz. The frequency range depends on the region where DECT is used:

- ☐ 1880 MHz - 1900 MHz for European countries
- ☐ 1910 MHz - 1930 MHz for Latin America region
- ☐ 1900 MHz - 1920 MHz for China
- ☐ 1920 MHz - 1930 MHz North America (lower transmission power, -3 dB)

The modulated data rate is 1152 kb/s. DECT uses in the OSI physical layer the following multiplexing techniques:

- ☐ FDMA (Frequency Division Multiple Access)
- ☐ TDMA (Time Division Multiple Access)
- ☐ TDD (Time Division Duplex)

The RFP-PP communication radio signal carries time division multiplexed frames; each frame is 10ms long. Each frame contains 12 time slots which carry data from RFP to the PPs, and 12 time slots which carry data from PPs to the RFP. This means that two time slots in every frame are needed for a full duplex connection to a PP. See [Figure 3-3 Carriers and Timeslots in the DECT Air Interface](#).

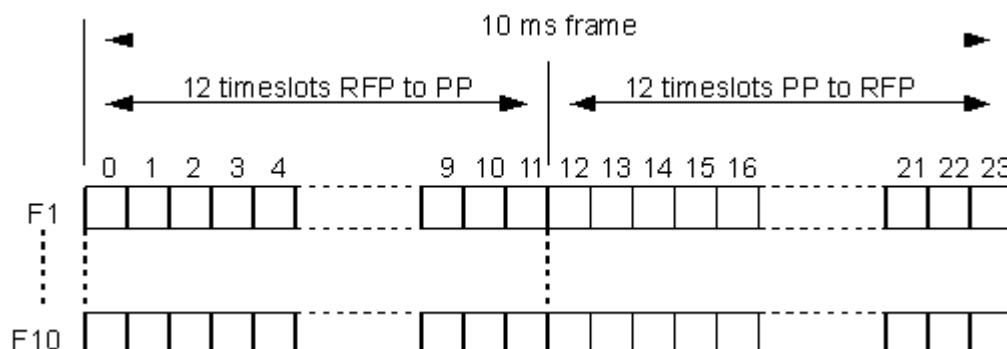


Figure 3-3 Carriers and Timeslots in the DECT Air Interface

Each time slot may carry 32 kbs Adaptive Differential Pulse Code Modulated (ADPCM) speech/user data. Each time slot pair can contain ADPCM speech/user data on any one of the ten carrier frequencies so that the RFPs carrier frequency often needs to be changed between time slots: Refer to [Figure 3-4 Each time slot can use any of the 10 Carrier Frequencies](#). The information within the time slot does not completely fill the time slot; time is allowed for propagation delays, ramp up and ramp down of the transmitter and for switching of the carrier synthesizer between slots.

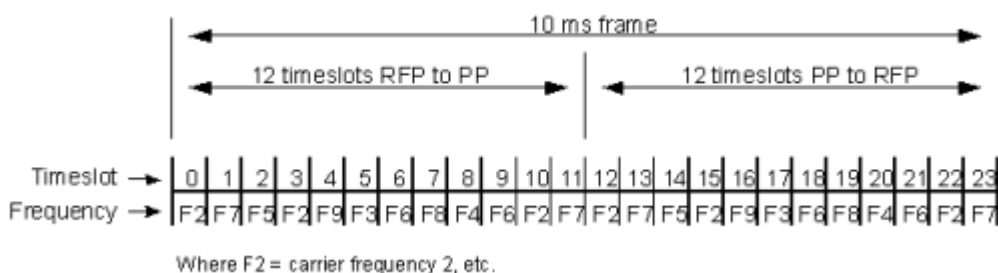


Figure 3-4 Each time slot can use any of the 10 Carrier Frequencies

A PP can use any of the 12 time slots (in each direction) on any of the 10 frequencies for a full duplex connection. So a maximum of 120 full duplex channels are available for connections to the PPs, within a cluster of a micro-cellular DECT system. In fact, this is only possible under ideal conditions; no disturbance, no interference, no other channels used, etc. Normally the conditions are not ideal in office or factory buildings, but the number of channels available will still be more than sufficient.

Note that there is always a fixed relation between the downstream timeslot number (from RFP to PP) and the upstream timeslot number (from PP to RFP) in one connection:

- ☐ Upstream timeslot number = downstream timeslot number +12
- ☐ Upstream and downstream timeslot in one connection use always the same carrier frequency

SECTION 3 **BEACON SIGNAL**

3.1 **General**

The beacon signal is a signal which is transmitted by an RFP in case the RFP is idle (no active calls).

This beacon signal contains the System Identifier of the DECT System, the so called PARI (Primary Access Rights Identifier) and the number of the RFP, the RPN (Radio Part Number). By means of this information the PP recognizes to which system a signal belongs, and whether it is subscribed to that system or not. When there is a call for a PP, it also contains paging information.

When the RFP is not idle (there is an active call via the RFP), the beacon signal information is also transmitted in the call connection. Therefore, the beacon signal is not necessary at an RFP which has one or more calls active. In the DECT application in the Business Mobility IP DECT, there are two beacon signals transmitted per RFP (DAP) when the RFP (DAP) is in idle condition. If there is a call only one beacon signal remains active. When there are a number of calls via the RFP (DAP), no beacon signal is transmitted anymore.

3.2 **Beacon Signal and PP**

When the PP is in idle condition (not involved in a conversation) it scans the environment for the signals of a nearby RFP (DAP). It locks onto the best signal that can be found. This signal can be a beacon or a channel which is used for a call, because such a channel contains the beacon signal information.

The PP uses the signal to synchronize its timing with the central system, and then it monitors the information transmitted via that RFP for calls to itself.

If the PP detects too many errors in the received signal (due to interference or weak signal) the PP tries to find another better signal and locks onto another RFP.

In this way, the PP user can move around the area from cell to cell and remain in contact with the DECT system via a radio link with a very good quality.

SECTION 4 **CALL HANDLING PROCEDURES BETWEEN PP AND RFP**

4.1 **Setting Up a Call**

In case the PP user wants to make a call, he/she goes off hook. The PP selects an unused channel at the RFP to which it is locked. This channel is in one of the timeslots (0 ... 11) from RFP to PP; for the communication from the PP to the RFP, the corresponding timeslot is selected in the timeslot range 12 ... 23. This results in a full duplex connection via the air. The connection setup goes through this RFP via the Business Mobility IP DECT system to the SIP Proxy. (The voice connection is setup between the RFP/DAP and the SIP User Agent.)

4.2 **Paging and Answering a Call**

If a PP is locked to a system, it continuously scans the beacon signal for paging information. (This beacon signal can be part of an existing call or as standalone beacon.) If the PP recognizes its own address in the paging data, it selects an unused channel at that RFP to answer the call. This channel is in one of the timeslots (12 ... 23) from PP to RFP; the RFP uses the corresponding timeslot (0 ... 11) from RFP to PP to communicate with this PP. After the setup of the channel/bearer has been successful, the handset starts alerting the mobile user. The user presses the "off-hook" key to answer the call. Then the speech path is opened via the bearer that has already been setup.

4.3 **Encryption**

Most portable sets are capable of encryption and so the user data is encrypted over the air interface. This ensures the privacy of the conversation. Encryption is a process by which the digitised speech is "scrambled" making it impossible for anyone monitoring the frequency to listen to the conversation. For this scrambling, a DCK (DECT Ciphering Key) is used. This is a key which is agreed at the first time data has been transferred between the PP and the RFP (the moment that the PP "locks" to the DECT system).

SECTION 5 **CLUSTER ARRANGEMENT**

5.1 **General**

A cluster is defined as a logical group of radio cells belonging to one DECT system. Within this arrangement bearer handover is possible. [Figure 3-5 Cluster Arrangement](#) shows an ideal cluster arrangement of radio cells in which each cell has a boundary with a number of other cells. An omnidirectional radio signal is transmitted equally in all directions so that the actual radio signal from the RFP in cell 1 overlaps slightly into cell 2, cell 3, cell 4, and so on. Similarly, the radio signal from the adjacent cells overlap into cell 1. So, cell 1 can be seen as the

centre of a cluster of cells. If a certain frequency is used in a certain timeslot in cell 1, it cannot be used in any of the adjacent cells in the same timeslot because of interference at the cell boundary. But that same frequency can be used in cell 8.

Thus, within a cluster a certain channel/frequency combination can be used again, simultaneously, only if the cell which uses such a combination does not interfere with another cell which uses the same combination.

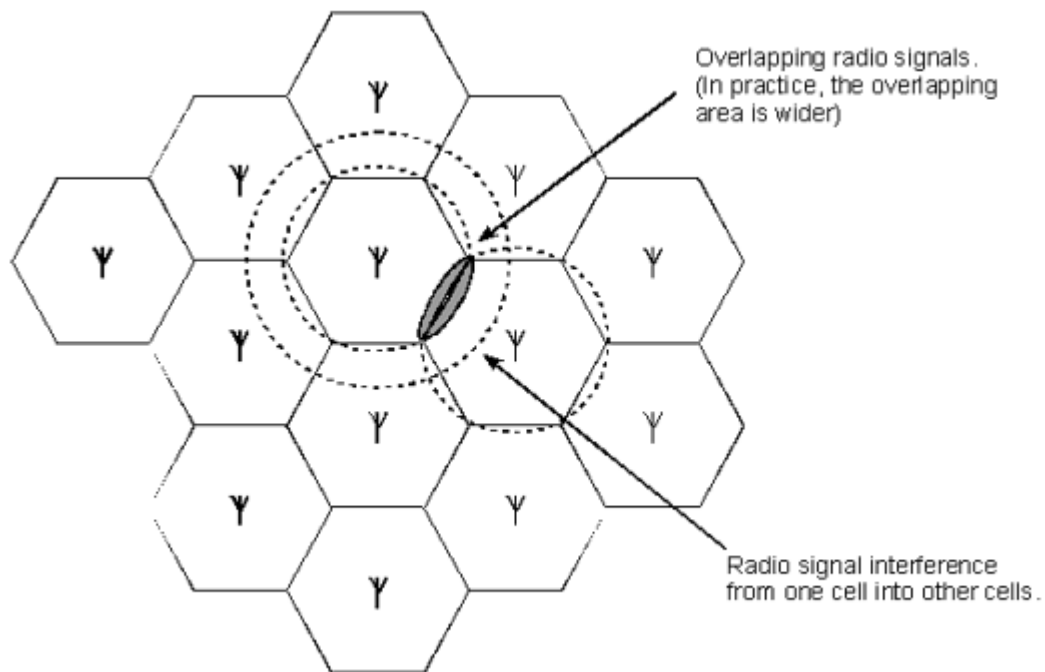


Figure 3-5 Cluster Arrangement

5.2 RFP Behavior in a Cluster

Each RFP constantly scans the area for signals in each channel. These signals can be generated by other RFPs or other equipment. The RFP selects one or two free channels to transmit the beacon signal. (The number of beacon signals depends on the number of active calls via the RFP.)

5.3 PP Behavior in a Cluster

The PP also picks up all sorts of signals which may come from the closest RFP, the next cell or from outside equipment. It locks onto a good RFP signal, and when it must make or receive a call it chooses a channel with the least interference to do this.

When a call is made to a portable telephone then that telephone must be paged. This means that all RFPs transmit a paging message. The information in each active timeslot transmitted by the RFP contains paging data, whether it is in use

for a connection or being used only as a beacon. If an idle PP is locked onto a beacon it examines the signalling data in that signal for paging data. Thus, it always receives all paging requests, so any calls to that PP will be received and recognized. When a paging request is detected for this PP, it starts setting up a connection with the RFP. The PP scans the channels regularly so that it knows which channels are available at the nearby RFP. The PP selects a channel which is not being used. It uses this channel to set up the call.


The PP alerts the PP user, who can then answer the call.

In case the PP user wants to make a call (own initiative), he/she presses the off-hook button. It starts setting up a connection with the RFP. (The PP scans the channels regularly so that it knows which channels are available at the nearby RFP.) The PP selects a channel which is not being used and uses this channel to set up the call.

SECTION 6 **HANDOVER**

Both the RFP and PP monitor the quality of the radio link. If the interference on a certain carrier frequency and timeslot combination causes problems, it might be necessary to switch to another frequency and/or timeslot at that same base station. This is called intra-cell handover. This handover procedure requires that the connection can be supported on 2 channels simultaneously, for a while, to allow a "seamless handover" (no breaks and hiccups during the handover). First, the new channel is chosen and the connection is set up via this channel, while the old channel is still in use. Then the old channel is disconnected.

If the mobile user roams from one cell to another, during the conversation, he goes probably out of range of the first RFP and into the range of the second. In that case, when the quality of the transmission requires it, the radio link switches over to the new RFP. This is called inter-cell handover. Once again it is a seamless handover.

 *If the mobile user roams from one cell to another, during the conversation, he goes probably out of range of the first RFP and into the range of the second. In that case, when the quality of the transmission requires it, the radio link switches over to the new RFP. This is called inter-cell handover. Once again it is a seamless handover.*

SECTION 7 **CALL QUALITY CONTROL**

Both the RFP and the PP monitor the quality of the call.

If the PP decides that the quality is not acceptable, it can do one of three things:

1. Request that the RFP uses its other antenna to communicate with the PP. The signal in the cell may suffer from fading, so that at one place the signal might be

poor while very close to it the signal may be acceptable. To counteract this, each RFP has two antennas mounted close together. The system tries to select the best antenna for each channel separately. This method of using two antennas is referred to as antenna diversity.

2. If the quality of the connection warrants it, the PP can request a handover to another channel. That channel may be on the same RFP (intra-cell handover) or on another RFP (inter-cell handover).

During handover, the communication to the PP is built up over the new channel so that for a short time the communication is available over both the old and the new channel. Then the old channel is disconnected. The user does not notice any break in the communication due to handover.

3. **Mute** the output (voice connections). It blocks the stream of information from radio signal to user (ear piece, in a telephone). This stops noisy signals being passed on to the user. It is done as a temporary measure, only. Note that muting is done on both ends of the connection independently.

If the RFP decides that the quality of the connection to a certain PP is not acceptable it can do one of three things:

1. Use the other antenna (antenna diversity). The PP does not notice the change.
2. Tell the PP that a handover is necessary. The PP always initiates the handover after selecting the best channel as seen from the PP.
3. It can temporarily block the data stream from PP to the SIP Proxy. (Note that muting is done on both ends of the connection independently.)

SECTION 8 SUBSCRIPTION AND DE-SUBSCRIPTION

Before a PP can be used, it must be subscribed (registered) to the system. That means that a relation must be defined between the DECT System and the PP. There are three identifiers used to define the relation between the system and the PP:

- ☐ **IPUI (International Portable User Identity)** - This is the identity number of a PP. It is issued from the system to the PP during subscription. From that time onwards, the PP is recognized by the system at its IPUI. This number is a unique number in the system, there is no other PP with the same IPUI.
- ☐ **PARK (Primary Access Rights Key), PARI (Primary Access Rights Identity), SARI (Secondary Access Rights Identifier)** - The PARI is a worldwide unique identifier for an individual DECT system. When stored in the handset, it is called the PARK. A DECT system can transmit a second "ARI" (Access Rights Identifier), called the SARI. The SARI is explained in [Section 9 Secondary Access Right Identifier \(SARI\)](#). The unique DECT system identifier (PARI, and sometimes also the SARI) is delivered on a certificate, together with

the system. It must be entered in the system manually.

- ❑ **UAK (User Authentication Key)** - This is a secret key which uniquely defines the relation between the PP and the DECT system (PARI or SARI)

When a PP is subscribed (made known) to a DECT system, the relation between the PARI of the DECT System and the IPUI of the PP is defined, see [Figure 3-6 UAK Relation between the IPUI and the PARI](#). The PARI is stored in the PP as PARK, the PP gets a unique identifier (IPUI) and a secret key (UAK) is assigned to the relation between the PP and the DECT System. From now on the PP knows to which system (PARI) it is subscribed. (In this section only the PARI is mentioned. For info on the SARI, consult [Section 9 Secondary Access Right Identifier \(SARI\)](#))

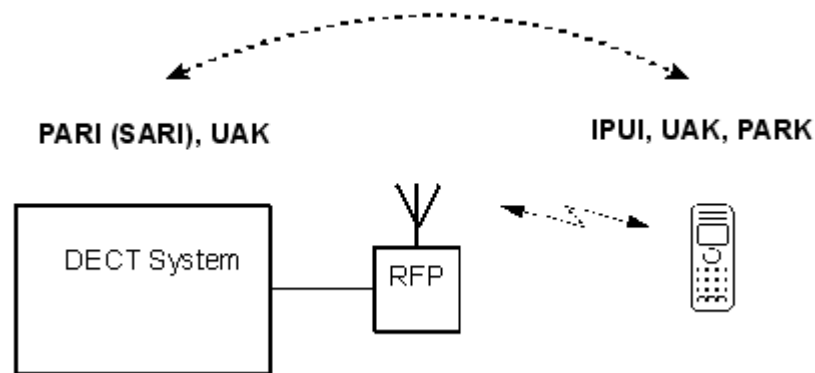


Figure 3-6 UAK Relation between the IPUI and the PARI

For the subscription procedure the WEB interface for Management must be used. This WEB interface provides access to the configuration settings in the DAP Controller/Manager, which is the Server that controls the DECT System. In the WEB interface for DECT Management, one or more extension numbers can be created and then selected to start the subscription procedure the (these) extensions (PP). Also one or more existing extension number(s) can be selected to subscribe a handset to. Then the DAP Controller/Manager generates a code ("PIN code" or also called "Authentication Code") which is visible via the WEB Interface. This code must be entered in the PP within a certain time period. If the operation has been completed successfully, the PP is subscribed to the system and is allowed to make and receive calls. (Assumed that the handset is known and registered in the PABX as well.)

A portable can be subscribed to more than one DECT system. Therefore, it can be used in areas covered by different DECT systems or in different areas with their own DECT system. This allows you for example, to use the same PP for the DECT system which is operational in your company and also for your home DECT. Also if the company is located at different sites, it is possible to use the same PP at the different sites, if DECT systems are present on these sites. It has a different extension number for each DECT system. It cannot roam from one of these areas to the other, while

busy with a conversation. The user of the portable must ensure that his set is communicating with the required DECT system, when making calls in a certain area. This may be done manually by a selection key, depending on the type of the portable. There are also PPs which selects DECT systems automatically.

The WEB interface for DECT Management can be used to de-subscribe ("terminate" or "disable") the PP. Such a service condition of a PP can always be displayed at the WEB interface for DECT Management.

A portable which has been "terminated", still contains the subscription data, but cannot gain access to the system. (If the PP supports a "reset" and this is executed at the PP, the subscription data in the portable is removed also.) The Administrator (user of the WEB interface for DECT Management) can use the "terminate" command (remove subscription) in case the portable has been lost or damaged.

A portable which has been "disabled" via the WEB interface for DECT Management has been put on the blacklist in the DAP Controller/Manager. When the PP is or becomes within reach of the radio signals, the DAP Controller/Manager and the PP exchange information which results in the de-subscription of that PP. It is no longer recognized by the DECT system and it is free to be subscribed again. This is the normal way to de-subscribe a portable set.

If a portable has been disabled, but the DECT System cannot reach the PP and complete the de-subscription, the "terminated" command can be used after the "disable" command.

SECTION 9 SECONDARY ACCESS RIGHT IDENTIFIER (SARI)

The SARI (Secondary Access Right Identifier) has the same function as the PARI, but it is used as a second identifier in case the PARI does not match between the DECT system and the PP.

The PARI is a unique number belonging to one DECT system only. The SARI can be the same identifier, used in more than one DECT system. The DECT system transmits both PARI and SARI as identification signals.

If the PP detects a DECT signal in the air, it checks whether the PARI in that signal matches with its own PARI data in the subscription record. If so, the PP "locks" to that signal. If not, the PP does a second check but now on the received SARI. If that matches, the PP "locks" to that signal.

The Secondary Access Rights (SARI) is used in case you want to use your PP on more than one DECT system (no handover possible between the systems!). The PP uses the same subscription record (comprising the PARK, IPUI and UAK) in the

handset for PARI or SARI. For using a SARI, you must subscribe your PP to one system, and copy the subscription record to other systems, all having the same SARI. You don't need to subscribe that PP anymore to the other systems.

Figure 3-7 Using SARI in three DECT Systems gives an example of three different DECT systems (three different PARIs) and one SARI. In this example the PP is subscribed to the SARI of system X. This SARI is not unique because the other systems have the same SARI. Therefore the subscription record can be copied from DECT System X to the other DECT Systems. (The DECT Manager allows you to copy the subscription record from one DECT System to another.) When the PP receives radio signals from system Y or system Z, it first checks the PARI of that system and if that doesn't match with its PARK it will do a check for the SARI of that system. The SARI matches with the PARK in the PP, and because the subscription data was copied, the UAK will also match. So, the PP can also be used on systems Y and Z.

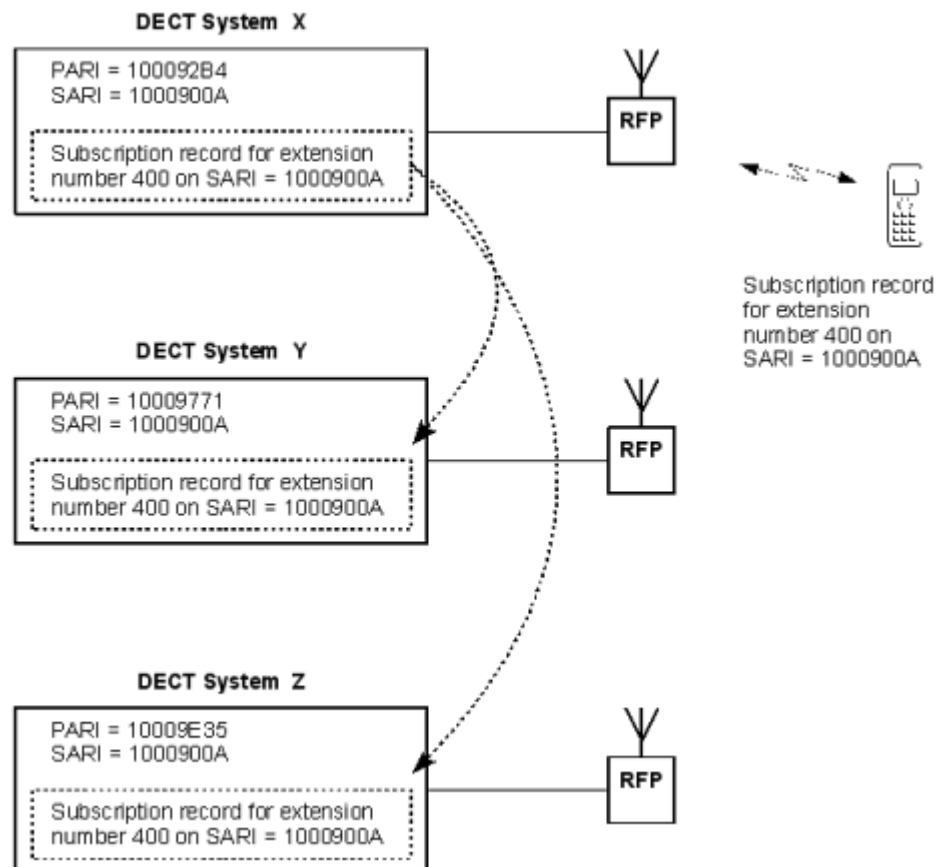


Figure 3-7 Using SARI in three DECT Systems

THIS PAGE INTENTIONALLY LEFT BLANK

DECT in IP Network

SECTION 1 **SYSTEM ARCHITECTURE**

In [Figure 4-1 Business Mobility IP DECT - System Configuration](#), you see the general configuration of the Business Mobility IP DECT system in an SIP Proxy configuration.

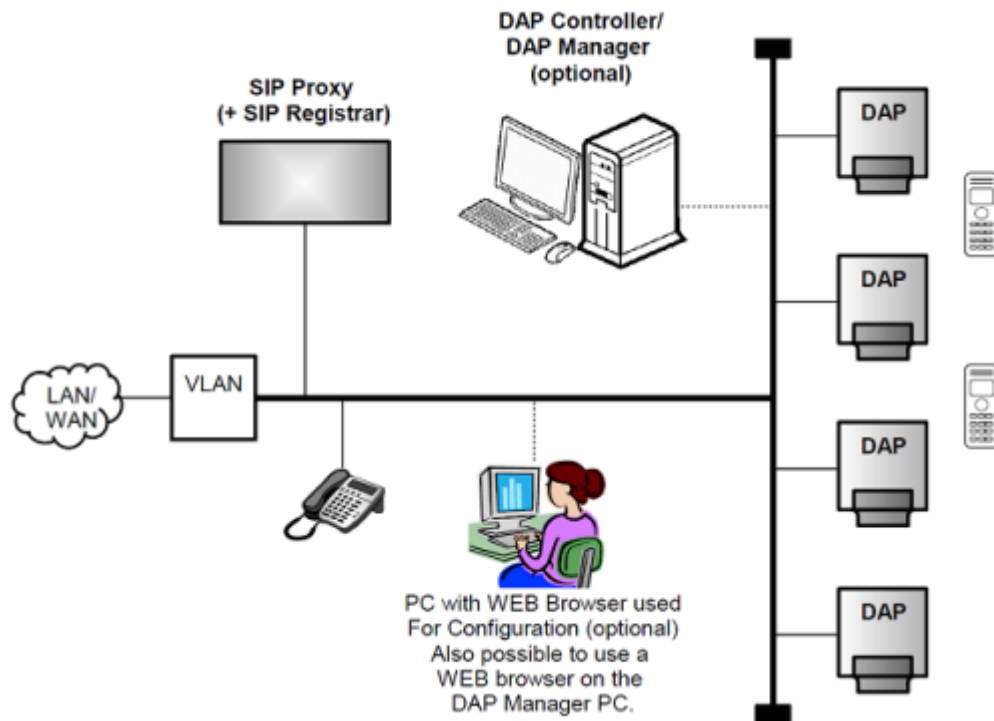


Figure 4-1 Business Mobility IP DECT - System Configuration

1.1 DAP

The DAP (DECT Access Point) is the actual DECT transmitter/receiver. There are three generations of DAP types: AP200, AP300 and the AP400. The AP400 series is the latest model.

All DAP Types supports up to 12 simultaneous calls. For the AP400, functionality licenses are applicable.

The DAPs are powered via the Ethernet interface (PoE).

Besides radio traffic, the DAPs take care of subscription control and call control data handling to/from the SIP Proxy.

The AP200, AP300 and AP400 are equipped with internal antennas. For all types, there is a version that supports connecting external antennas: the AP200E, AP300E and the AP400E.

1.2 DAP Controller/Manager

The DAP Controller/Manager performs the following main functions:

- WEB Server for management (based on IIS = Internet Information Services)
- Distribution of subscription data over the DAPs
- Firmware Uploading to handsets
- Collecting Subscription data
- Low rate messaging Services
- Controlling the IP DECT system in case there are Branch Office location

Besides the items mentioned above, the DAP Controller software comes with a Configurator, to setup the IP DECT Configuration.

When the Business Mobility IP DECT system is up-and-running and management actions are not needed, the DAP Manager can be disconnected and is not needed anymore, except for the following functions.



- Business Mobility IP DECT configuration with branch offices
- Low Rate Messaging Services (LRMS)
- Maintenance
- Collecting diagnostic data

1.3 SIP Proxy

The SIP Proxy Server accepts session requests made by a SIP UA (User Agent). The UA in this configuration, is the user that is subscribed to the IP DECT system, or any other SIP phone. When the SIP Proxy receives a call requests it will normally consult the SIP Registrar server to obtain the recipient UA's addressing information. The SIP Proxy can be combined with the SIP Registrar.

1.4 SIP Registrar

The SIP Registrar server contains a database with the address information of all User Agents in the SIP domain. The Registrar server receives and sends UA IP addresses and other pertinent information to the SIP Proxy server.

-  *The SIP Registrar and SIP Proxy are logical "roles" in the SIP structure that can be played by separate devices but also by one device. For the purpose of clarity, in the figures in this chapter the two roles are depicted on separate devices.*
-  *In this manual you will only see the SIP Proxy server and the SIP Registrar server and no other SIP servers like a SIP REdirect server or SIP Location server. The reason for this is that the IP DECT system (holding the SIP UA's) communicates with the SIP and Proxy and SIP Registrar and not to other SIP server types. The other SIP servers work on a different level in the SIP configuration.*


1.5 VLAN Router

The VLAN Router is a "switch" that separates the IP traffic between the WAN and the VLAN. It is strongly recommended to setup a dedicated Ethernet network for the Business Mobility IP DECT configuration because of the high Quality of Service (QoS) requirements.

The load on the network can be high due to rerouting of calls via the LAN.

1.6 PC with WEB Browser

Via the WEB Browser, you can access the DAP Manager. Via this WEB interface, you can subscribe handsets and change a limited number of configuration settings. Note that the WEB browser must be Internet Explorer 6.0 or higher!

-  *The WEB Browser is shown in the picture as a separate PC. However, the WEB browser on the DAP Controller PC can be used as well! This means that a separate PC with WEB browser is not necessary.*

When there is a call for a DECT handset, SIP Proxy sends a call setup message (Invite) to a DAP. The DAP forwards this message to the handset. When the handset goes off hook, the speech path is established between the handset, the DAP (as SIP UA) and the other party (other UA).

However, before you can establish a call, the handset must have been subscribed and registered in the SIP Registrar. If the handset is subscribed in the IP DECT system but not in the SIP Registrar, it is no problem because the registration will automatically take place. It is also possible to setup calls without registration in a Registrar server. In that case you must setup the Business Mobility IP DECT system, to communicate with the SIP Proxy only.

In the following sections, processes in the system are described in more detail.

SECTION 2 HANDSET SUBSCRIPTION/REGISTRATION

Before you can use a handset, the handset must be subscribed to the Business Mobility IP DECT system. Besides that the handset must be registered as UA in the SIP Registrar server. Subscription requires manual intervention, registration is done automatically. [Figure 4-2 Phases in the Subscription Process](#) shows the phases in the subscription process.

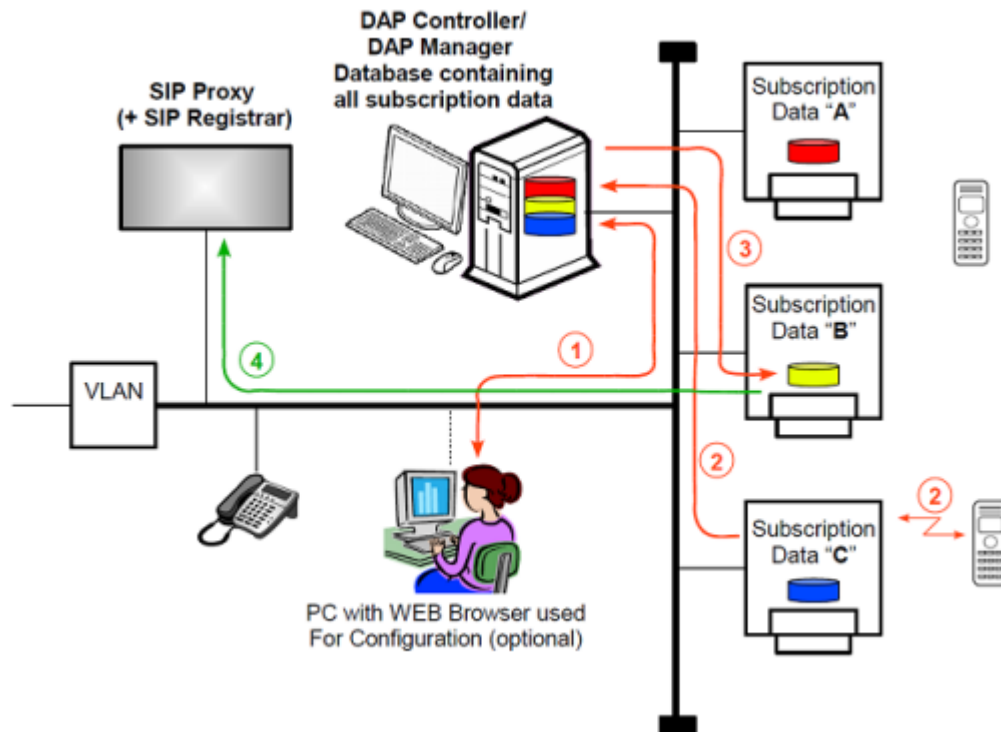


Figure 4-2 Phases in the Subscription Process

The following phases are distinguished in the subscription process.

1. The administrator starts a subscription process via the DECT Manager WEB

page. This WEB page is accessible from a WEB browser in the network. The administrator "enables" a subscription, which means that the subscription process is started. The Business Mobility IP DECT System is now waiting for action from a handset.

2. Now the subscription must be executed from the handset. The handset user must enter the PIN code that is displayed on the DECT Manager WEB page. When the PIN code is entered on the handset, the subscription record is created in the DAP Manager Database.
3. The DAP Manager will distribute the subscription data to one of the DAPs. Distribution has the following characteristics:
 - ◆ The DAP Manager tries to distribute the subscription records equally over the DAPs.
 - ◆ The maximum number of subscription records per DAP is 25.
 - ◆ Once a subscription record is stored into a DAP, it will normally not be moved to another DAP anymore. There are two exceptions on this: If you "Delete" a DAP manually from the DAPs list in the DECT Manager, the subscription records of that DAP will be distributed over the remaining DAPs. If the handset moves to/from a branch office, the subscription record moves with the handset to/from the branch office. Moving subscription between main site and branch office(s) is activated when the handset does a "location registration" in the main site or branch office. Note that the DAP Manager must be active to make this moving possible.
 - ◆ If DAPS are connected in a Branch office, the Branch office is regarded as a subscription island. The subscription record for a handset is either in a DAP at the main site or in a DAP at (one of) the branch office(s). When a handset executes a "location registration" at the main site or one of the branch offices, the subscription record is moved to the island where the location registration was done.
4. The DAP sends a SIP Register to the SIP Proxy/Registrar to register itself as a SIP extension (UA).

After the subscriptions are executed, each DAP contains a number of subscription records. The DAP Manager contains subscription data of all handsets in the system. If the DAP Manager is disconnected, the system remains operational.

The subscription records in the DAPs are stored in Flash Memory.

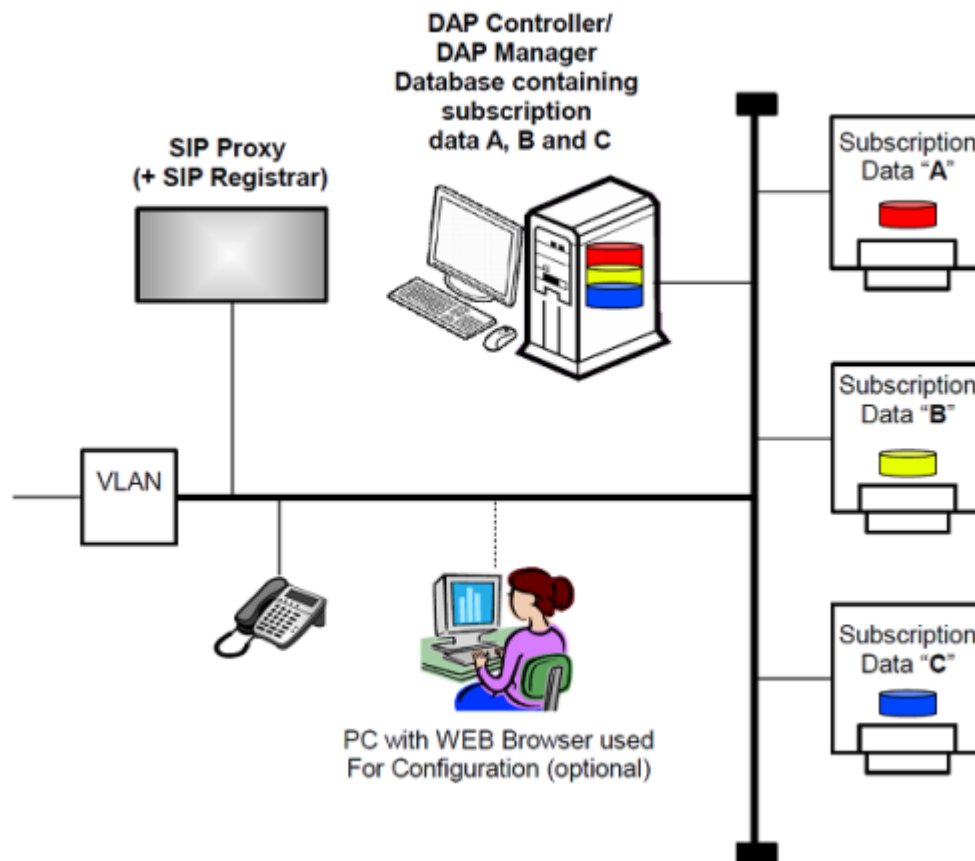


Figure 4-3 Subscription Locations

SECTION 3 **AUTOMATIC DISTRIBUTION WHEN DAP DOWN**

When a DAP goes down, the subscription records in that DAP are not accessible anymore, and therefore, the associated handsets cannot be used anymore. However, the subscription records of a broken DAP are automatically distributed over other DAPs after 10 minutes down time. This time is adjustable, the shortest time is 5 minutes.

This automatic distribution requires that the DAP Manager must be up and running. If not, automatic distribution does not take place!

When you connect the DAP Manager after a DAP went down, the timer starts from the moment that the DAP Manager is up and running. This means the you can replace the faulty DAP with a new one, with moving the original subscriptions to the new DAP within those 10 minutes. This time is configurable.


SECTION 4 **HANDSET REGISTRATION IN SIP REGISTRAR**


DECT Handset registration means that a DECT Handset makes itself know to the SIP Registrar. This information is needed to store relation between the extension (UA) number and its IP address and/or the full computer/device plus domain name. The Registrar holds a database containing the data of all UAs that are registered in the (local) domain.

Registration data can be stored for a limited time period only, which is by default 3600 seconds. This time period is issued to the Registrar server. The Registrar server normally accepts this time period, but may also change the time period. The Registrar tells the Business Mobility IP DECT system the stored time period (in the "ACK" message). When the time expires, the registration is removed from the Registrar. However, the Business Mobility IP DECT system knows when the timer expires and will execute a register again.

An IP DECT handset registers its number:

- ☐ At subscription
- ☐ When the DAP holding the subscription record of an extension (UA) starts up
- ☐ With an interval of 1 up to 25 minutes (depending on the number of subscriptions in the DAP).

 *It is not always necessary to do a registration to a Registrar service. Depending on the SIP servers configuration and the SIP Proxy type, registration can be done implicitly via a call setup (INVITE) request from the UA to the SIP Proxy. In that case no Registrar server is used and no registration expiry timer is used.*

 *The registration takes place between the DAP where the subscription record of the handset resides and the SIP Registrar. So, the handset does not have an IP address and the handset does not contact the SIP Registrar directly.*

SECTION 5 **HANDOVER MECHANISM**

The handover mechanism ensures seamless handover from one DAP to the other DAP in a multi DAP (radio) environment. So in other words, when a handset is in an existing voice call, it can move between the DAPs without losing the connection or hearing a click.

In [Figure 4-4 Call Connection Before Handover](#), a call is depicted between a SIP IP telephone and a DECT handset with extension number 200. The speech path is a peer-to-peer VoIP connection between the SIP IP extension and a DAP.

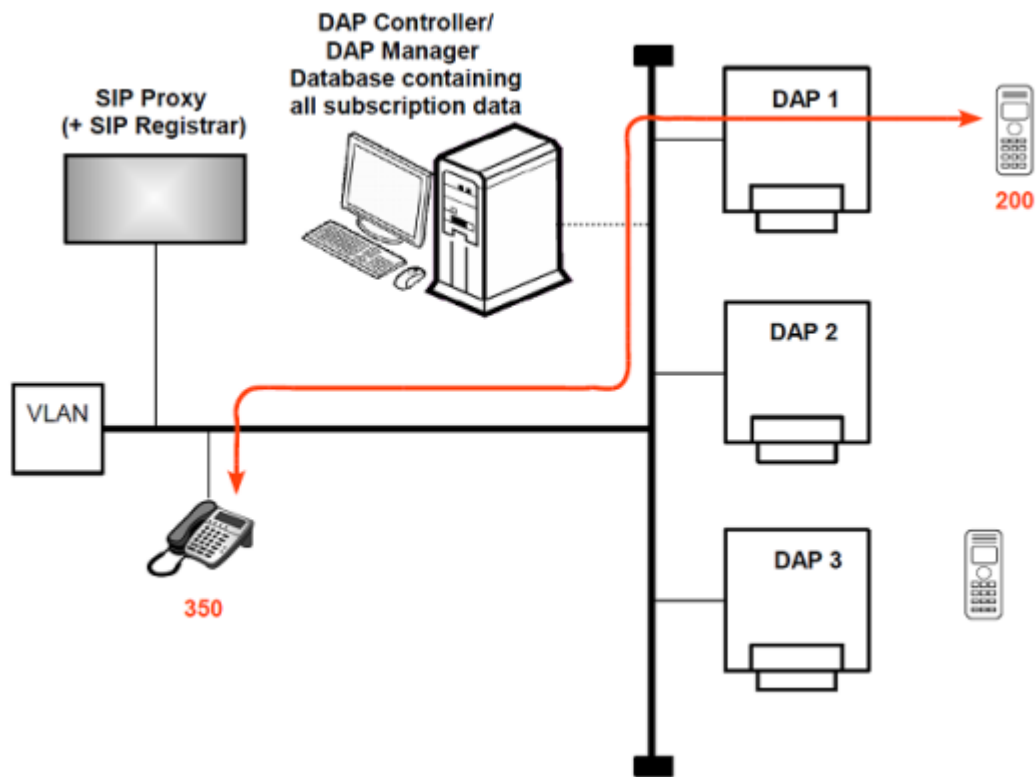


Figure 4-4 Call Connection Before Handover

However, handset 200 moves from one DAP to another DAP. See [Figure 4-5 Handover Action Started](#). The handset searches for a better radio signal, and detects that the second DAP has a better signal. The handset issues a request for handover to the new DAP. However, the new DAP does not know where the existing voice connection to handset 200 resides so it issues a multicast request for searching previous connection to handset 200 over the network with DAPs. The original/first DAP responds to this request because the call was initially be set up via this DAP.

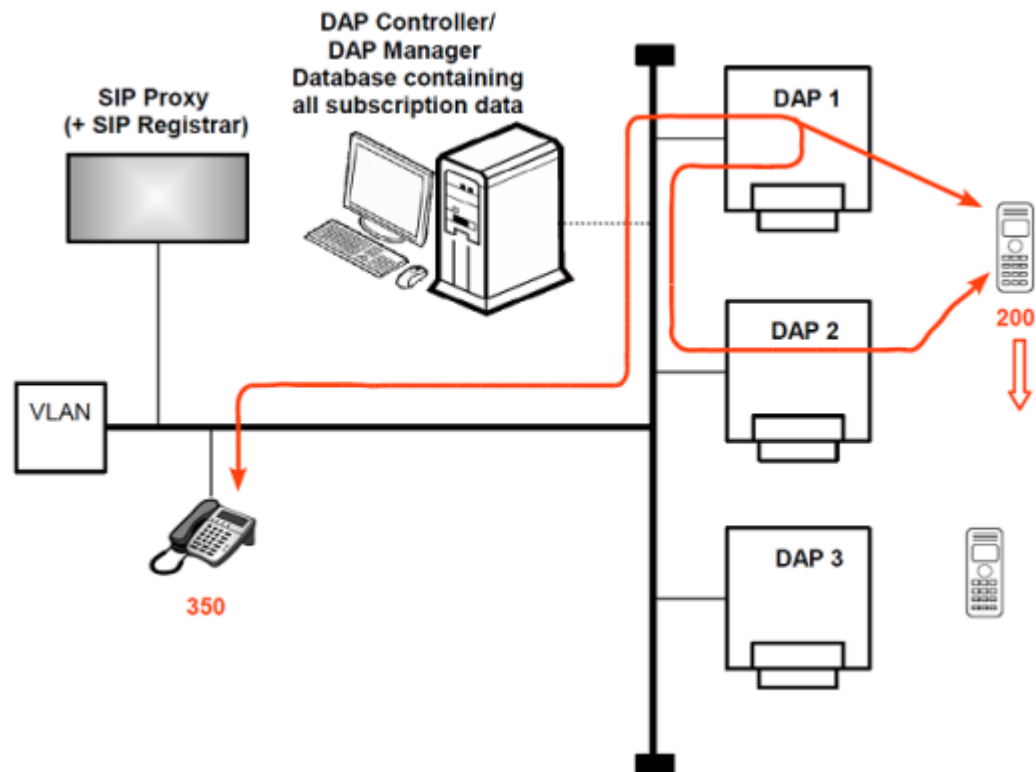


Figure 4-5 Handover Action Started

Now the connection is copied from the original/first DAP to the second/new DAP. See [Figure 4-6 Handover Taken Place, New Connection Active](#). The original/first DAP will release the radio connection to the handset and the new connection remains in place. Note that the original connection is not removed from the original DAP, but this DAP "relays" the connection to the second DAP. The original DAP cannot release the IP voice connection, because the IP voice connection between the SIP IP extension and the DAP 4 is established, based on a combination of sockets. This combination is fixed during the connection.

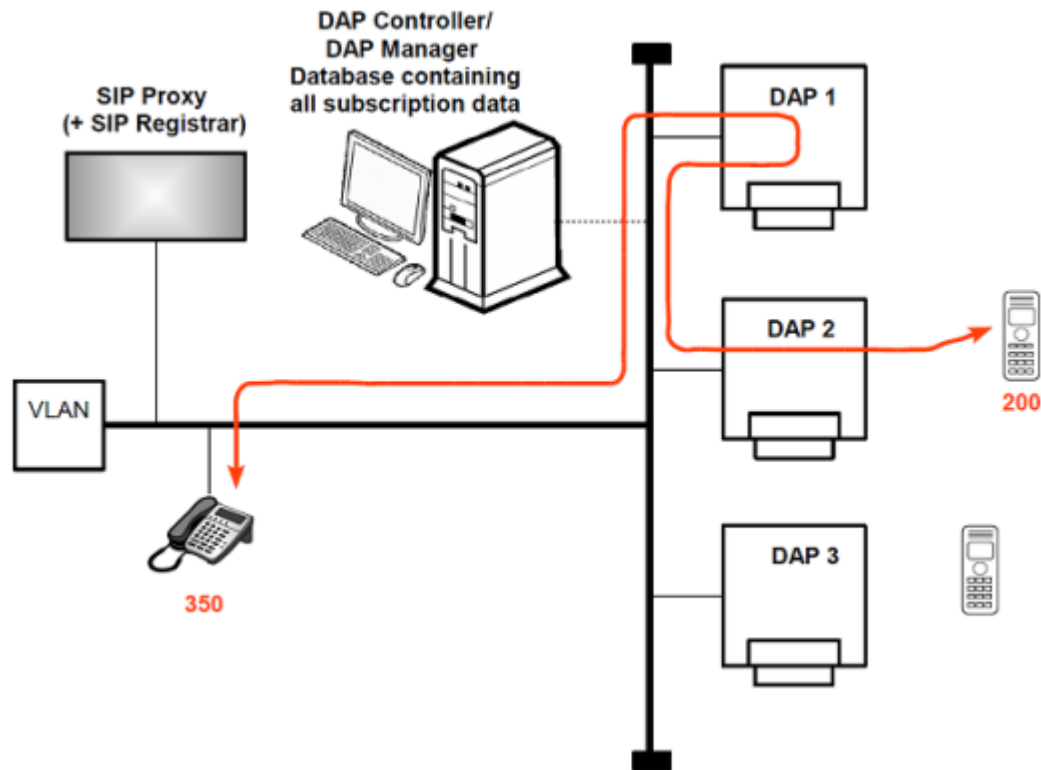


Figure 4-6 Handover Taken Place, New Connection Active

When a second handover takes place from DAP 2 to DAP 3, DAP 1 will setup a second relay to DAP 3 and REMOVE the relay to DAP 2. So the maximum number of relayed RTP streams per call in the network is 1.

SECTION 6 IS DAP MANAGER REQUIRED?

The DAP Manager is not required for call handling. A simple Business Mobility IP DECT system will therefore look like [Figure 4-7 Simple Business Mobility IP DECT configuration without DAP Manager](#).

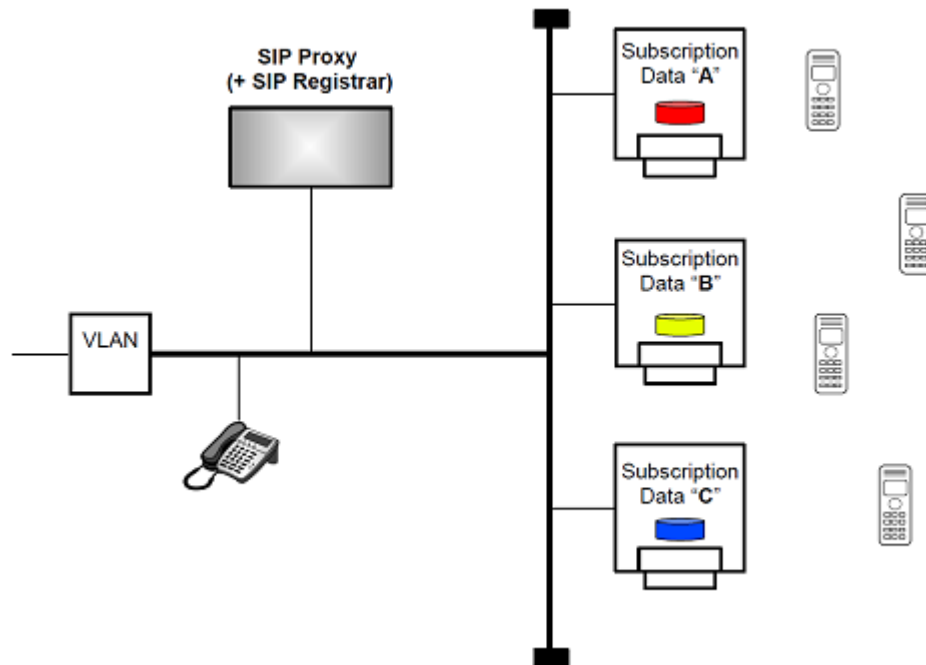



Figure 4-7 Simple Business Mobility IP DECT configuration without DAP Manager

The subscription data is stored in the DAPs.

The DAP Manager is temporary needed in the following cases:

- ☐ **During installation** - During installation the DAP Manager is needed to enter licence information, extension numbers, to subscribe handsets etc.
- ☐ **Management** - For any system management action the DAP Manager is needed
- ☐ **Replacing a DAP** - When you replace a DAP be aware that it may contain subscription data. Therefore, you need to open the DAP Manager WEB interface and execute a delete DAP. Then the subscription data that was in this DAP is put into the remaining DAPs. If you put a new DAP in place, initially it will not contain subscription data. Only after executing a subscription procedure, it may contain subscription data.

 *Be aware of the fact that in a number of system configurations, the DAP Manager is always needed.*

In the following cases, the DAP Manager is always needed:

- ☐ **Branch office configuration** - If your Business Mobility IP DECT system comprises a Main site and one or more branch offices over a router using unicast, these DECT islands require the DAP Manager for automatically moving subscription data when a handset moves from one island to another (island = main site or (one of) the branch office(s)). The DAP Manager is not necessary for call handling.

Also the DAP Manager is needed for backup of subscription data. If there are branch offices in the DAP Controller configuration, the subscription records are stored in RAM in the DAPs. If a DAP goes down and starts up again, the DAP will get the subscription data from the DAP Manager! If there are NO Branch office DAPs the subscription data is stored in FEPRAM in the DAPs. In that case, the DAP Manager is not needed as subscription database.

- ☐ **Low Rate Messaging Service (DECT Messaging)** - DECT Messaging always require the DAP Manager.
- ☐ **Sending alarm e-mails or sending SNMP traps** - The DAP Controller is capable of sending an e-mail when a DAP goes down, or a predefined threshold of channel occupation is exceeded or when the DDS service in the DAP Controller goes down. Also it can send an SNMP trap in case of one of these events (for more info, consult the Advanced Data manual).
- ☐ **Collecting diagnostic data** - The DAP Controller can collect detailed diagnostic and performance data. This automatically enabled when the DAP Controller is up and running.

SECTION 7 RADIO SYNCHRONIZATION

7.1 How it Works

The radio network structure supports seamless handover of existing calls. This means that when there is a call, and the handset moves from one radio to another, that other radio should take over the call. The call may not be interrupted and the user may not hear any click or what so ever. If the handset needs to re-synchronize to the other radio, then the user will hear at least a click. So, supporting handover requires an accurate synchronization of the radio signals in the air. How is this achieved?

Synchronization cannot take place via the cabling structure, because Ethernet does not allow transport of synchronous data, or in other words, the timing of data sent via Ethernet is not accurate enough. Therefore synchronization must go via the air.

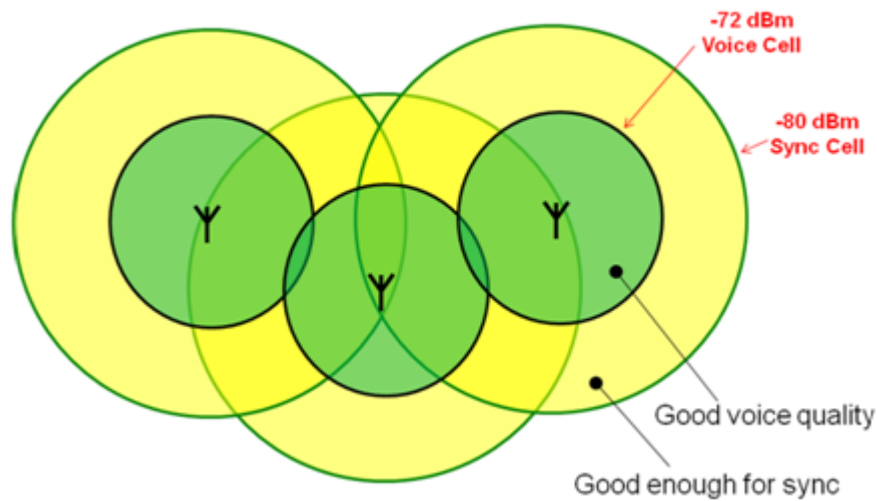


Figure 4-8 Radio Synchronization

A DAP (Radio) cell can be seen theoretically as a circle around the DAP. In [Figure 4-8 Radio Synchronization](#), you see two circles around the DAP: one in which you have sufficient radio signal strength for a good voice quality, and another (wider) circle with sufficient signal strength for synchronization. Due to the cellular structure of a DECT Radio Network, there must always be overlap in the cells with sufficient voice quality. The wider cell limit around the DAP will therefore have quite some overlap with the other cell, and will reach to the radio of the other cell. This means that the DAPs of the overlapping cells receive (weak) radio signals of each other. However these radio signals are still strong enough for synchronization purposes.

The receiving DAP checks the radio signals on PARI, to make sure that it belongs to the same DECT system. If they belong to the same DECT system, the DAPs will synchronize with each other according to predefined rules.

The DAPs are always transmitting via a minimum of two bearers. If there are no voice calls via a DAP, the DAP will transmit two dummy bearers. If there is one or more voice calls via the DAP, there will be one dummy bearer plus the voice call(s).

7.2 Synchronization Hierarchy

When DAPs try to synchronize to each other, there must be a hierarchy structure. One or more DAPs must be assigned as synchronization source. The system arranges this itself, and under normal conditions you don't need to do anything. However, if you have a complex DAP cell structure, manual intervention might be needed.

When a DAP is started up, it will try to synchronize to a DAP in the environment. Each DAP has its own unique identifier, the RPN (Radio Part Number). The RPN is a hexadecimal two digit number. A DAP will always try to synchronize to a DAP that has a **lower** RPN.

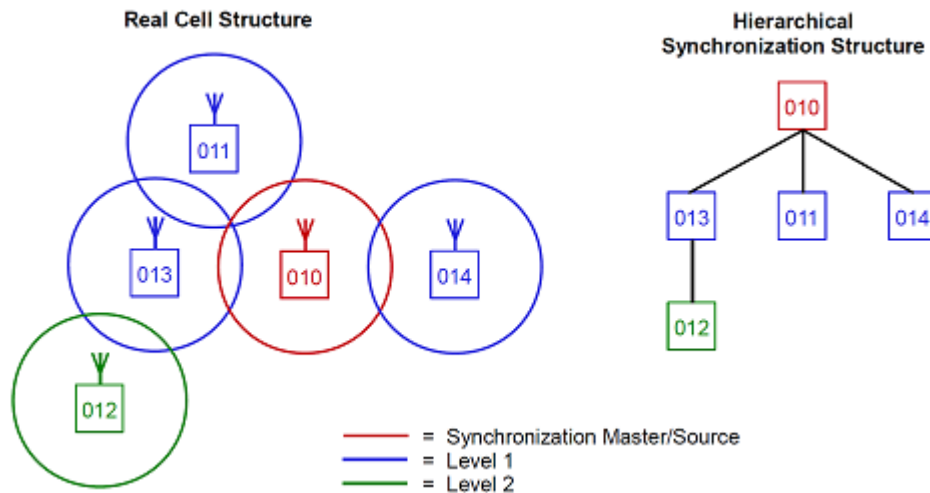


Figure 4-9 Synchronization Structure

In [Figure 4-9 Synchronization Structure](#), you see an example of a simple DAP structure. When the system starts up, the DAPs try to synchronize to the DAP with the lowest RPN. For DAP 010 it means that it will become the synchronization source! The DAPs with RPNs 011, 013 and 014 will synchronize to RPN 010. However, RPN 012 will synchronize to RPN 013 although RPN 013 is a higher number. Finding a synchronization source is not limited to one level deep only. DAP 012 knows that DAP 013 is synchronized to a DAP (010) that has a lower number than itself. Therefore DAP 012 will synchronize to DAP 013, because it is aware that DAP 013 gets its source from a DAP with a lower number.

If a DAP "sees" more than one other DAPs, the DAP will synchronize to the DAP that has the shortest path to the synchronization master. If the path to the master is the same number of hops for more DAPs, the DAP will synchronize to the DAP with the lowest RPN.

It is possible that there are more than one "synchronization islands" in the system. In that case, each synchronization island has its own synchronization master. The synchronization algorithm is applicable for each individual island.

The DAP Controller keeps track of the synchronization structure. Note that the RPN number that the DAPs have, are assigned once, when they start up after installation. The DAP that reports itself at first will get the lowest number, which means that it will become the source for providing the synchronization to the DAP network structure.

If you want to make a DAP a synchronization master, or give a DAP a higher position in the synchronization structure, you can assign a lower RPN number to a DAP manually. RPNs can be assigned manually via the DECT Manager WEB interface.

The automatically assigned RPNs start at:

010

The automatic assignment of RPNs starts at 010 when the IP DECT system is setup as Distributed DAP Controller.

Manually assigned numbers can be in the range 000 . . . 00F.

After the numbers are assigned at the first time start up, these numbers are stored in a file in the DAP Manager and will not change anymore, even after system start-up.

7.3 Coverage and Signal Strength Calculation

Synchronization between DAPs requires sufficient radio signal strength between DAPs. The following items are relevant for the signal strength for synchronization.

- To achieve a good voice quality, the minimum signal strength at the receiver in the handset and DAP, must be -72 dBm. (This includes a margin of -10 dBm for fast fading -dips.)
- Synchronization is possible if the strength of the received signal from another DAP is -80 dBm ... -85 dBm (this is adjustable).
- In open area, the distance is doubled if the received signal strength is 6 dB lower. This means that at a minimum signal strength for good voice quality of -72 dBm and a distance "X", the signal strength at the double distance (2X) is -78 dBm. See [Figure 4-10 Signal Strength Considerations](#).
- In open area there is more than sufficient signal strength for synchronization. The expected level at the double distance is -78 dBm. The required level is -80 dBm ... -85 dBm. This leaves a safely margin of 2 ... 7 dB.
- In practice there can be and will be objects in between the DAPs which may introduce some loss. However, there are also (many) objects that causes reflections, which means that the signal will reach the DAP via other paths as well with sufficient signal strength. Real life installations have proven this theory.
- The error rate in the received frames can be much higher than for speech. (50% frame loss is still acceptable).

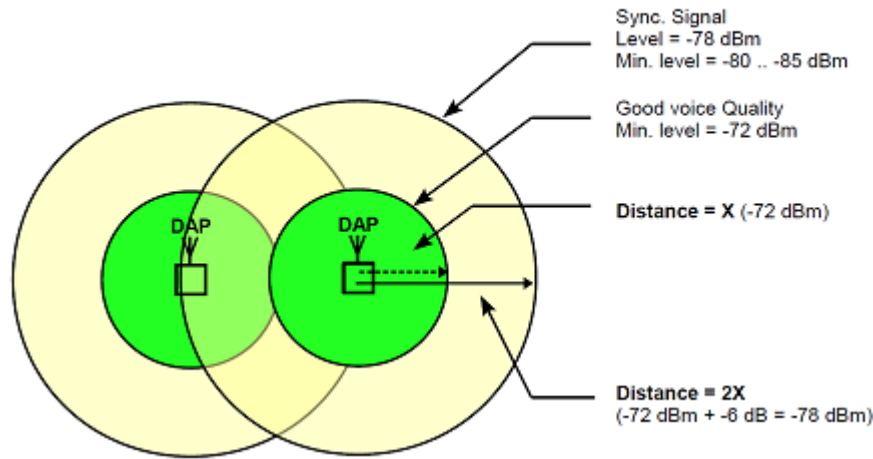


Figure 4-10 Signal Strength Considerations

Practice has indicated that coverage measurements for traditional DECT can also be applied for Business Mobility IP DECT.

SECTION 8 IP PORT NUMBER ASSIGNMENTS

IP Port Numbers are assigned for a speech connection. They are assigned per session, and then released again.

In the DAP Controller, there is a predefined "pool" of IP port numbers. This is specified in file `dapcfg.txt`. You can access the data in this file using the DAP Configurator tool (see chapter 8 "CONFIGURATION - DAP CONFIGURATOR TOOL") and adapt the port number range to your wishes.

SECTION 9 DAP CHARACTERISTICS

9.1 General

The following DAP types exist:


- AP200 Series, till November 2010
- AP300 Series, from November 2010 till June 2012
- AP400 Series, current AP400 version (from June 2012 onwards)

All of these DAPs share common characteristics. These characteristics are described in section [9.2 Common Characteristics](#).

Type dependant characteristics are given in the following subsections.

9.2 Common Characteristics

○ Features

 *The following list contains features that are only supported if the PBX supports it at well.*

- ☐ DECT GAP and CAP compatible.
- ☐ DECT Seamless handover.
- ☐ DECT Low Rate Messaging Service (LRMS) (Max. number of characters depends on the type of handset used.)
- ☐ CLIP and Name Display.
- ☐ Enquiry
- ☐ Call Progress tones.
- ☐ DTMF tones.
- ☐ Message Waiting indication.
- ☐ DAP Software downloadable

○ Capacity

- ☐ Maximum number of simultaneous calls: 12
Please note that this maximum number of calls is only applicable when the DAP is synchronization source/master. If the DAP is not the synchronization master, the maximum number of simultaneous calls is 11. Also note that the maximum number of simultaneous calls per DAP is also limited by licenses in a licensed version of IP DECT.
- ☐ Maximum number of simultaneous relay calls: 12
- ☐ Maximum number of DAPs per network: 256
- ☐ Maximum number of DAPs with DAPs in Branch Offices: 750
- ☐ Maximum number of simultaneous calls per network with 256 DAPs: $11 \times 255 + 12 = 2817$. This depends on the network configuration and available DAP channels.

○ IP Interface Characteristics

- ☐ 100 Base-T Full duplex, full support of auto-negotiation in Ethernet Switch

Maximum cable length according to the IEE802.3 specification (100 meters).

- ☐ Audio Coding: G711
- ☐ DTMF generation: H.245
- ☐ Call control protocol: Proprietary.
- ☐ IP protocols: DHCP and TFTP

○ **Environmental Conditions**

- ☐ Storage temperature range: -25° to +55° Celsius
- ☐ Operational temperature: 0° to +40° Celsius
 - ✎ The operational temperature range is 0° to 40° Celsius. When you use a DAP outdoor, there is an outdoor box available that will enlarge the temperature range. Please contact your supplier for more information.

9.3 AP200 Characteristics (not available anymore)

The AP200 is the General release of the DAP for the Radio Traffic. It complies with all characteristics mentioned in section 2.9.2 "Common Characteristics". In addition to that it supports G.729 (G.729AB).

9.4 AP200S (not available anymore)

The AP200S complies with the common characteristics as given in [9.2 Common Characteristics](#). The AP200S does not support G.729.

The AP200S must be used with the associated DAP Controller software Release 4 for AP200S or with DAP Controller Release 5.

9.5 AP200E (not available anymore)

The AP200E is the same as the AP200 but allows you to connect external antennas. When used in an AP200S configuration it behaves as if it is an AP200S.

9.6 AP300

The AP300 is described in the AP300 Customer Engineer Manual. Please consult the AP300 Installation Manual for more information:

- ✎ *The AP300 and AP300E can be mixed with the AP200 and AP200S in the same system. However, make sure that either all DAPs in the same system do support G.729 or all DAPs do not support G.729. A mix is not allowed.*

9.7 AP300E

The AP300E is the same as the AP300 but allows you to connect external antenna's. When used in an AP200S configuration it does not support G.729.

9.8 AP400

This is the generic AP400, NEC branded.

9.9 AP400G

This is the generic AP400, un-branded.

9.10 AP400E

The AP400E is equipped with connectors to connect External Antennas.

9.11 AP400C

The AP400C is used for IP DECT with PBX type: IPC100/IPC500, SV8100, SL1000/1100

9.12 AP400S

Maximum of 4x AP400S in one system with PBX type: IPC100/IPC500, SV8100, SL1000/1100 PBXs

SECTION 10 AP200/AP200S POWER PROVISION

An AP200 can be powered on two different ways:

- ☐ **Line powering** - The AP200/AP200S supports Line powering according to specification IEEE802.3af. It supports both versions: "phantom power" as well as "power over spare wires". The voltage at the patch panel should be between 42 Volts and 60 Volts. Note that the distance depends on the cable type and the voltage at the patch panel.

- ☐ **External Power Supply** - External Power supply connected to the Power Connector on the AP200. This power supply should meet the following requirements:
 - AC/AC Power adapter
 - Secondary voltage: 40 V AC, +10%/-10%
 - Maximum power consumption: 10 Watts

SECTION 11 **AP300/AP400 POWER PROVISION**

The AP300/AP400 is powered via PoE. It supports Class detection. The AP300/AP400 is a Class 2 device when used on PoE Switches. For more information consult the AP300/AP400 Installation Manual.

SECTION 12 **MORE THAN 256 DAPS**

IP DECT allows you to setup an IP DECT System with more than 256 DAPs. There are two possibilities.

- ☐ **System with Branch offices** - Maximum number of DAPs per IP DECT system with Branch Offices is 750. Per Main site or Branch Office, the maximum number of DAPs is 256.

This configuration can be setup with the standard IP DECT installation. For more info, see [Section 13 RPN Number Ranges per Branch Office on page 4-20](#) and [Section 5 System Configuration on page 11-17](#).

- ☐ **One IP DECT Cluster with seamless handover** - Maximum number of DAPs per IP DECT System is 750, all on one location (Main Site). Please note that this type of system is possible on "project" base and is not part of the standard installation. For more information, please contact your IP DECT supplier.

SECTION 13 **RPN NUMBER RANGES PER BRANCH OFFICE**

You can specify the range of RPN numbers that you want to use in the Head Quarter and in the individual Branch Offices. That allows you to use up to 750 DAPs in one IP DECT installation. Per Branch Office, the maximum number of DAPs is 256. Also in the Head Quarter, the maximum number of DAPs may not exceed 256.

The Branch office DAPs are not allowed to "see" DAPs of other Branch Offices or the Head Quarter.

Because the RPN number range is related to the Head Quarter or to Branch Offices, the RPN number range is related to an IP network segment.

The DAP Configurator lets you set up the configuration in a very simple way, by means of assigning RPN numbers to a Branch Office.

The RPN numbers in the DAP Manager exist of three digits instead of two. The RPN number that is displayed in the handset (in special mode) consists of the two least significant digits of the RPN number in the DAP Manager.

The configuration is stored in a file: **bo_adm.txt**.

THIS PAGE INTENTIONALLY LEFT BLANK

Licenses

SECTION 1 GENERAL

From IP DECT Release 6.0 onwards, licenses are introduced. All licenses has to be entered into the DAP Controller.

SECTION 2 FUNCTIONAL LICENSES

The following functional Licenses are available:

- ☐ **Maximum number of DAPs** - You must have a license for the number of DAPs. Please note that the total number of DAPs that you specify in this license, is the sum of license unities of 10 and 50 licences. E.g. when you have 70 DAPs, you need one license for 50 DAPs and 2 licenses for 10 DAPs. $(1 \times 50) + (2 \times 10)$. The maximum number of DAPs in a certain configuration is determined by the DAP types. This can be:
 - ☐ 4 - in case of the AP400S system
 - ☐ 256 - in case of the AP400C and AP400E
 - ☐ 750 - in case of the AP400, AP400G and the AP400E
- ☐ **For Future use: CAT-iq Data Licenses** - Please note that this license is not yet available and is planned for future use.
- ☐ **Redundancy Central Site** - This license is required to have a redundant DAP Controller configuration in the Central site.
- ☐ **Branch Office Survivability** - You need this license to allow Local DAP Controllers in one or more Branch Office locations.
- ☐ **Software Upgrade Allowance** - To upgrade a Release 6.0 to a higher version, you need an Upgrade License. When the license is activated, it provides a window of one month to install a higher version.

Please note that this license is made dependant on the system size. The steps are:

- 10 DAPs
- 50 DAPs
- 100 DAPs
- 256 DAPs

Please note that the total number of DAPs is the sum of the licences. E.g. when you have 70 DAPs, you need one license for 50 DAPs and 2 licenses for 10 DAPs. (1x50) + (2x10).

- ☐ **Messaging License** - Messaging is licensed in the DMLS and in the DAP Controller. Licenses are exchangeable between the DMLS and the DAP Controller, so if you have a licence for DMLS, you can import that license into the DAP Controller and vice versa. In the DAP Controller, the license is related to the number of DAPs in the system and should be the same number as specified in the first item in this list of licenses. For more info on the Messaging License, consult Section3.6 DMLS Licenses.
- ☐ **Location Detection License, on top of the Messaging License** - This license is available on the DMLS and also in the DAP Controller. Licenses are exchangeable between the DMLS and the DAP Controller, so if you have a licence for DMLS Location Detection, you can import that license into the DAP Controller and vice versa. The Location detection license is applicable for single point and multipoint on the DMLS. When you order the license, you must order it on top of the Messaging License. In the DAP Controller, the license is related to the number of DAPs in the system and should be the same number as specified in the first item in this list of licenses.

SECTION 3 PROJECT BASED LICENSES

There are a number of licenses that are only available on project base. Special support is required.

- ☐ **Large Configuration License - Big Projects License:** This license is required when your IP DECT system consists of more than 256 DAPs in one cluster with seamless handover. This license requires a RAP (Risk Assessment Procedure) and includes on-site support.
- ☐ **Dual Band Mode - Cruise Line License:** This is a special license for IP DECT installations on cruise ships. This license requires a RAP (Risk Assessment Procedure) and includes on-site support.

- ☐ **Reflection Cancelling:** This is a special license for IP DECT in environments with a lot of reflections. This license requires a RAP (Risk Assessment Procedure) and includes on-site support.
- ☐ **ATEX (IECEx) License:** This is a special license for the use of "intrinsic safe handsets" in environments with a higher explosion risk.
 - ATEX = ATmospheres EXplosibles
 - IECEx = International Electrotechnical Commission Explosive

SECTION 4 **SYSTEM ASSURANCE LICENSE**

The system assurance license is a license to allow software upgrading from Release 6.0 to higher versions. The license is based on the number of DAPs. The license is already mentioned in [Section 2 Functional Licenses](#).

Note that there are two ways to get the Software Upgrade License:

- ☐ By means of the NEC ordering tool
- ☐ By means of becoming a member of the System Assurance Program

When the license is activated, it provides a window of one month to install a higher version.

SECTION 5 **FROM RELEASE 5 TO RELEASE 6**

IP DECT Release 5 was license free, in IP DECT Release 6.0 and higher you need license for the various functions and features.

When you upgrade from Release 5 to Release 6, the system will automatically generate a license file with all the features that your system had in Release 5. So, you do not need to have a license prior to upgrading.

This license has the following characteristics:

- ☐ It will cover all existing system configuration
- ☐ It is Free of Charge

You must send the license file that is generated to NEC for registration. For new features, you must order a new license.

SECTION 6 DMLS LICENSES

From Release 6 onwards, the DMLS is licensed in the DAP Controller License mechanism. You don't need a dedicated license for the DMLS anymore. The license is based on the number of DAPs.

In the DAP Controller, there is a license for "DECT Messaging" and for "DECT Location detection". The Location Detection license is on top of the Messaging License.

There are two options to enable the DMLS Messaging/Location feature:

- ☐ **DMLS License String** - When you already have a DMLS license string, you can use that license in the DMLS and you can import that license string into the DAP Controller License mechanism by means of the button "Add DMLS". (See section 9.13.3 License Information Window.). Please note that this is applicable for the Messaging license as well as for the Location license.
- ☐ **DAP Controller License for Messaging and perhaps also Location detection** - When you have a license for Messaging or Location detection on the DAP Controller, you can synchronize the DMLS application with it. The DMLS can retrieve the license data from the DAP Controller license mechanism by means of one button.

When you have a "CTI license" for Messaging on the DAP Controller, you do not need to have the Messaging license in the DAP Controller.

SECTION 7 WHERE TO ENTER AND WHERE TO FIND THE LICENSE DATA?

With version 6.0 DAP Controller software you must obtain a license from the License Manager Server (LMS). To do this you must create a DECT site to apply the version 6.0 licenses to using the PARI code from the IP DECT license CD as the hardware key code. The DECT license is not applied to the main SV8100 site, but is applied to the DECT site that you create.

The following steps are used to obtain this license.

1. Obtain PARI code from the IP DECT License CD.
2. Log into license manager.
3. Create a DECT site using the PARI Code from the IP DECT License CD as the hardware key code.
4. Apply DECT license from the Available Purchase Orders to the DECT system created in step 3.

5. Create license file and download to support PC.
6. Apply DECT license to DAP Controller following the steps in section [9.9 License Handling on page 11-42](#).

For more information, consult the applicable sections in the chapter that describes the DAP Configurator Settings:

- ☐ [9.9.1 Install a New License File on page 11-42](#)
- ☐ [9.9.2 Reading out the Licenses on page 11-43](#)
- ☐ [9.9.3 License Information Window on page 11-44](#)


THIS PAGE INTENTIONALLY LEFT BLANK

Network Configurations

SECTION 1 TYPICAL CONFIGURATIONS

From IP DECT Release 6.0 onwards, licenses are introduced. All licenses has to be entered into the DAP Controller.

The IP DECT system must be implemented in a company infrastructure. As mind setting tool, this chapter gives you four typical configurations with the advantages and disadvantages. All configurations are based on using one IP DECT system (DECT Cluster) in the network. You should consider which configuration you must implement at the customer site. In the IP DECT Advance Data Manual, you will find more information about the system behavior over a router, in chapter "System Behavior over Router".

 *All IP switches that are involved must support IP multicast, with "IGMP snooping" disabled.*

Furthermore, disable "Spanning Tree Protocol" on ports that are used for DAPs and set the switch ports to "fast forwarding".

SECTION 2 SIMPLE CONFIGURATION

2.1 Network Configuration

[Figure 6-1 Example of Simple IP DECT Network Configuration](#) shows an example of a simple configuration. All IP DECT devices are put in one subnet. This subnet is based on one or more IP switches. If the switches serve more than one VLAN, all IP DECT devices are put in one VLAN (therefore behaving as one subnet).

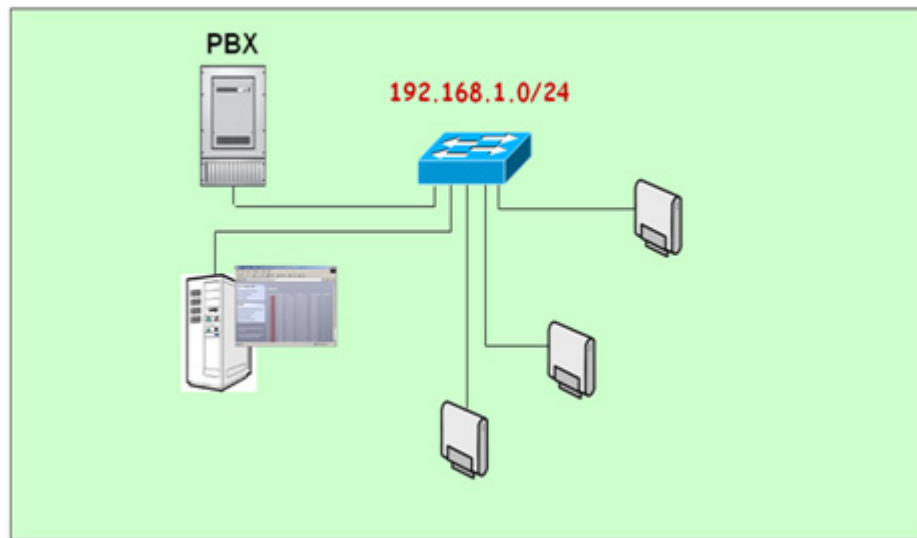


Figure 6-1 Example of Simple IP DECT Network Configuration

The general characteristics of a simple configuration are as follows:

- Seamless handover is supported between all DAPs.

2.2 Settings in DAP Configurator

The DAP Configurator is described in [Configuration - DAP Configurator Tool on page 10-1](#). However, in this section you will find an example of a setup for a simple configuration ([Figure 6-2 Setup for Simple Configuration Example](#)).

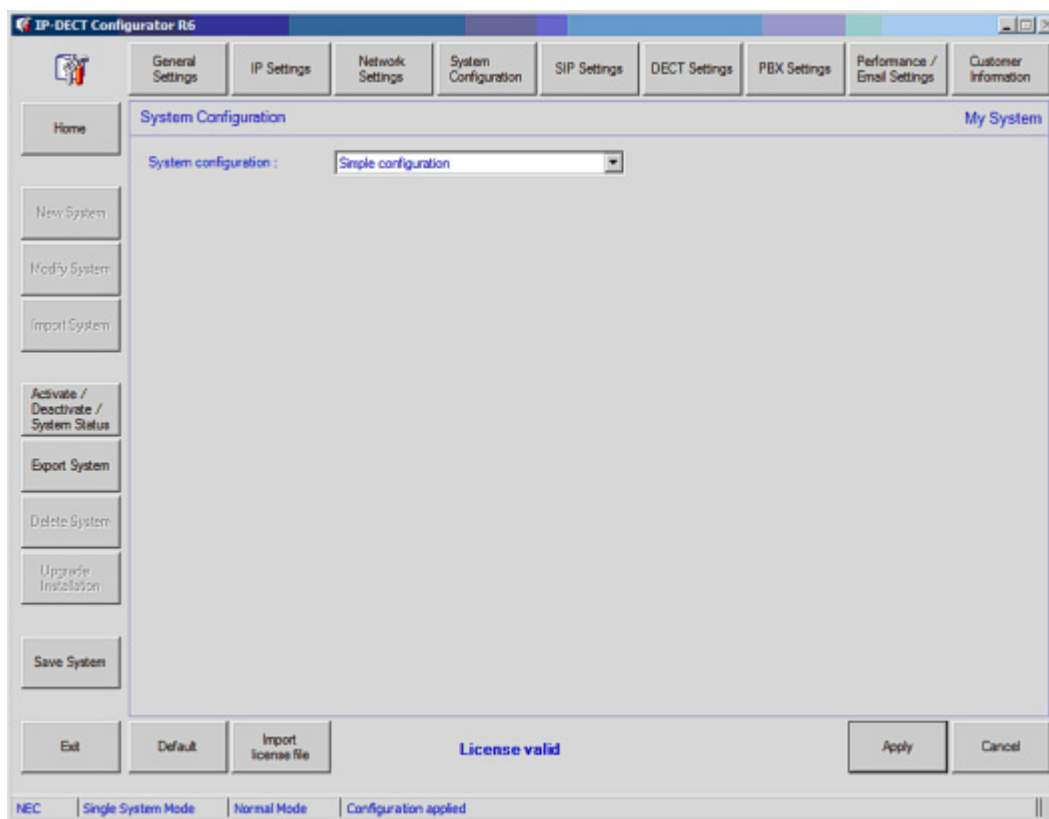


Figure 6-2 Setup for Simple Configuration Example

SECTION 3 BRANCH OFFICE SOLUTION

3.1 Network Configuration

Figure 6-3 Example of an IP DECT Configuration with a Branch Office shows an example of a Branch Office configuration with a main office (head quarter) and two Branch Offices. Main Office and Branch Offices are in different subnets connected via routers. Routers can be connected over the WAN.

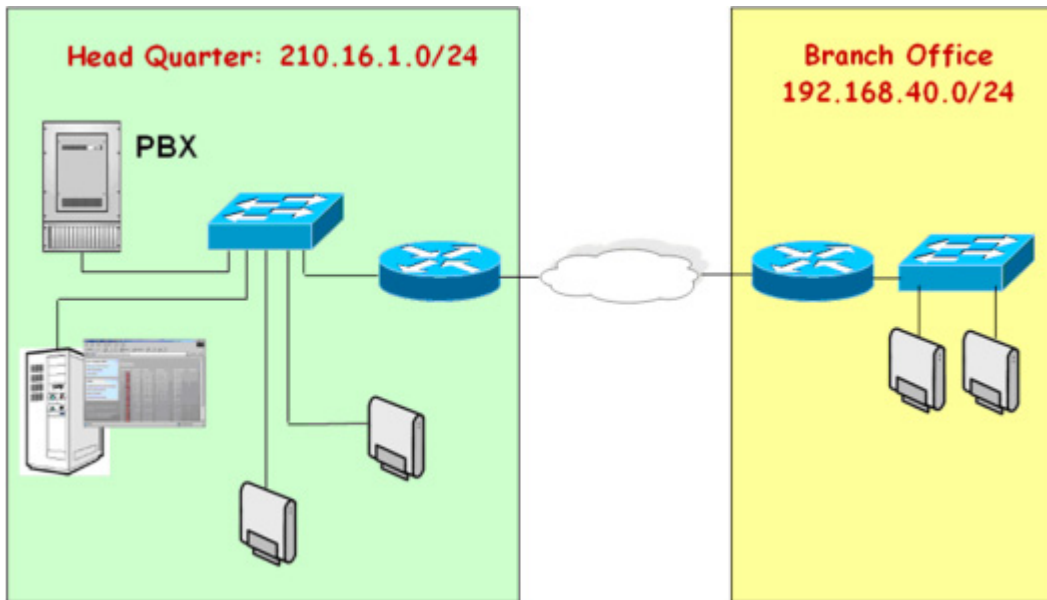


Figure 6-3 Example of an IP DECT Configuration with a Branch Office

The general characteristics of an IP DECT configuration with Branch Offices are as follows:

- Allows interconnections with limited bandwidth between Head Quarter and Branch office(s).
- Allows interconnections with poor QoS between Head Quarter and Branch office(s). (Radio Links, ADSL etc.)
- No PBX needed in Branch Office(!).
- Seamless handover is supported in Branch Offices and in Main Office.
- No handset handover between Head Quarters and (individual) Branch Offices.
- Head Quarter and individual Branch Offices must be in separate subnets (router(s) needed).
- No IP multicast support required for Routers.
- Multicast TTL = 1, which means that IP multicast packages does not cross a router.

3.2 Settings in DAP Configurator

The DAP Configurator is described in Chapter 8. CONFIGURATION - DAP CONFIGURATOR TOOL. However, in this section you will find an example of a setup for a Branch Office configuration, [Figure 6-4 Branch Office Configurator Example](#).

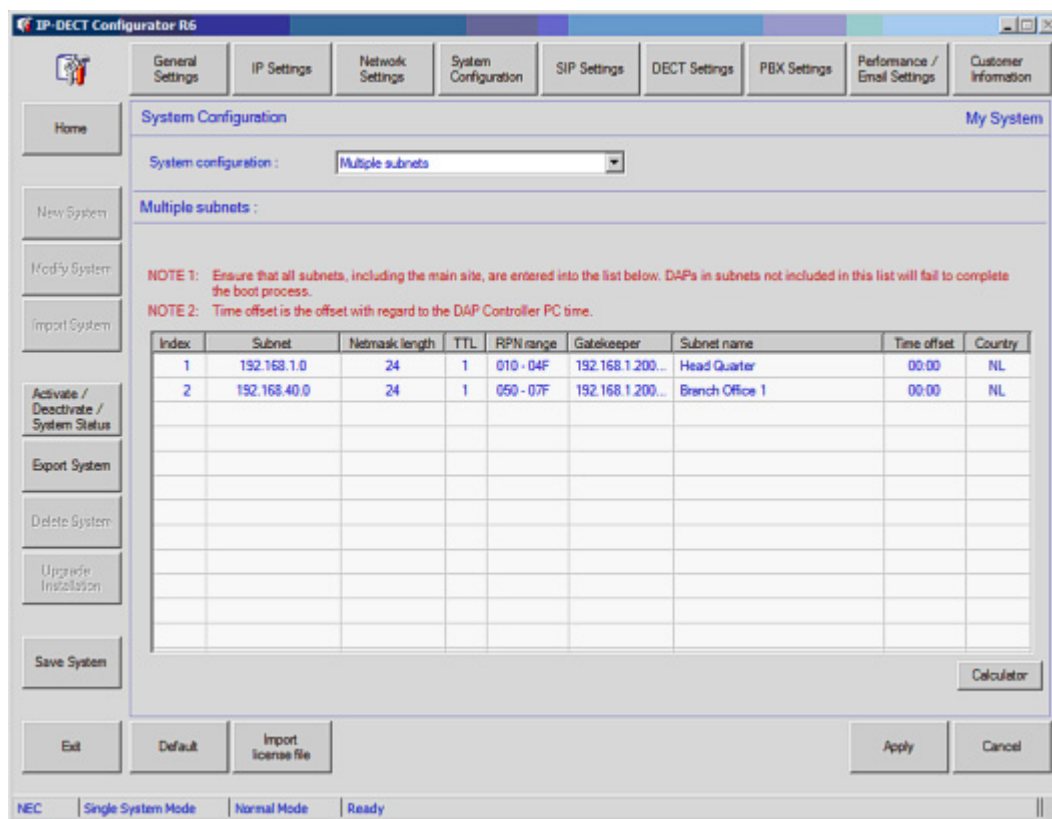


Figure 6-4 Branch Office Configurator Example

SECTION 4 ROUTED HEAD QUARTER

4.1 Network Configuration

Figure 6-5 Example of an IP DECT Routed Head Quarter Configuration shows an example of a Routed Head Quarter configuration with a head quarter and two subnets connected via one or more routers. The subnets in the network are part of one company network.

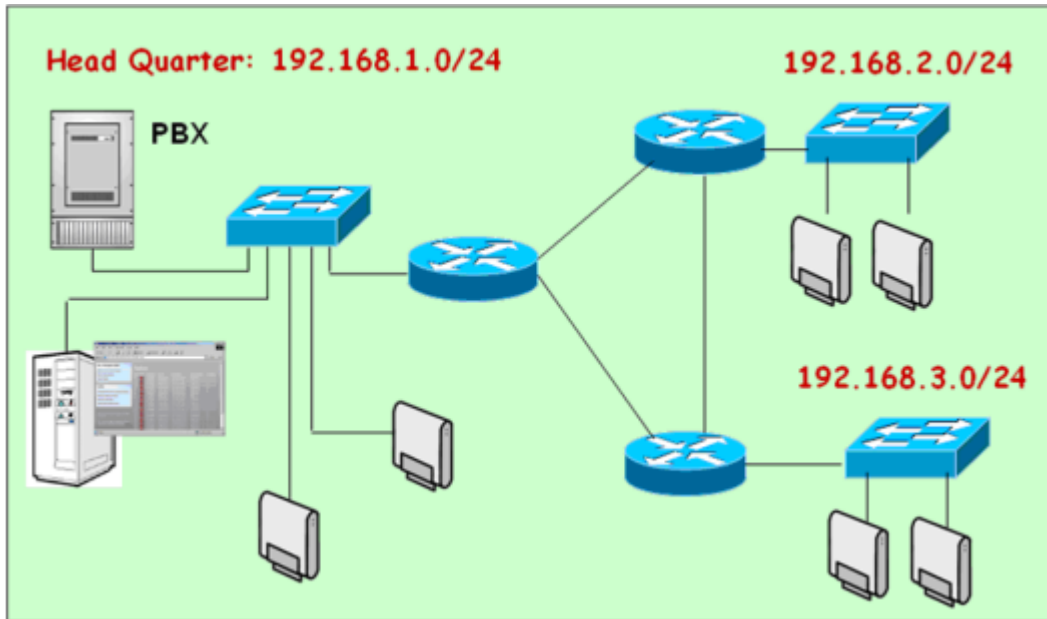


Figure 6-5 Example of an IP DECT Routed Head Quarter Configuration

The general characteristics of an IP DECT Routed Head Quarter configuration are as follows:

- Used for a Large Campus network that is split up into different (geographical) subnets.
- The network supports QoS and IP connectivity all over the Campus.
- IP DECT configuration behaves as one large IP DECT system.
- Full support of seamless handover between all DAPs in the IP DECT system.
- Routers must support IP Multicast routing.
- The IP Multicast address for IP DECT is the same in all segments.
- Multicast TTL > 1, which means that the routers pass on the IP multicast packages.
- In the IP DECT configuration, you must enter the subnet mask that is needed to cover all networks (e.g. 255.255.252.0) for up to four subnets as in the previous example.

4.2 Settings in DAP Configurator

The DAP Configurator is described in [Configuration - DAP Configurator Tool on page 10-1](#). However, in this section you will find an example of a setup for a Branch Office configuration, as seen in [Figure 6-6 Branch Office Configuration Example](#).

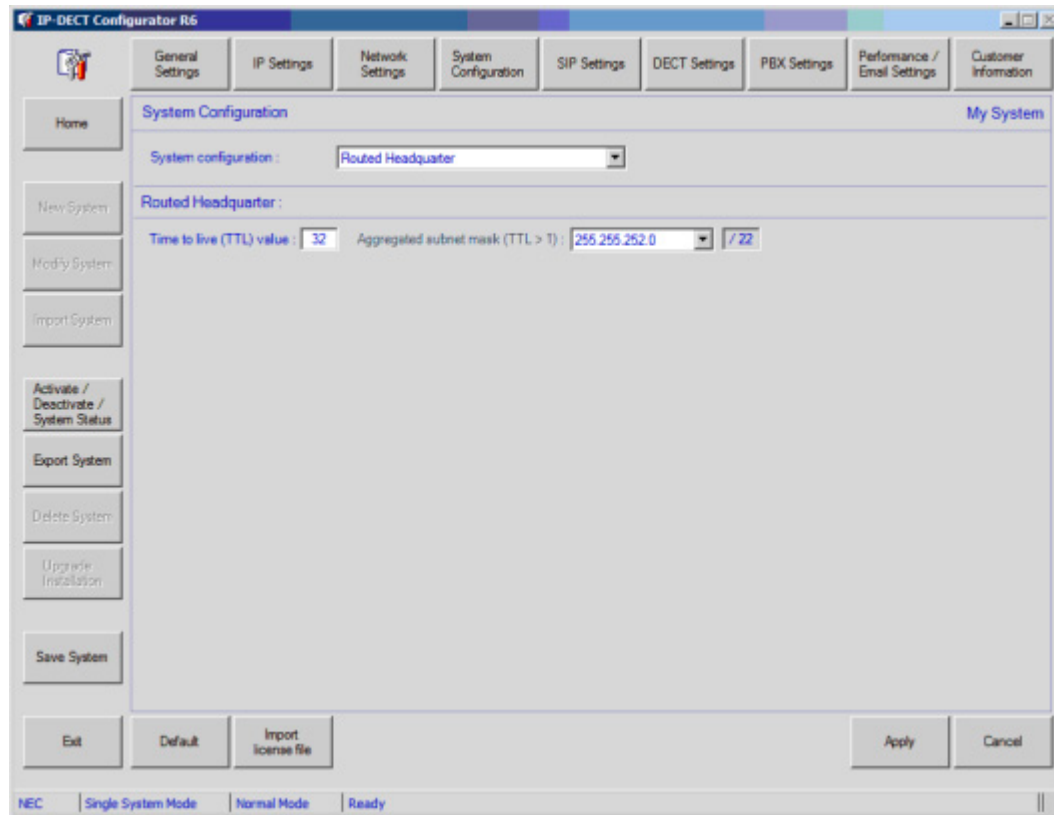


Figure 6-6 Branch Office Configuration Example

Please note that the TTL is the TTL value for IP Multicast, which must allow Multicast traffic over the Routers in the Routed Head Quarter. That should be higher than 1, but based on the TTL settings in the Router, it is advised to use a TTL value of 32.

Please note that the Aggregated subnet mask is the subnet mask that includes all three networks in the Head Quarter. So, this is NOT the IP subnet mask on the Network adaptors on the IP Network segments. Please do not mix up the Aggregated Subnet Mask and the normal IP Subnet mask.

SECTION 5 ROUTED HEAD QUARTER WITH BRANCH OFFICES

5.1 Network Configuration

Figure 6-7 Example of an IP DECT Routed Head Quarter Configuration with Branch Office shows an example of a Routed Head Quarter configuration with a head quarter, one subnet connected via one or more routers and a Branch Office. The subnets in the network are part of one company network, the Branch Office is connected over the WAN (or low throughput LAN).

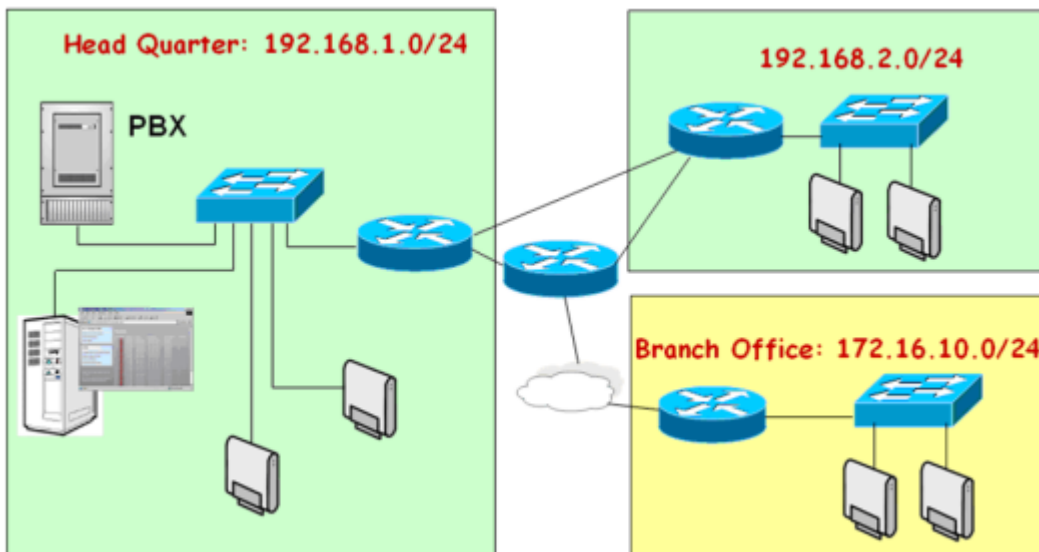


Figure 6-7 Example of an IP DECT Routed Head Quarter Configuration with Branch Office

The general characteristics of an IP DECT Routed Head Quarter configuration with Branch Office(s) are as follows:

- Hybrid of Routed Head Quarter and Branch Offices (see previous sections).
- Used for a Large Campus network that is split up into different (geographical) subnets in combination with (remote) Branch Offices.
- In the Routed Head Quarter part, all characteristics which are mentioned previously for the Routed Head Quarter are applicable.
- For the Branch Office, all characteristics which are mentioned in the section covering the Branch Offices are applicable.
- In the Head Quarter the Multicast TTL >1, in the branch Office the Multicast TTL =1(!).

- Edge Router, connected to the WAN, should not forward Multicast packages to the WAN.
- Full support of seamless handover between all DAPs in the Head Quarters configuration with the subnet.
- Routers in the Head Quarter must support IP Multicast routing.
- In the IP DECT configuration, you must define which subnets are in the Head Quarters and which subnet(s) is/are Branch Office subnets. You must do that by means of specifying the subnet mask that is needed to cover all Head Quarters subnetworks (e.g. 255.255.252.0 for in this example.).

5.2 Settings in the DAP Configurator

The DAP Configurator is described in [Configuration - DAP Configurator Tool on page 10-1](#). However, in this section you will find an example of a setup for a Routed Head Quarter with Branch Office configuration as seen in [Figure 6-8 Routed Head Quarter with Branch Office Configuration](#).

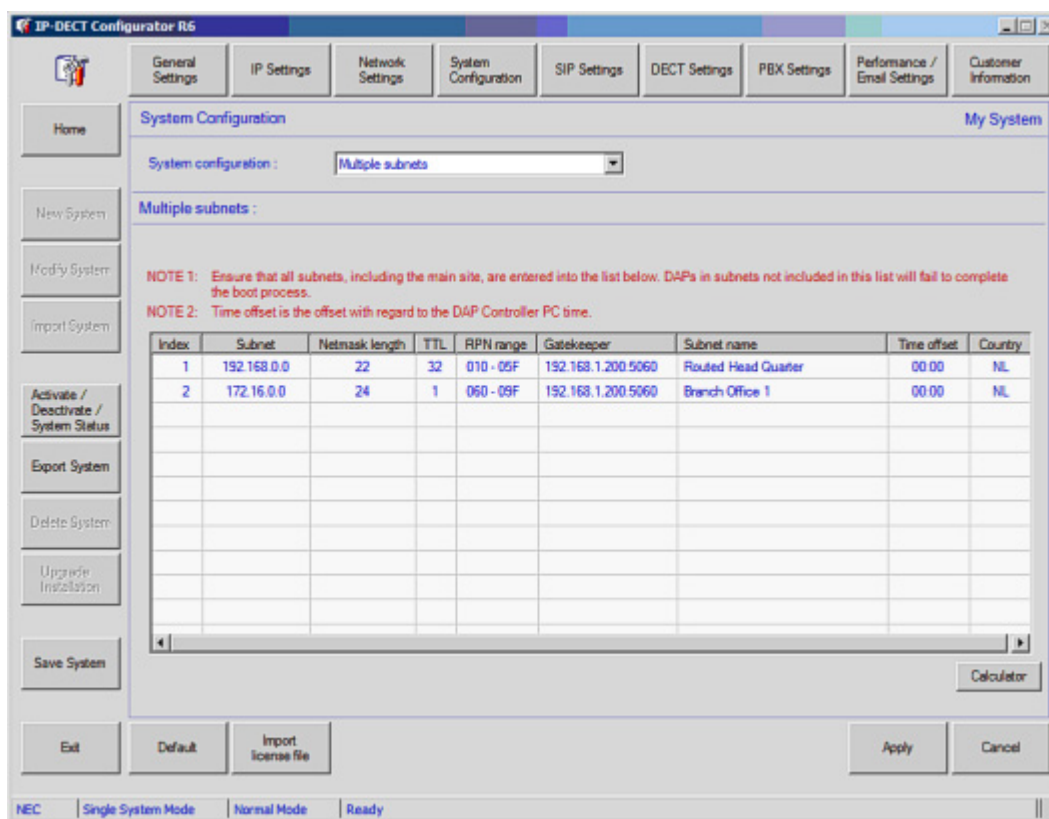


Figure 6-8 Routed Head Quarter with Branch Office Configuration

SECTION 6 ROUTED HEAD QUARTER WITH BRANCH OFFICES

6.1 Network Configuration

Figure 6-9 Example of an IP DECT Routed Head Quarter Configuration with a Routed Branch Office shows an example of a Routed Head Quarter configuration with a head quarter, one subnet connected via one or more routers and a Branch Office. The subnets in the network are part of one company network, the Branch Office is connected over the WAN (or low throughput LAN).

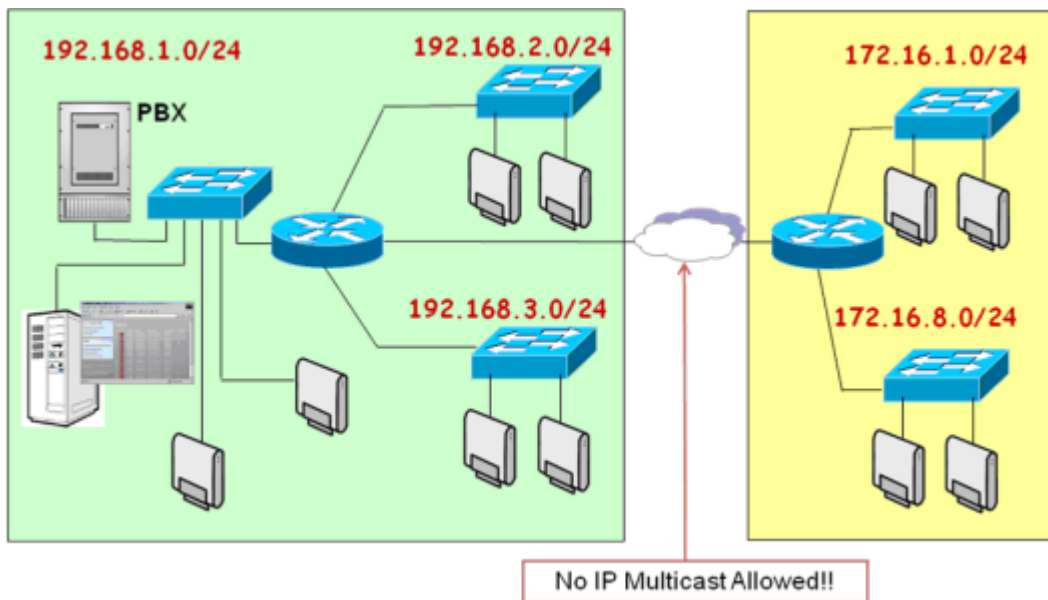


Figure 6-9 Example of an IP DECT Routed Head Quarter Configuration with a Routed Branch Office

The general characteristics of an IP DECT Routed Head Quarter configuration with Routed Branch office are as follows:

- Hybrid of Routed Head Quarter and Branch Offices (see previous sections).
- Used for a Large Campus network that is split up into different (geographical) subnets in combination with remote Routed Branch Offices.
- In the Routed Head Quarter part, all characteristics which are mentioned previously for the Routed Head Quarter are applicable.
- In the Routed Branch Office part, all characteristics which are mentioned previously for the Routed Head Quarter are applicable, except for that the Routed Branch Office must be in different subnets than the Routed Head Quarter.

- In the Head Quarter the Multicast TTL >1, and in the branch Office the Multicast TTL >1(!).
- Edge Router, connected to the WAN, should not forward Multicast packages to the WAN.
- The Routers between the Routed Head Quarter and the Routed Branch Office should block Multicast!
- Full support of seamless handover between all DAPs in the Head Quarters configuration with the subnet. Full support of hand over in the Routed Branch Office. No handover between the Routed Head Quarter and the Routed Branch Office.
- Routers in the Head Quarter must support IP Multicast routing.
- Routers in the Routed Branch Office should support IP Multicast Routing.
- In the IP DECT configuration, you must define which subnets are in the Head Quarters and which subnet(s) is/are Branch Office subnets. You must do that by means of specifying the Aggregated subnet mask that is needed to cover all Head Quarters subnetworks (e.g. 255.255.252.0 for in this example.). Also in the Routed Branch Office, you must calculate the Aggregated subnet mask that covers all subnets in the Routed Branch Office.

6.2 Settings in the DAP Configurator

The DAP Configurator is described in [Configuration - DAP Configurator Tool on page 10-1](#). However, in this section you will find an example of a setup for a Routed Head Quarter with Routed Branch Office configuration as seen in [Figure 6-10 Routed Head Quarter with Routed Branch Office Setup Configuration Example](#).



DAP Installation Items

SECTION 1 GENERAL

The DAPs should be installed on the positions which were determined in the Site Survey (also called Deployment). Besides that, the following should be respected:

- ☐ DAPs must be installed with the antennas in vertical position, because that is how the Site Survey is done (normally). (Radiation pattern differs between horizontal and vertical position.)
- ☐ Do not mount a DAP to a metal surface.
- ☐ Do not roll up remaining cabling behind a DAP.

SECTION 2 DAP POWER PROVISION

The DAPs support Power over Ethernet, the so called PoE (laid down in IEEE802.3af specification). The DAPs support both types of PoE: phantom power as well as power over spare wires.

The following overview gives the specifications of the PoE.

- ☐ Voltage at the DAP: minimum 36 Volts, maximum 57 Volts.
- ☐ Connector: Standard RJ45 connector, using the spare wires pins (wires). See [Figure 7-1 Layout Ethernet Connector RJ45 on the DAP](#).
- ☐ Maximum cable length: 100 meters.

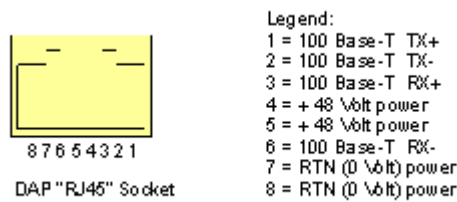


Figure 7-1 Layout Ethernet Connector RJ45 on the DAP

SECTION 3 DHCP AND TFTP REQUIREMENTS

The DAPs must get their IP addresses, configuration file and firmware from the IP network using a DHCP Server and a TFTP Server.

3.1 DHCP Server

When a DAP starts up, it tries to contact a DHCP server on the network. It should get the following items from the DHCP server:

1. IP Address
2. Subnet Mask
3. Default Gateway IP address
4. Next Boot Server IP address. This is the IP address of the TFTP Server (DHCP option 066)
5. Configuration file name (dapcfg.txt) available via the TFTP server (DHCP option 067)

Note that you must enable option 67 in the DHCP server whether you fill in a file name or not. If you do not fill in a file name, the DAP will try to upload the default configuration file name dapcfg.txt. If you fill in a file name in option 67, the DAP will upload the configuration file name that you have entered here. It is strongly recommended to leave the file name field blank.


The easiest way to provide the DAPs with the correct data from the DHCP server, is using the DHCP server that comes with the DAP Controller installation software. The DAP Configurator tool allows you to setup the required DHCP server configuration easily.

The DHCP Server that comes with the installation of the DAP Controller/Manager is by default installed when you do the installation for "Multiple System". If you do the installation for "Single System", the DHCP server is not installed by default. However, if you select "Custom" installation you can choose to install or not install the DHCP server.


However, if you don't want to use the DHCP server that comes with the DAP Controller installation, e.g. because there is DHCP server already in the network, you can use a DHCP server of your choice. But make sure that the required parameters are delivered to the DAPs.

3.2 TFTP Server

The configuration file and the firmware are uploaded to the DAP(s) using a TFTP server. The DAP Controller software includes a TFTP Server. You can select that TFTP server using the DAP Configurator. When you use the TFTP server that comes with the DAP Controller, the TFTP Server configuration is automatically setup correctly.

 *The TFTP Server that comes with the installation of the DAP Controller/Manager is by default installed when you do the installation for "Multiple System". If you do the installation for "Single System", the TFTP server is not installed by default.*

However, if you select "Custom" installation you can choose to install or not install the TFTP server. See installation procedure in Section 7.2 Installing the DAP Controller Release .

 *Do not use the TFTP Server that comes with the DAP Controller for permanent use. The TFTP Server is included in the DAP Controller software, in order to allow you to setup a system easily, without DAP Controller permanently connected. In a customer network with the DAP Manager permanently connected, please use the TFTP server that the IT Manager recommends you to use.*

3.3 Operation without DHCP or TFTP Server

If your DHCP server and or TFTP server is not permanently connected, you can store the IP address and the configuration file in the DAPS in Flash memory. Note that the firmware is always stored in Flash memory in a DAP.

To store the IP address configuration in Flash memory in the DAP, the following two requirements must have been met:

- The DHCP server must issue an "Infinite" lease time. (The DHCP server that comes with the DAP Controller issues such a lease time by default!)
- In the configuration setup, you must select "Replace" from the drop down menu for IP Configuration in the boot options in the DAP Configurator screen. See [Section 3 IP Settings on page 11-3](#).


After this the DAP does not need a DHCP server anymore.

To store the Configuration file in Flash memory in the DAP, the following two requirements must have been met:


- The DHCP server must issue an "Infinite" lease time. (The DHCP server that comes with the DAP Controller issues such a lease time by default!)

- In the configuration setup, you must select "Replace" from the drop down menu for DAP Configuration in the boot options in the DAP Configurator screen. See [Section 3 IP Settings on page 11-3](#).

When IP configuration and configuration file are stored in the DAP, the DAP does not need to have a DHCP server nor TFTP server anymore in the startup processes.

 *When a DAP starts up, it still does a DHCP request and TFTP request. If it gets valid data from the DHCP Server and TFTP server, and a valid configuration file with boot options set to "erase" or "Replace" it will either erase or replace the stored data. If it doesn't get those three items (DHCP, TFTP and valid file) the DAP ignores the data that it has got, and starts up with the stored data.*

3.4 Using other DHCP and/or TFTP Servers

 *If you install the DAP controller/Manager software as "Single System" the DHCP and TFTP server are normally not installed. This means that you must use your own DHCP or TFTP server. Consult the "Business Mobility IP DECT Advanced Data Manual", Chapter "Other DHCP/TFTP Servers" for examples of other servers.*

It is possible to use a DHCP server or TFTP server of your choice. However, the DHCP server must provide the five parameters as mentioned in [3.1 DHCP Server on page 7-2](#). Also mind the lease time specification if you want to store IP configuration and/or DAP configuration data in the DAP(s).

The TFTP server must be capable of handling as many simultaneous TFTP request as there are DAPs. Remember, if the DAPs start up simultaneously, they do a TFTP request simultaneously.

In the IP DECT Advanced Data Manual, you find examples of how to setup other DHCP and TFTP servers.

Preparing DAP Manager PC

SECTION 1 **HARDWARE REQUIREMENTS**

The PC that is used for the Business Mobility IP DECT software must comply with the following requirements:


- ☐ CPU speed: 2,4 GHz or higher
- ☐ 1 Gb RAM or more
- ☐ DVD-ROM drive
- ☐ 2Gb hard disk space free

SECTION 2 **SOFTWARE REQUIREMENTS**

2.1 **Operating System**

The operating system for the DAP Controller/Manager PC should be as follows:


- Windows 2003 SP2. Windows 2003 requires Rel. 2.
- Windows XP Professional, SP2/SP3.
- Windows 7 (not the Home version!)
- Windows 2008 SP2
- Windows 2008 R2

 *The DAP Controller/Manager supports the International (English US) version of the above mentioned MS Windows operating systems. Other MS Windows language versions are not explicitly tested but are not expected to show any problems. In case of problems please contact your IP DECT Supplier, and clearly indicate which MS Windows version is used and the nature of the problem.*

2.2 IIS and Internet Explorer

Besides the operating system, the Windows WEB server, called IIS (Internet Information Services) is required. However, during installation, IIS is automatically installed.

When you install the DAP Controller software under Windows XP or Windows 2003, the system may ask for the Operating System CD-ROM/DVD-ROM.

 *On the client computer, you must use Internet Explorer 6.0 or higher to view the DECT Manager WEB pages.*

2.3 .NET Framework


The DAP Controller software requires .NET Framework 4.0. However, this is automatically installed when installing the DAP Controller software.

If there is already another version of .NET Framework on your PC, it does not do any harm. .NET Framework versions can co-exist.

2.4 DHCP Server and TFTP Server

- DHCP Server - A DHCP Server is required in the network. However, the DAP Controller software Release 5 includes a DHCP Server which is automatically configured when you run the DAP Configurator tool. You may also use an existing DHCP Server in the Network, or your own DHCP Server. For more info on other types of DHCP Servers, consult chapter "Other DHCP/TFTP Servers" in the IP DECT Advanced Data Manual.

However, make sure that the DHCP Server has correct settings for the Business Mobility IP DECT and reference to the TFTP Server. Also make sure that you have specified a default gateway/router address in the DHCP server, which is within the subnet address range of the DAPs.

 *You should use the built-in DHCP server that comes with the DAP Controller only in very small installations (< 10 DAPs).*

- TFTP Server - This can be an existing TFTP Server in the Network, or your own TFTP Server or the TFTP Server that is included in the IP DECT software. It is recommended to use the built-in TFTP server only in small installations (< 20 DAPs). For larger installations you should use a professional TFTP server.

SECTION 3 VIRTUALIZATION

The DAP Controller Release 6 supports virtualization on VMWare and Xen.

The Virtual Machine system should meet the requirements for a non virtualized server. If the network connection on the virtual machine is shared with another virtual machine or the Host, make sure that there is sufficient bandwidth available for the DAP Controller Virtual Machine.

SECTION 4 MARATHON FAULT TOLERANCY

Marathon software with the EverRun® software and Citrix XenServer can be used to provide fault tolerance on various software applications. IP DECT Release 6 supports working on a Marathon platform, to provide fault tolerance.

For more information on the Marathon software, please consult the NEC Unified web page.

Please note, that IP DECT supports built-in Redundancy on the DAP Controller and Proxy without Marathon,. See [Redundancy \(General\) on page 12-1](#).

THIS PAGE INTENTIONALLY LEFT BLANK

Installing The DAP Controller/Manager

SECTION 1 PRECONDITIONS

Make sure that you have decided which DHCP Server you are going to use. Also make sure that you have decided which TFTP server you are going to use.

Also make sure that the network components (Switches, Routers) are correctly configured for VoIP and IP multicast. Be fully aware of the network topology! Make sure that the network supports IP Multicast between all network components that are used for Business Mobility IP DECT.

SECTION 2 INSTALLING THE DAP CONTROLLER RELEASE 6

To install the DAP Controller Release 6, follow the steps below.

1. Make sure that you are logged in with Administrator Rights!
2. Un-zip the DAP installer package.
3. Double click setup.exe or setup.
4. Depending on the version of your Windows operating system, you will now see a security screen from Windows saying **"Do you want to allow the following program to make changes to your computer?"**
5. Click **Yes**. [Figure 9-1 System Configuration Check](#) displays. This indicates that the DAP Controller software supports your version of Windows.
6. Click **Next** to proceed.

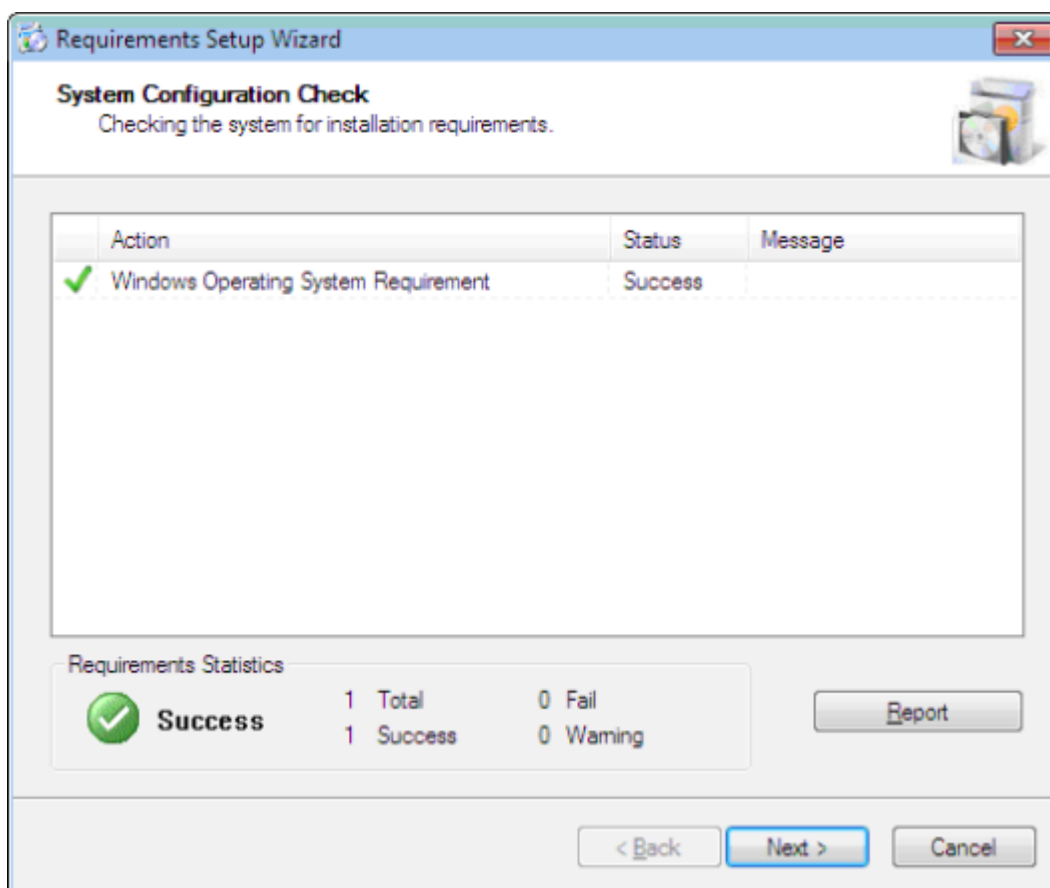


Figure 9-1 System Configuration Check

Now the installation of "Prerequisites" takes place. Note that this can take several minutes! When all required prerequisites are installed, [Figure 9-2 Install Prerequisites](#) displays.

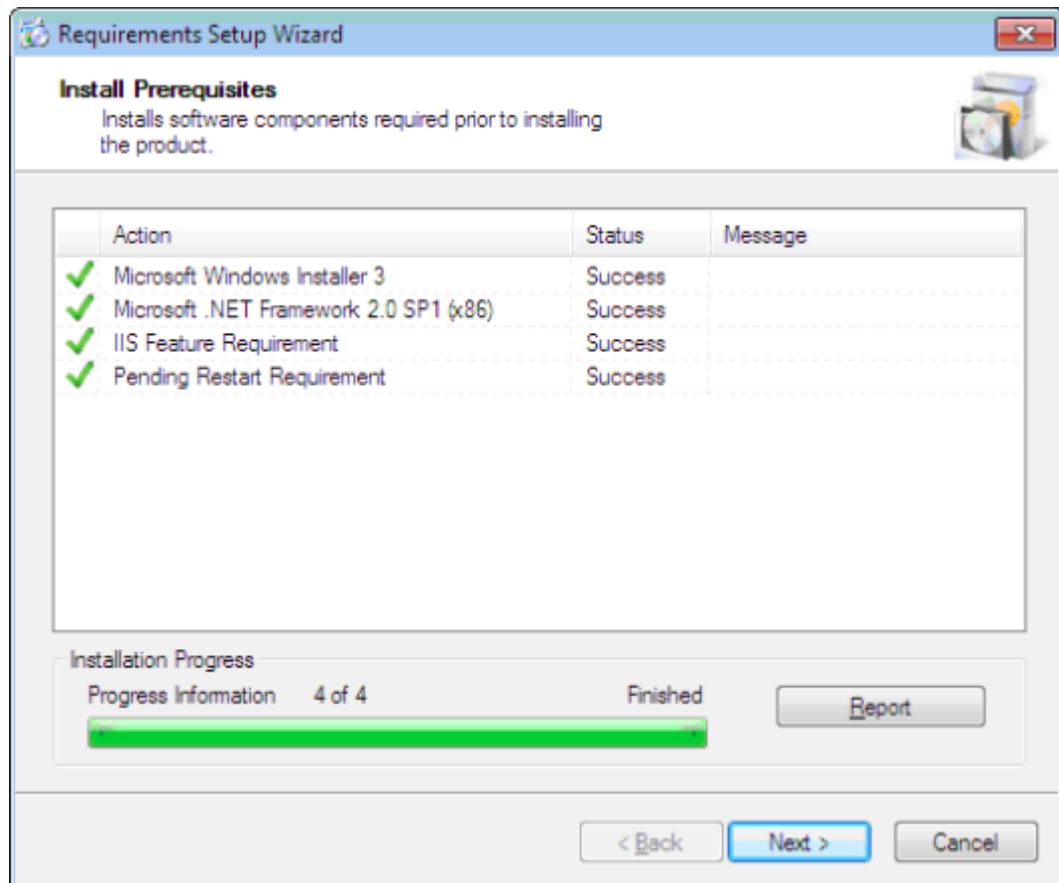


Figure 9-2 Install Prerequisites

In case of Windows XP or Windows 2003, the system may ask for the Windows Operating System CD/DVD-ROM. If asked for, insert the CD/DVD-ROM.

7. Click **Next** to continue. [Figure 9-3 Install Shield Wizard](#) displays, indicating that the system is ready to start the installation of the DAP Controller.

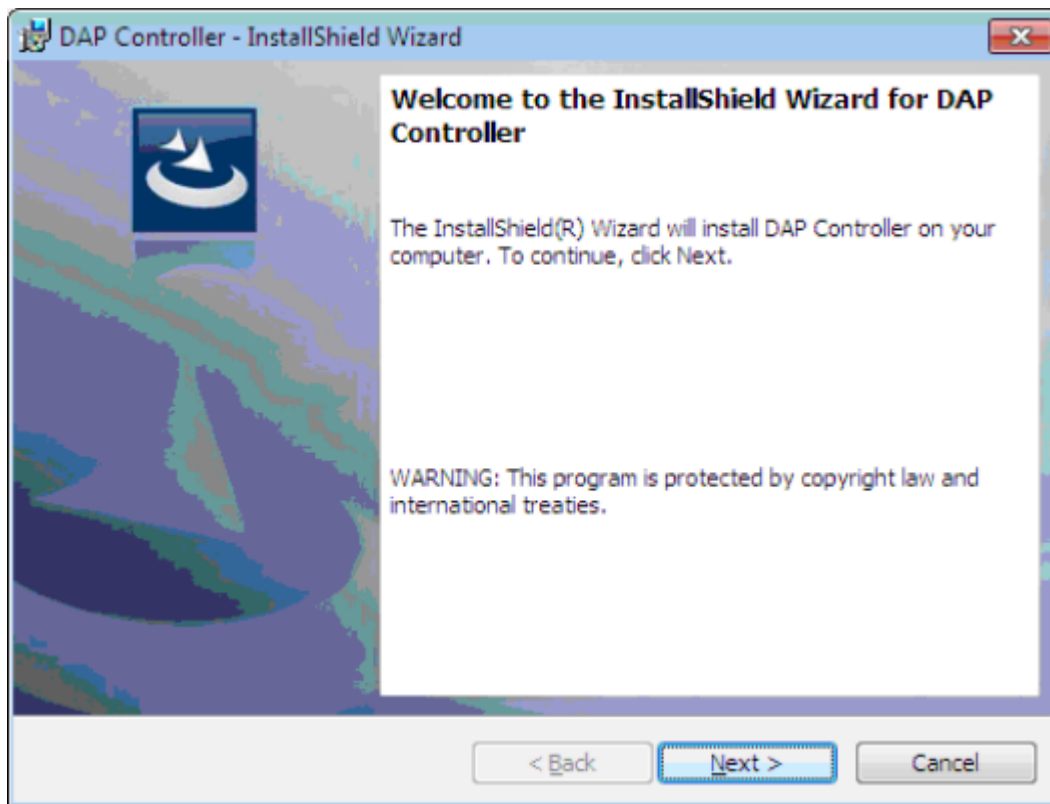


Figure 9-3 Install Shield Wizard

8. Click **Next** to continue. [Figure 9-4 Choose System Type](#) displays.

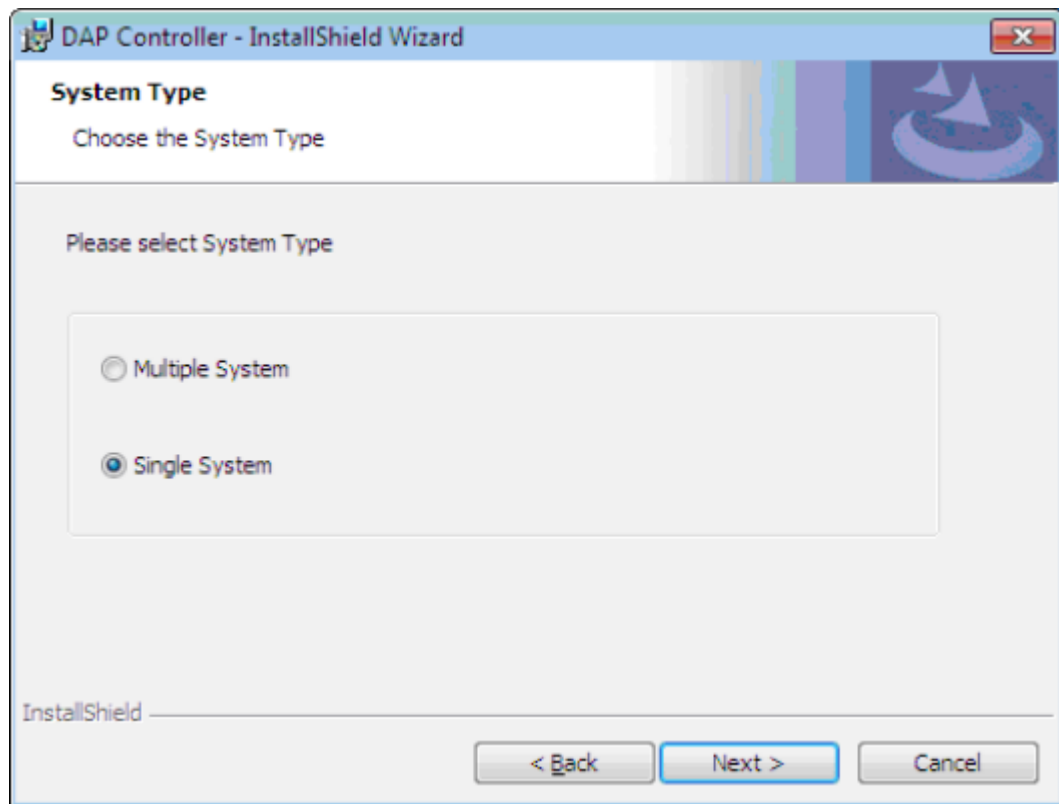





Figure 9-4 Choose System Type

9. Please select the system type that you prefer, **Multiple System** or **Single System**.

Select **Single System** if you want to manage only one IP DECT system, or **Multiple System** if you want to manage more than one IP DECT system with your PC. Click Next.

-  If you select **Single System** the DHCP Server and TFTP Server are not installed (by default). However, if you want to install them anyway, select the option "**Custom**" in step 9, and select DHCP Server and TFTP Server to install.
-  If you select **Multiple System**, the Services that are installed for IP DECT are installed with startup parameters "**Manual**". This means that they will not start automatically when Windows boots up. If you select **Single System**, the Services will be installed with startup parameters "**Automatic**".
-  You can always change the settings from Multiple System to Single System and vice versa later on. See [Section 4 Single Site / Multi Site on page 10-8](#).

10. Click **Next**. [Figure 9-5 Choose Setup Type](#) displays.

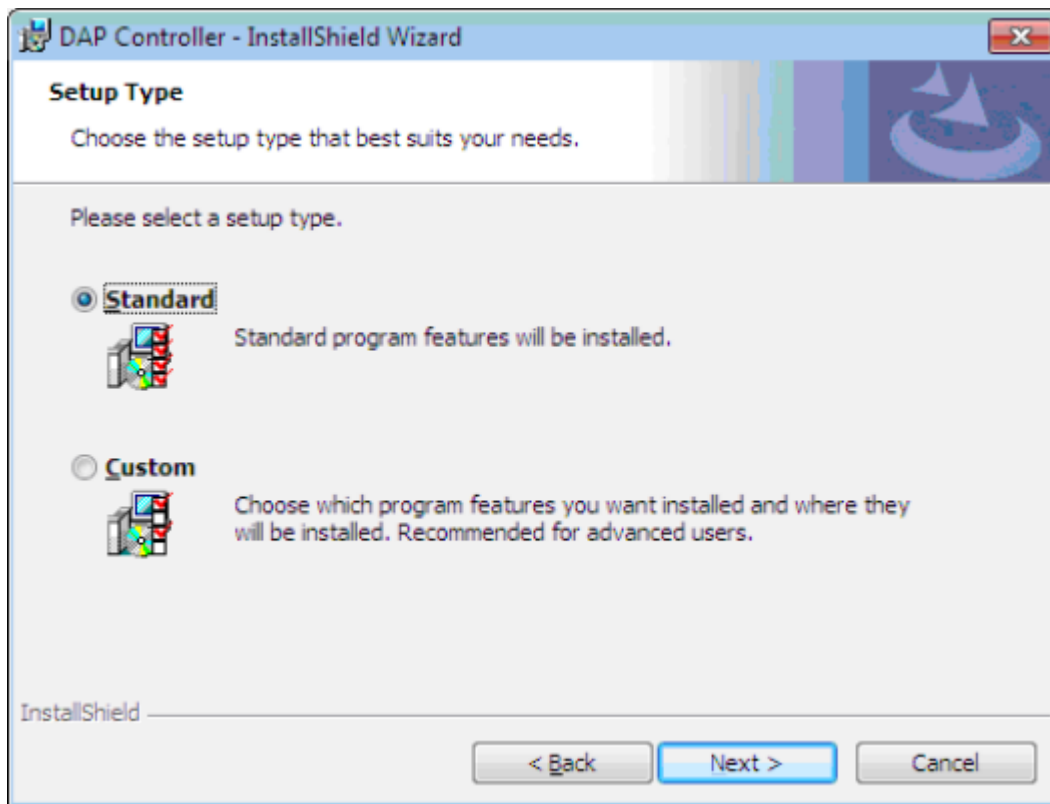


Figure 9-5 Choose Setup Type

In this window you should specify the Setup Type.

11. Select **Standard** and click **Next**.

OR

If you want to fine tune the installation, select **Custom** and click **Next**.


 *The system has collected sufficient info to start the actual installation.*

Figure 9-6 Ready to Install displays.

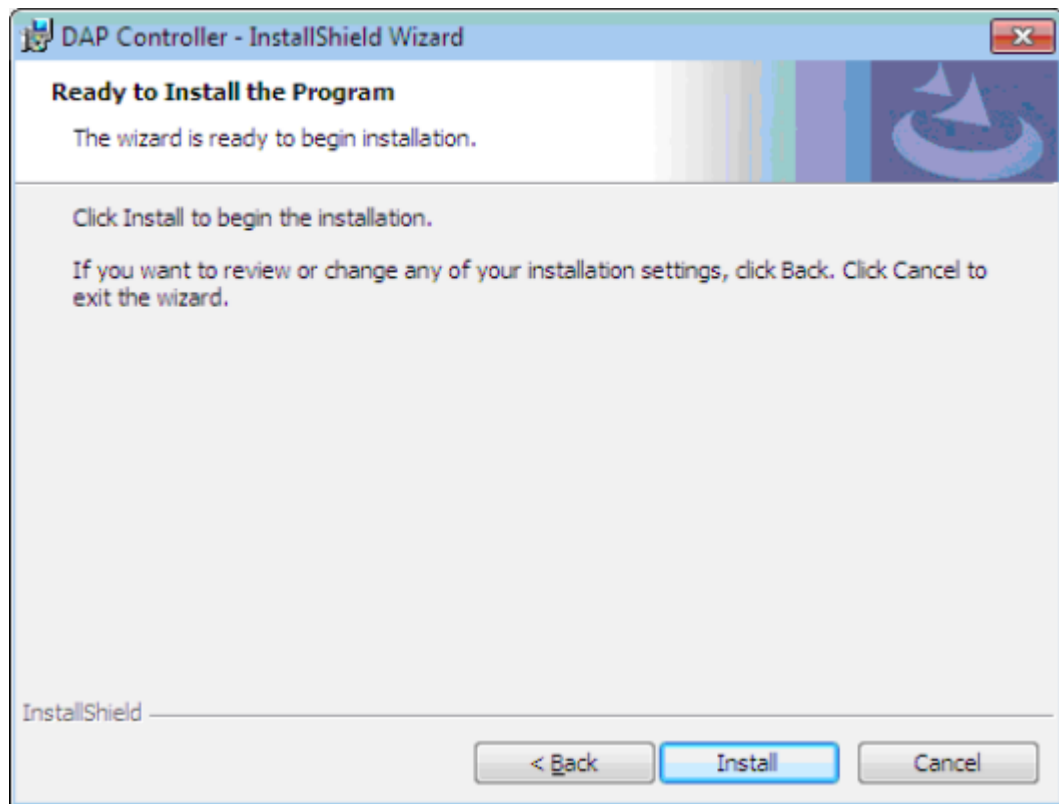


Figure 9-6 Ready to Install

12. Click **Install** to begin the installation. When the installation is finished, [Figure 9-7 Installation Complete](#) displays.

When the **Launch DAP Configurator** is checked, the DAP Configurator will start after clicking **Finish**. If not, the installation finishes, but the DAP Configurator will not start. However, you can start the DAP Configurator from the Programs menu later.

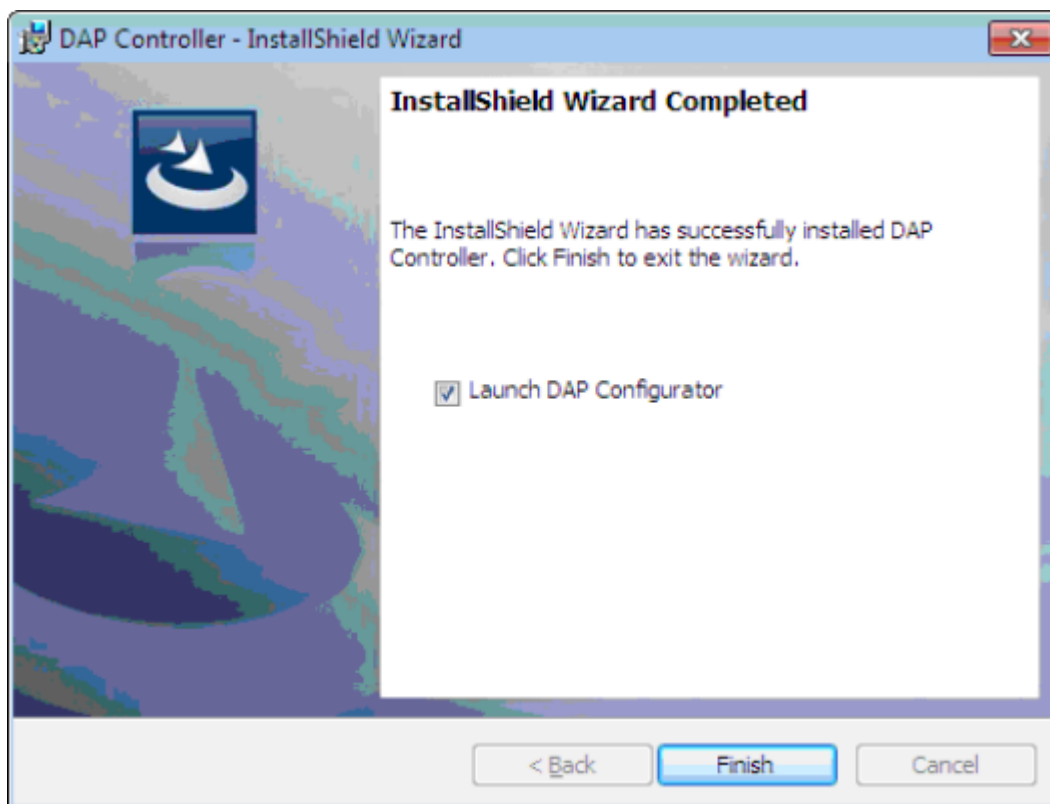


Figure 9-7 Installation Complete

13. Click **Finish**.

Configuration - DAP Configurator Tool

SECTION 1 **GENERAL**

The DAP Configurator is a tool for creating the configurations files for the DAP Manager and DAPs. It is automatically installed when you install the DAP Controller/Manager. It is also automatically started up during the installation of the DAP Controller/Manager.

After you went through the DAP Configurator windows and you have entered the correct data, a number of configuration files are created.

You can always start-up the DAP Configurator tool using the shortcut to the DAP Configurator tool in the **Start > All Programs > DAP Controller > DAP Application > DAP Configurator** menu.

SECTION 2 **USING THE DAP CONFIGURATOR**

Follow the steps below to set up the DAP Configurator tool.

2.1 Setting Up the Configuration

1. Make sure that the installation of the DAP Manager was successfully executed. If you selected to start the DAP Configurator automatically after the installation, continue to step 3 in this procedure. If not, continue with step 2 in this procedure.
2. Start the DAP Configurator tool, via **Start > All programs > DAP Controller > DAP Applications > DAP Configurator** as seen in [Figure 10-1 Starting DAP Configurator](#).

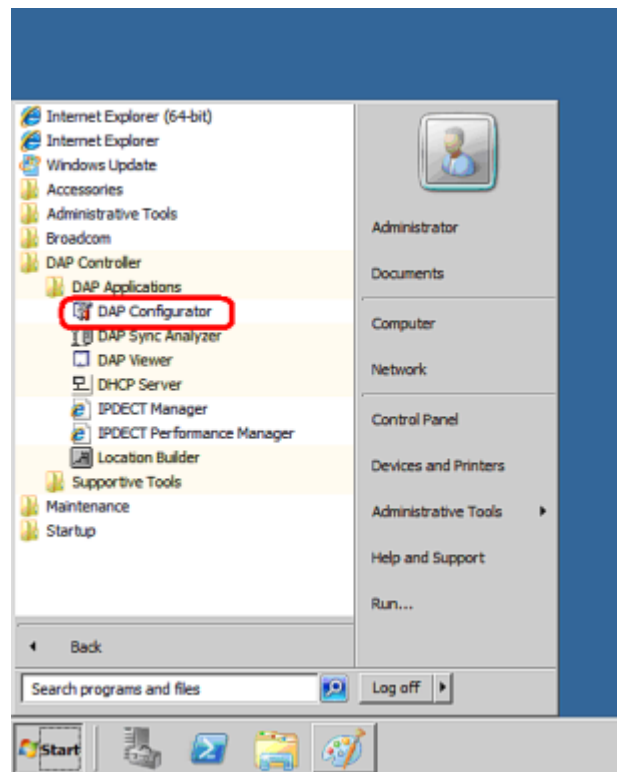


Figure 10-1 Starting DAP Configurator

If there is a problem with your network card (e.g. no cable connection), you will receive a message. Please solve the problem. If you do not see this message, continue with the next step in this procedure.

If you are starting the DAP Configurator for the first time, the system asks you for the license file as seen in [Figure 10-2 Select License File](#).

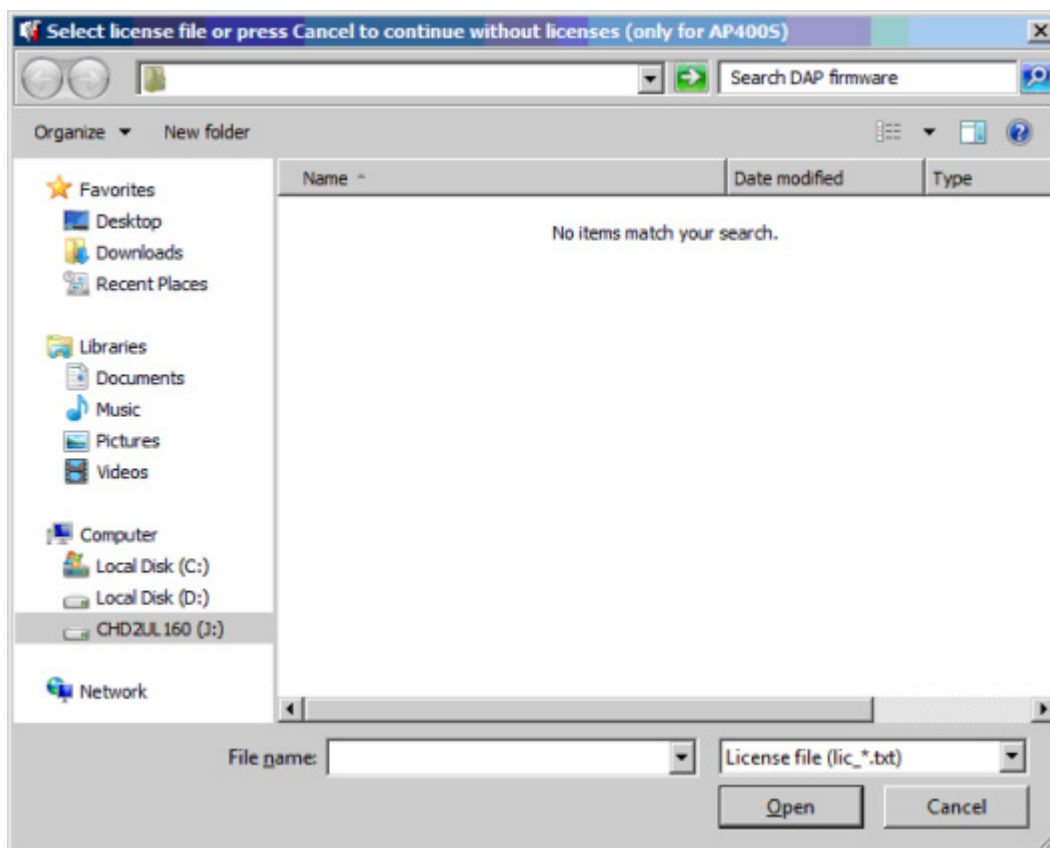



Figure 10-2 Select License File

3. Select the license file and click **open**. [Figure 10-3 System Control](#) displays.

 *If you do not have a license file, the system allows only up to 4 AP400S DAPs.*

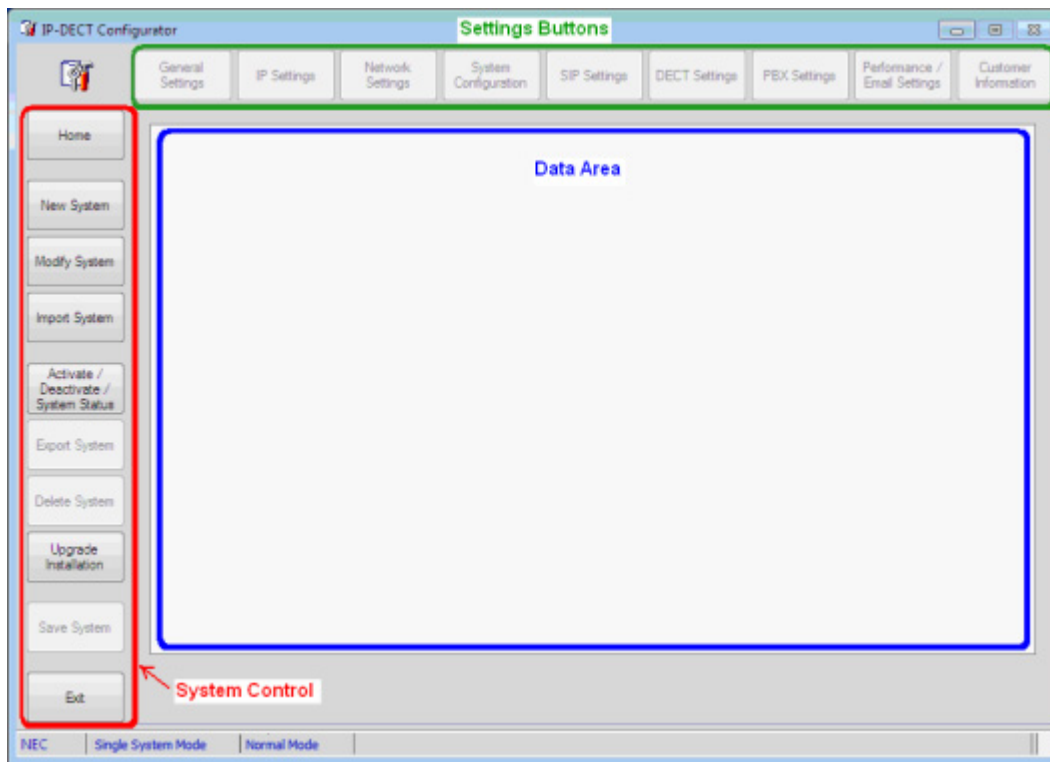


Figure 10-3 System Control


Note that there are three sections in this window:


- System Control section at the left side.
- Settings Buttons at the top part of the window.
- Data information part in the middle of the window.

If you start-up the DAP Configurator after configuring a system, you will see one or more extra buttons highlighted.

The way the buttons are greyed out may be different in your system.

4. In the System Control section (left side) click the button that is applicable to your need. For a new installation it will be **New System**.

 *If you don't want to start a new system installation, consult [Section 3 System Control Section](#) for more information on the buttons.*

 *If you want to change system settings, you must use the buttons in the top part of the window. These buttons are described in [Section 1 Settings Buttons on page 11-1](#).*


5. Continue with the section that is applicable for your situation.

SECTION 3 SYSTEM CONTROL SECTION

3.1 General

The System Control section is located at the left side of the IP DECT Configurator window.

Using one PC, you can manage more than one IP DECT system. For such an IP DECT system you must setup a configuration on your PC. For each individual system, you can change settings, using the buttons in the top part of the window. However, you can have only one IP DECT system configuration active at the time. Therefore, you can start or stop an IP DECT system.

 *When you "Stop" an IP DECT system, the DAPs remain up-and-running. This means that you can still make and receive phone calls. However, the DAP Controller/Manager function is stopped, which means that some functionality (e.g. messaging or moving between Branch Offices) does not work anymore.*




The System Control part consists of the following buttons:

- **Home** - Brings you back to the "start" screen.
- **New System** - Allows you to create a new system configuration on your PC.
- **Modify System** - Allows you to select a system configuration, and then manipulate or modify the system.
- **Import System** - Allows you to import a system configuration that has previously been exported. You can import individual files from the exported .zip file or you can import the exported .zip file in one go.
- **DAP Lite Download System (if displayed, it is greyed out)** - Not applicable for this configuration.
- **Activate/Deactivate System Status** - The system status button leads you to a window in which you can control the system status. See [3.2 System Status Window](#).
- **Export System** - Allows you to export a system configuration. The exported file is always a .zip file and contains all relevant system configuration files, including subscription data, DAP configuration, DHCP data etc. The generated file can be imported later or can be imported on another PC that you want to use as DAP Controller/Manager PC. Note that this file can be used as a backup of your entire system configuration. Note that you must select a System (configuration) first, using the **Modify System** button.
- **Delete System** - This removes a System (configuration) from your PC. Note that you must select a System (configuration) first, using the **Modify System** button.

- **Upgrade Installation** - This allows you to upgrade the installation in a convenient way. You are guided through the Upgrade procedure.
- **Save System** - This saves the changes that you have made on a System (configuration) to files on your PC. Note that after you saved the System (configuration), you can go to the System Status button and then make the system active.
- **Default** - Return to default settings.

3.2 System Status Window

[Figure 10-4 System Status Window](#) displays when you click the **System Status** button. Note that when you have more than one IP DECT system (configuration) you must selected a System first, using the **Modify System** button and that you have saved your new configuration before starting it.

-  *Make sure that you have stopped a previously running system.*
-  *If you have made a new configuration, or if you have changes configuration settings, make sure that you have saved the configuration first, using the **Save System** button.*
-  *Starting or stopping the system, only starts or stops the services and applications running on the DAP Manager PC. This means that the DAPs remain operational. Basic call handling is still possible if the DAPs are up and running.*

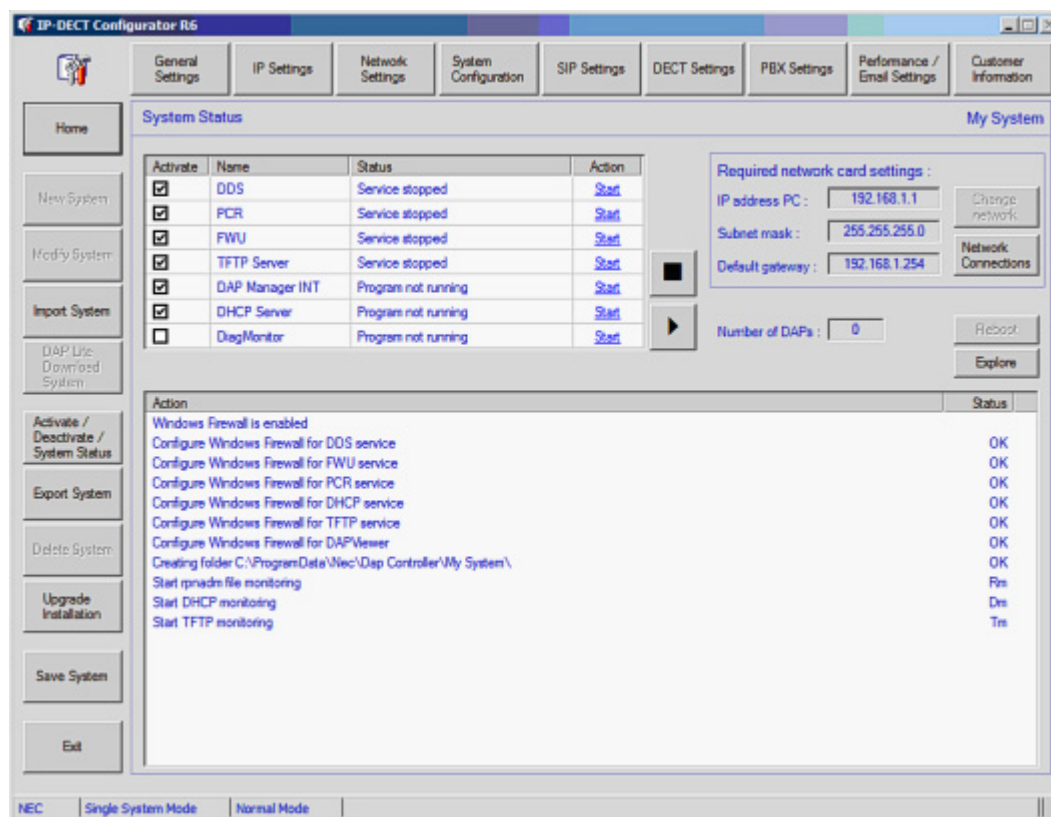


Figure 10-4 System Status Window

The following services can be started or stopped:

- **DDS** - DDS (DECT Data Server) takes care of all DECT processes to and from the DAPs.
- **PCR** - PCR (Performance Counter Retrieval) must be running to retrieve performance data files and to enable sending an e-mail when performance thresholds are exceeded or when a DAP goes down.
- **FWU** - FirmWare Upload must be running if you want to use Firmware Upload.
- **TFTP** - The TFTP Service refers to the TFTP server that was automatically installed with the DAP Controller/Manager software. Note that this is not the MS Windows TFTP server. A TFTP Server must be running when one or more DAPs start-up. The TFTP server supplies the DAPcfg.txt configuration file to the DAP(s). Note that there can be only one TFTP server running on your PC. If you start the TFTP service make sure that there is no other TFTP server running on your PC.
- **DAP Manager** - Starts up the WEB service for IP DECT in IIS and opens

the WEB Page of the DAP Manager in Internet Explorer.

If using Windows 2008, the status of the DAP Manager window (in Internet Explorer) cannot be displayed. You will see an exclamation mark in the "run" button to inform you.

The following programs can be started or stopped:

- **DHCP** - The DHCP server runs as an application. It can be started or stopped. Make sure that you are allowed to use a DHCP server on the Network.
- **DiagMonitor** - The DiagMonitor is used to collect diagnostics data.

In addition to the services and applications on the PC, you can also reboot the DAPs.

When you start a System, the IP DECT Configurator may ask you if you want to reboot the DAPs as well, [Figure 10-5 Reboot DAPS](#). Note that this can be necessary, because the configuration changes must be uploaded to the DAPs as well. This requires a reboot!

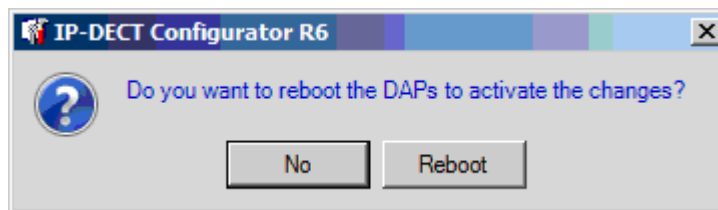


Figure 10-5 Reboot DAPS

SECTION 4 SINGLE SITE / MULTI SITE

If you use the DAP Manager PC to manage one IP DECT system only, you can create a single site system. If you want to use your DAP Manager PC to manage more than one IP DECT system you can setup the DAP Configurator to manage more than one site, "multi site". You have made a selection during the installation.

However, if you want to change the single site or multi site setting, follow the steps below:

4.1 Switching between Single Site and Multi Site

1. Make sure that the IP DECT Configurator is open. If not, open the IP DECT Configurator/DAP Configurator. See [Section 2 Using the DAP Configurator](#).
2. Using the DAP Configurator, left mouse click the top left IP DECT Configurator

icon. See [Figure 10-6 DAP Configurator Icon](#).



Figure 10-6 DAP Configurator Icon

3. In the window that is opened, click **More**. [Figure 10-7 About Configurator](#) displays.

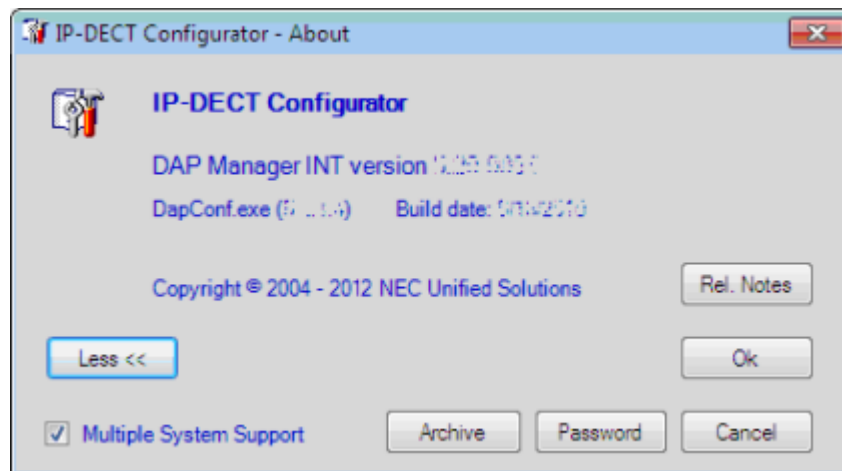


Figure 10-7 About Configurator

4. You can switch to **Multiple system Support** or **Single System** by means of the check box in the window. Click **OK** to activate your selection.

THIS PAGE INTENTIONALLY LEFT BLANK

DAP Configurator Settings

SECTION 1 SETTINGS BUTTONS

In the top part of the IP DECT Configurator window, you see a number of buttons that allows you to change settings in the system. In the following subsections these settings are explained.

SECTION 2 GENERAL SETTINGS

When you click **General Settings**, [Figure 11-1 General Settings](#) displays.

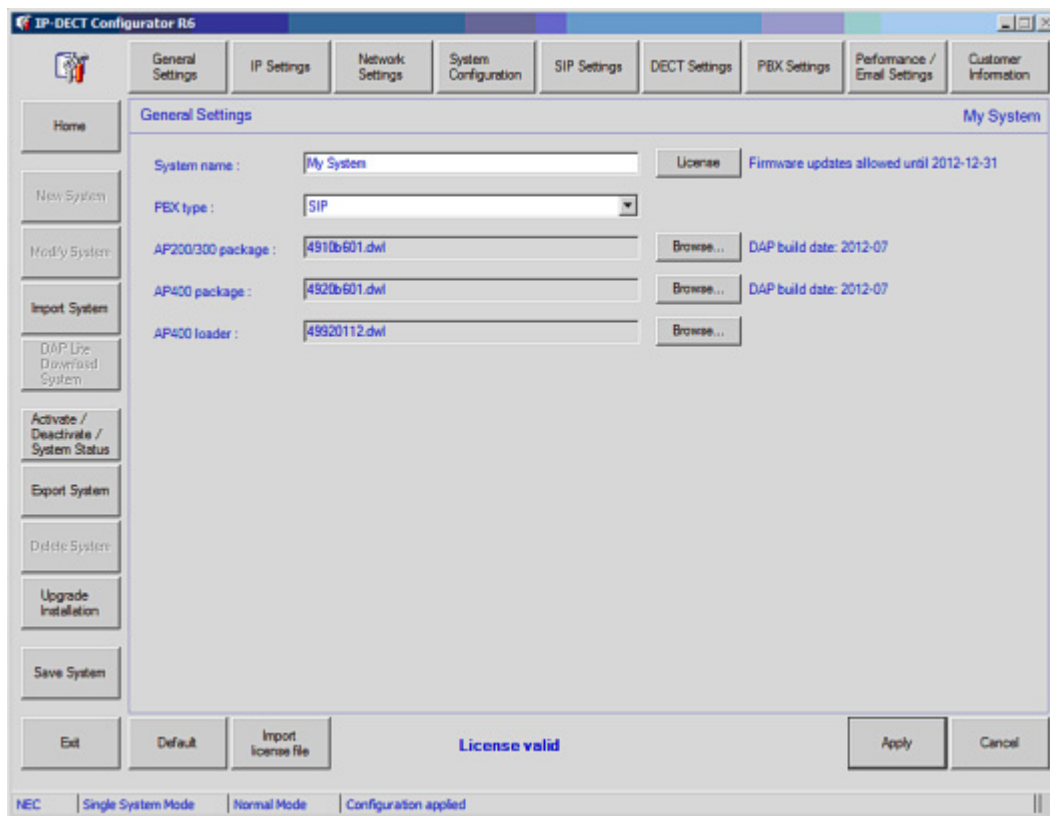


Figure 11-1 General Settings

The following items must be entered:

- ☐ **System Name** - Can be any given name. Note that this name will be used for a directory on the hard disk. This means that the name must comply with the requirements for Windows directory names.
- ☐ **PBX Type** - Select the platform to which the IP DECT system is (going to be) connected. Please note that there is a list of SIP Servers. Choose the SIP server of your choice. If your SIP server is not in the list, select "**SIP**" as for generic SIP.
- ☐ **AP200/300 Package** - Here you must enter the firmware file specification for the firmware package for the AP200 and AP300. For SIP, the file name should look like this: **4910bxyz.dwl** (e.g. 4910b610.dwl).
- ☐ **AP400 Package** - Here you must enter the firmware file specification for the firmware package for the AP400. For SIP, the file name should look like this: **4920bxyz.dwl** (e.g. 4920b610.dwl).
- ☐ **AP400 Loader** - The AP400 Loader is used for trouble shooting purposes only

and is provided per site on an as needed basis. If you received this firmware you would enter the Loader firmware package for the AP400. The file name would be similar to this: **49920112.dwl**

When finished, click **Apply**. On the bottom of the window, you should see, **License valid**. Continue by clicking button **IP Settings**.

SECTION 3 IP SETTINGS

3.1 The Window

When you click the **IP Settings** button, [Figure 11-2 IP Settings](#) displays.

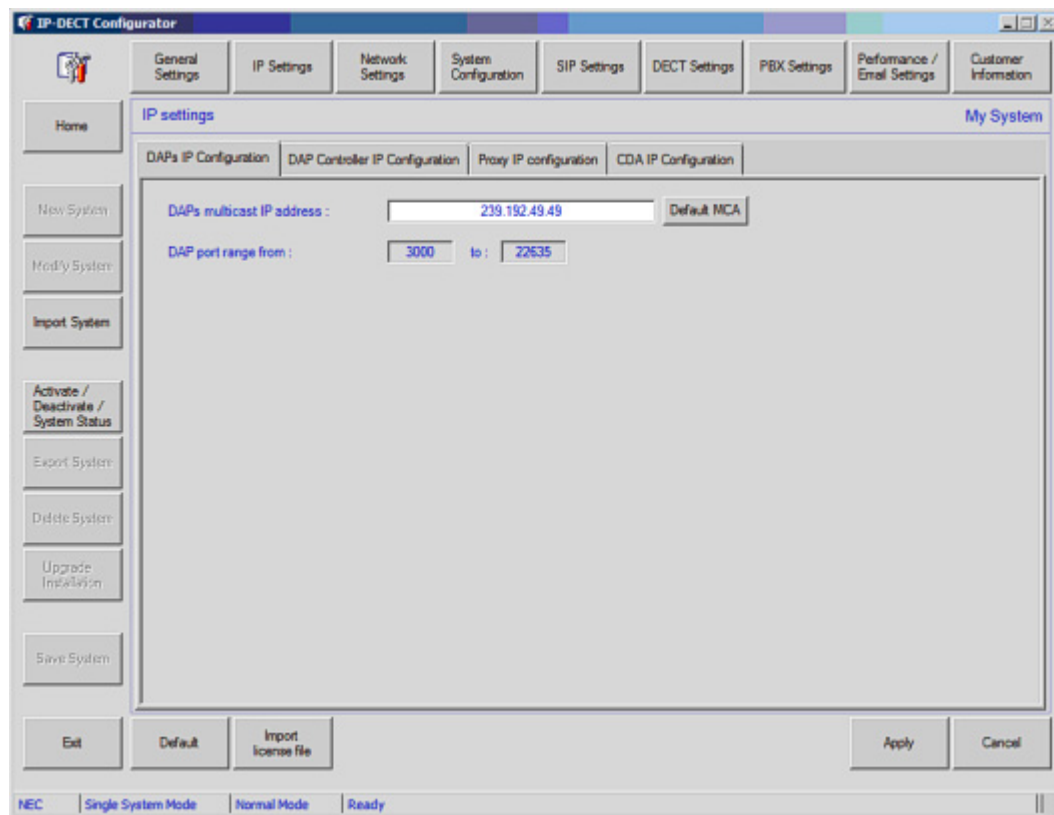


Figure 11-2 IP Settings

3.2 IP Settings, Tab "DAPs IP Configuration"

Please click the tab: **DAPs IP configuration**. Now the following fields can be edited:

- **DAPs Multicast IP address** - Specify a Multicast IP address. If the network for your IP DECT system is used for other purposes than IP

DECT as well or if the network has a connection to the company network or external network(s), you must ask the local IT manager for a multicast address. If your IP DECT system is in a closed network, you can click the button **"Default IP"** to use the default IP multicast address.

- **Port range from** - By default the port range on the DAPs will start at port 3000. Please note that you cannot change the port range.

3.3 IP Settings, tab "DAP Controller IP Configuration"

Please click the tab: **DAPs IP configuration**.

Depending on the Licenses that you have, one of the following screens is displayed, see [Figure 11-3 DAP Controller IP Configuration 1](#), [Figure 11-4 DAP Controller IP Configuration 2](#), or [Figure 11-5 DAP Controller IP Configuration 3](#).

If you have a multiple DAP Controller system, please read [DAP Controller Redundancy on page 13-1](#), before you continue making the configuration.

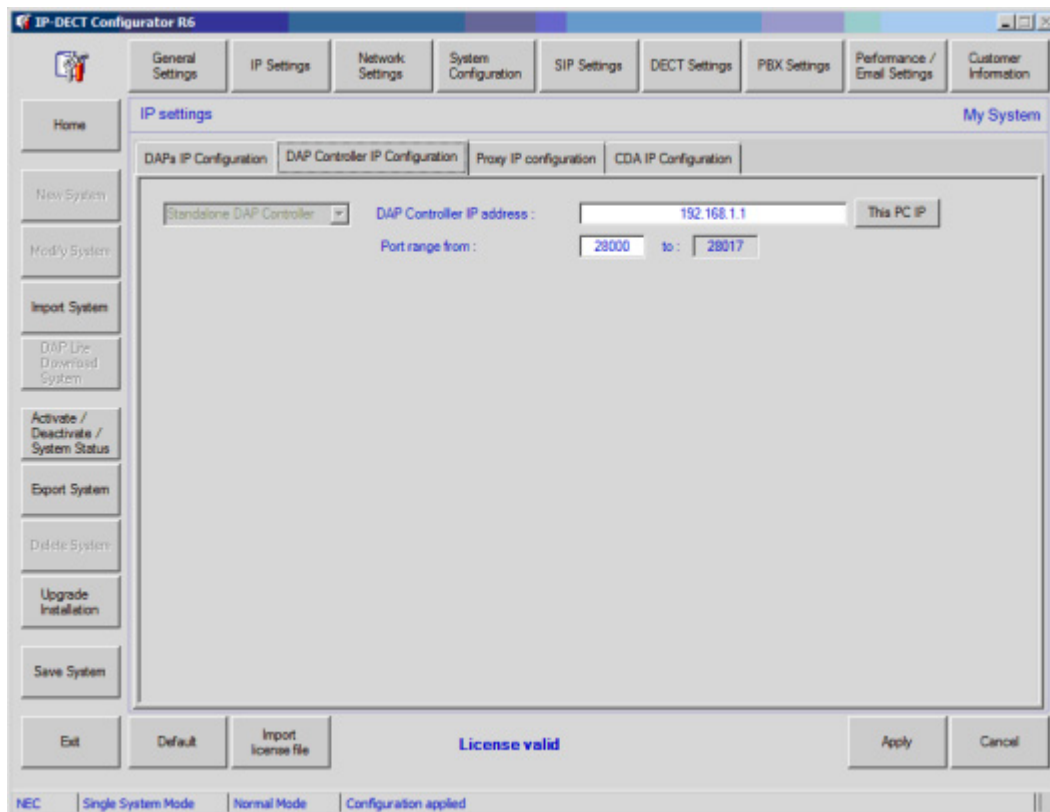


Figure 11-3 DAP Controller IP Configuration 1

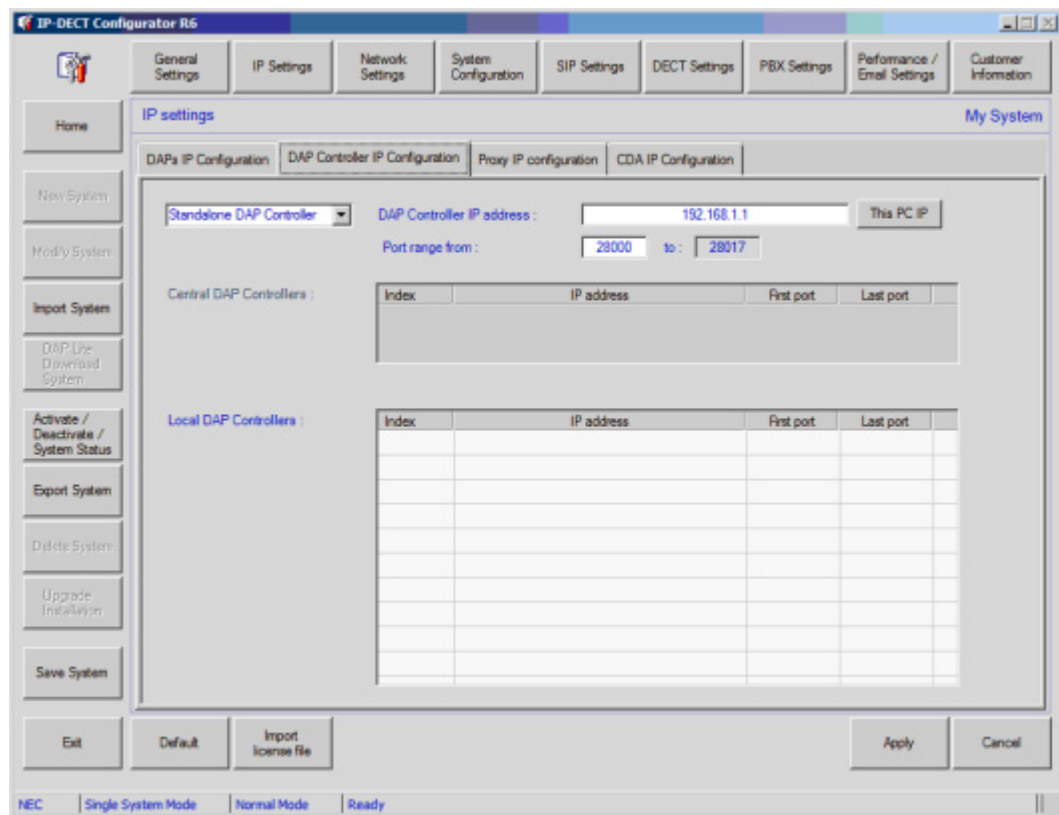


Figure 11-4 DAP Controller IP Configuration 2

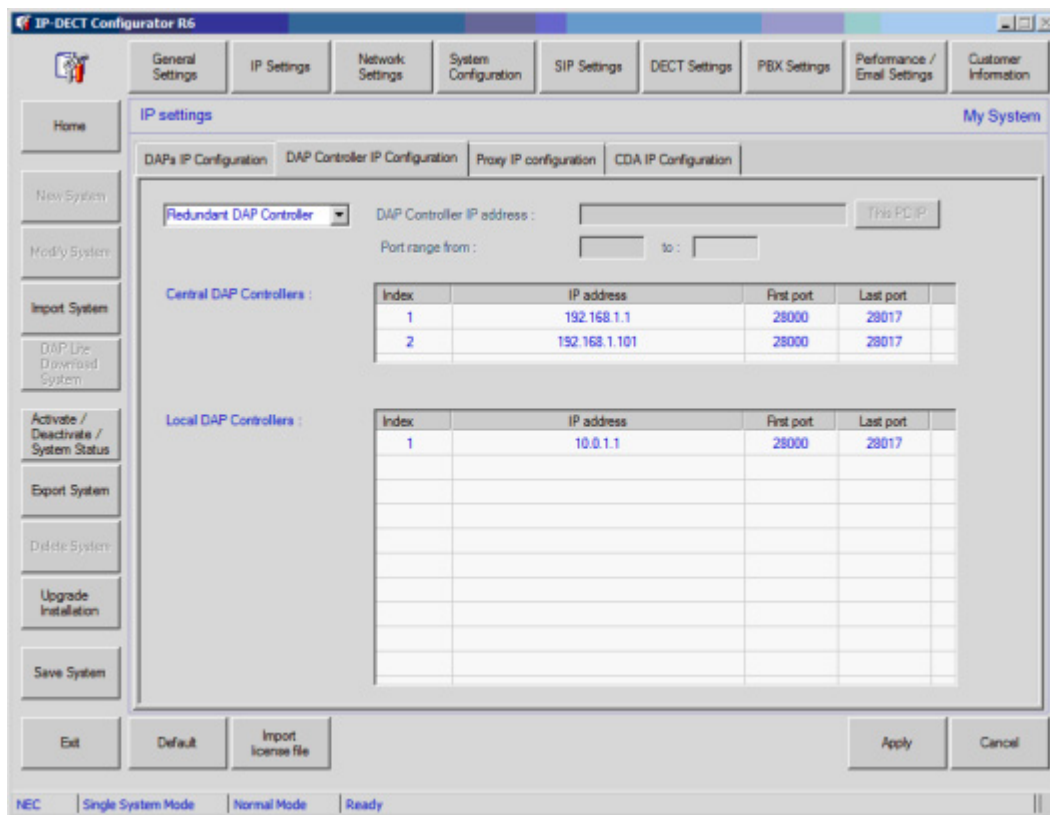



Figure 11-5 DAP Controller IP Configuration 3

You fill in the data of all DAP Controllers in the DAP Configurator of the Primary DAP Controller.

- **DAP Controller IP Address** - DAP Controller/Manager PC IP address. You can easily click the button "This PC IP" to copy the IP address of your PC into this field.
- **Port range from** - Start of port range in use for IP DECT on the DAP Controller/Manager PC. Note that this port range is automatically filled in. Please do not change manually.

Enter the IP Addresses of the DAP Controllers that are in your system.

 *When you enter more DAP Controllers than your License allows, you will get the message "License Violation".*

3.4 IP Settings, tab "Proxy IP Configuration"

Please click the tab: **Proxy IP configuration**, [Figure 11-6 Proxy IP Configuration](#) displays. Now the following fields can be edited:

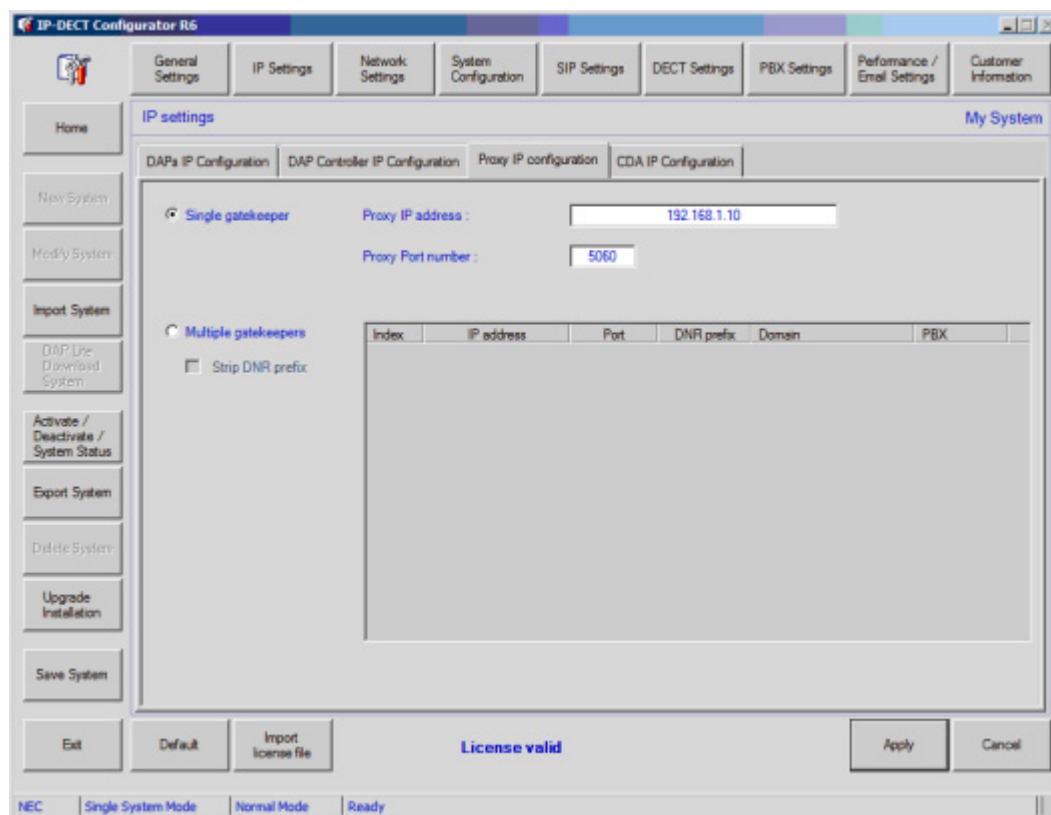




Figure 11-6 Proxy IP Configuration

- **Single Gate Keeper** - Click this radio button to select a system type with only one gatekeeper.
- **Proxy IP address** - Enter the IP address of the SIP Proxy.
- **Proxy port number** - Enter SIP port number on the SIP Proxy. The default port is 5060
- **Multiple gatekeepers** - When you click this radio button, are able to enter more than one SIP Proxy address. This is can be useful for redundancy reasons when having a dual SIP Proxy. You can add as many proxies as you want. Please note that this option is only available for SIP servers that support redundancy.
- **Strip DNR prefix** - When you check this checkbox, the system will strip one or more digits from the subscribed number and send the remaining digits to the SIP proxy. In case of a system with one SIP proxy the digit(s) are configured in the "SIP Settings" window, under the tab: **"Configuration settings"**. In case of a multi gatekeeper configuration, the digits are specified in the table of Proxies in this window.

3.4.1 Multiple SIP Proxies Settings

When you select **Multiple Gatekeepers**, the table in which you can add gatekeepers is activated. Right mouse click inside the table and select **new** to add a gatekeeper. The following items need to be entered.

- ☐ **Index** - This is a unique identifier per Proxy. This can be used to specify priorities in SIP Proxies ([SIP Proxy Redundancy on page 14-1](#)).
- ☐ **IP Address** - Enter the IP address of the next SIP Proxy. Note that the first proxy is already in the list.
- ☐ **Port** - Enter the port number for the next SIP Proxy.
- ☐ **DNR Prefix** (Optional) - You can enter an extension number prefix. If specified the extension numbers that start with this number will register on the associated SIP Proxy.
- ☐ **Strip Prefix** - If this check box is checked, the prefix of the subscribed number will be stripped. The remaining digits are sent to the SIP Proxy.
 -  This checkbox is valid for all Proxies in one go. You cannot switch this function on for one Proxy and switch off for another.
 -  This same check box is also available in the SIP Settings window under "configuration items". Both are the same!
- ☐ **Domain** - Specify the Domain IP address or the Domain name of the proxy. Note that in the SIP Settings button, there is also the possibility to enter a default Domain name which is used when you do not enter a Domain name here.
- ☐ **PBX** - Here you must select the PBX type.

3.5 IP Settings, Tab "CDA IP Configuration"

Please click the tab: **CDA IP Configuration**, see [Figure 11-7 CDA IP Configuration](#). Now the following fields can be edited:

- **Corporate directory IP address** - The IP address of the Central Directory Server (if applicable)
- **Corporate Directory port number** - Port number on the Central Directory server. Default port number is 30160

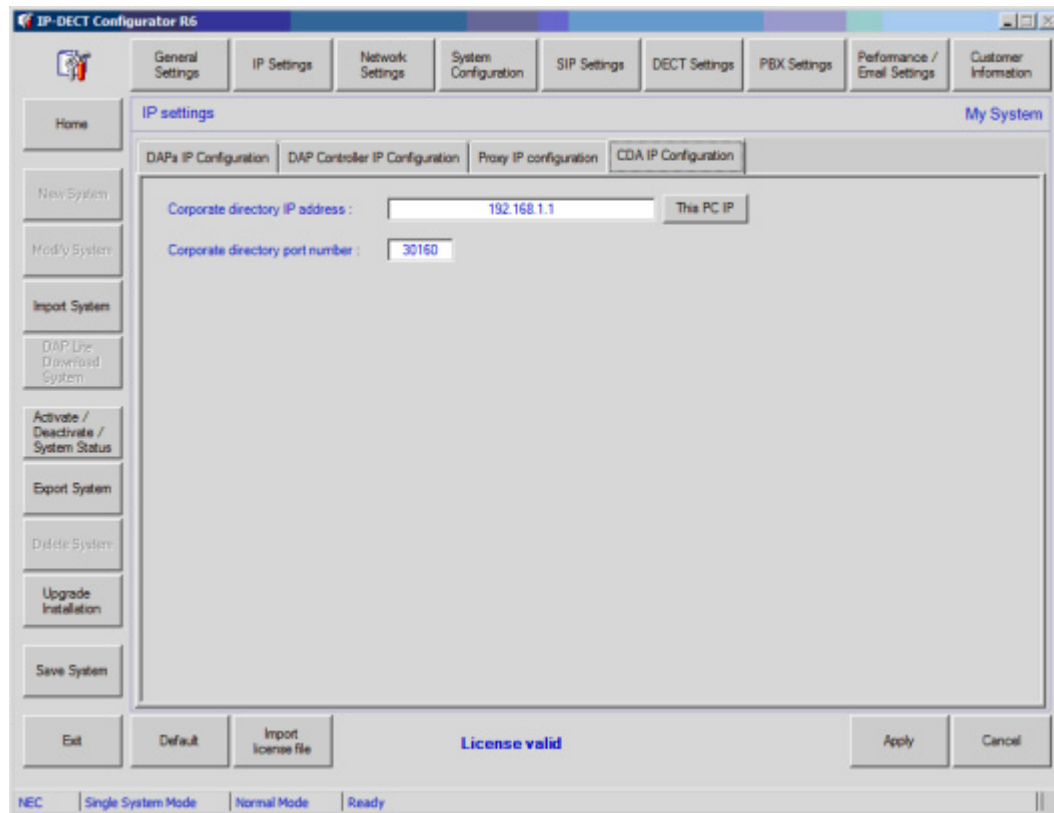


Figure 11-7 CDA IP Configuration

SECTION 4 NETWORK SETTINGS

4.1 Network Settings, Tab "Network Card Settings"

Please click the tab: **Network card settings**, see [Figure 11-8 Network Card Settings](#). Now the following fields can be edited:

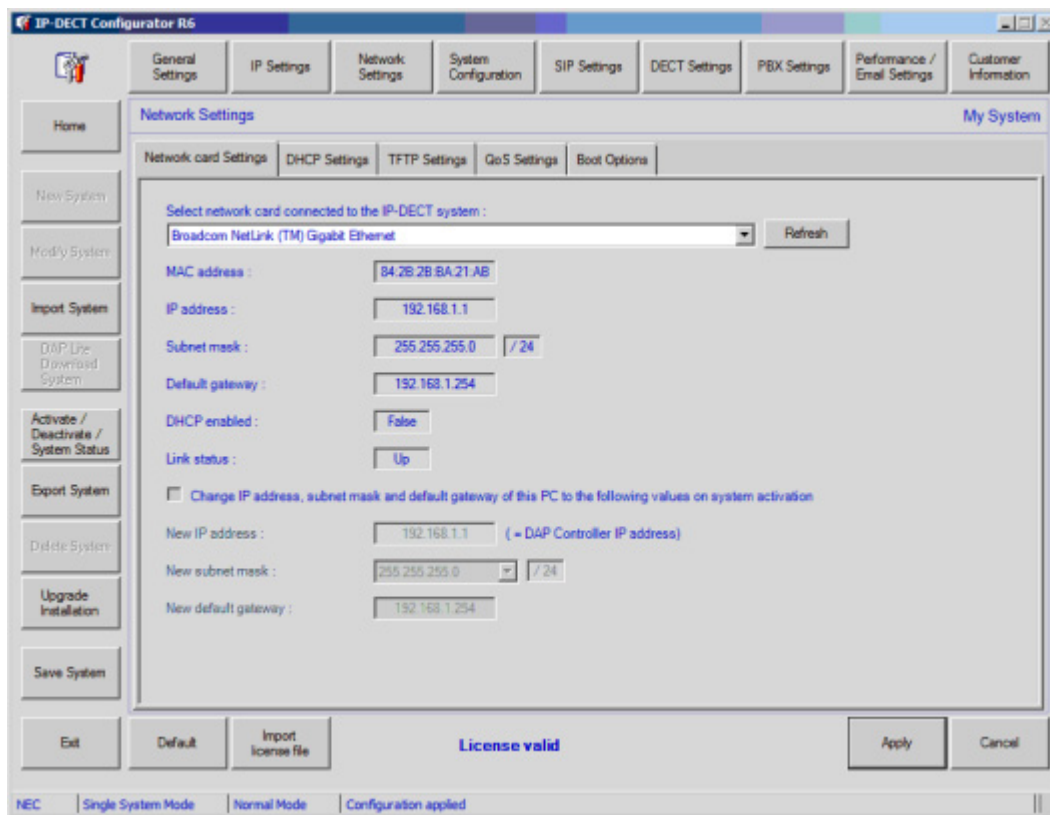


Figure 11-8 Network Card Settings

- **Select network card connected to the IP DECT system** - If you have more than one network card in your system, select the network card that you want to use here.

The network card data is displayed. Please note that you cannot change the network card data here!

- **Change IP address, subnet mask and default gateway of this PC in the following values on system activation** - If this box is checked, the IP address, subnet mask and default gatekeeper of your network card is automatically changed to the DAP Controller IP address that you have specified in [Section 3 IP Settings on page 11-3](#). This can be useful when you manage more than one IP DECT system with your computer. The moment that you start up one of your DECT system configurations, the IP settings of your network card are automatically changed to the right settings for that particular system.

Please note that the IP settings on the network card are automatically changed, but are not changed back to the previous settings.

This check box is greyed out in a Single System mode.

4.2 Network Settings, Tab "DHCP Settings"

Please click the tab: **DHCP Settings**, see [Figure 11-9 DHCP Settings](#). Now the following fields can be edited:

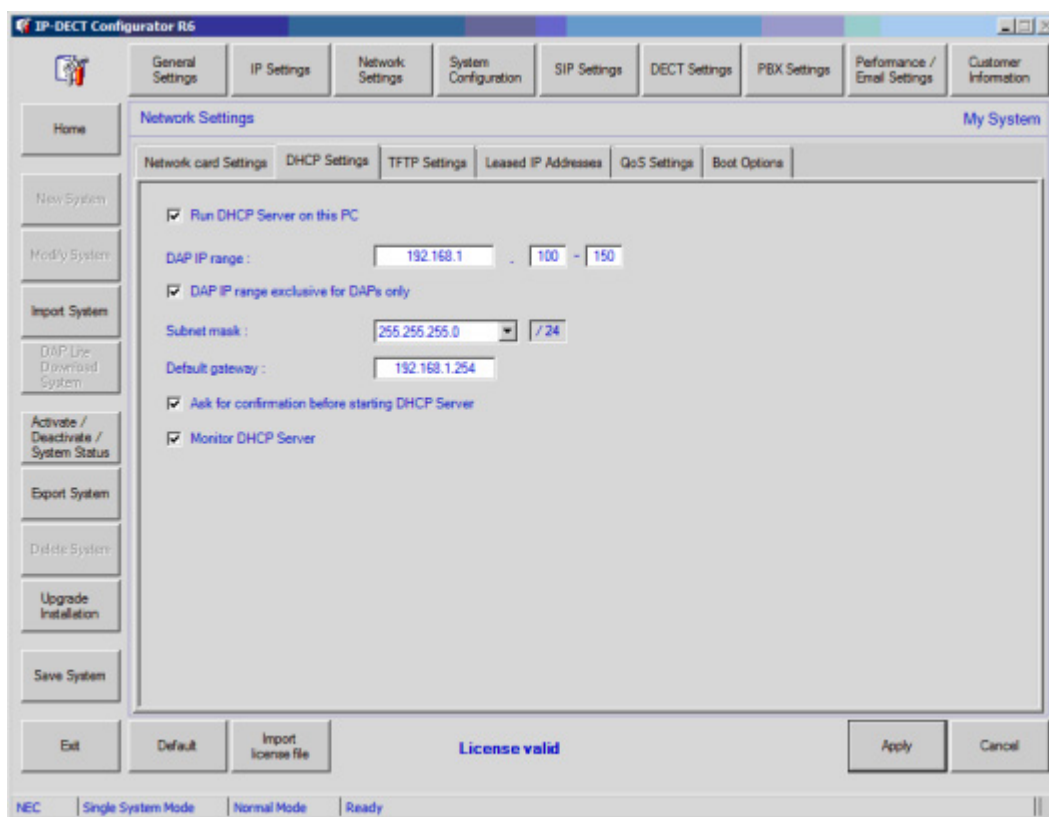



Figure 11-9 DHCP Settings

- **Run DHCP Server on this PC** - If you check this box, the DHCP Server that is installed on your PC for IP DECT will be activated. Note that this DHCP Server accepts DHCP requests from DAPs only if you check the checkbox "**DAP IP range exclusive for DAPs only**". In that case it will ignore other DHCP requests. When you use the DHCP Server it will issue addresses in the range that you specify in the "**DAP IP Range**".

When enabled, it runs as an Application under MS Windows. The settings are stored in the file **dhcpsrv.ini** in the system directory.

- **DAP IP Range** - Specify IP address range that will be issued to the DAPs.
- **DAP IP Address range exclusive for DAPs only** - If checked, the DHCP server will respond to DAP requests only. This is based on the "**Vendor Class ID**" that the DAPs issue when they do a DHCP request.
- **Subnet Mask** - Self explanatory
- **Default Gateway** - Self explanatory
- **Ask for confirmation before starting the DHCP server** - Self explanatory
- **Monitor DHCP Server** - This allows you to monitor the DHCP activity of the built-in DHCP server. You see the results in the System Status Window, which is opened when you click the button "Activate / Deactivate / System Status". See section [3.2 System Status Window on page 10-6](#).

 *The built-in DHCP issues an "unlimited" lease time.*

4.3 Network Settings, Tab "TFTP Settings"

Please click the tab: **TFTP Settings**, see [Figure 11-10 TFTP Settings](#). Now the following fields can be edited:

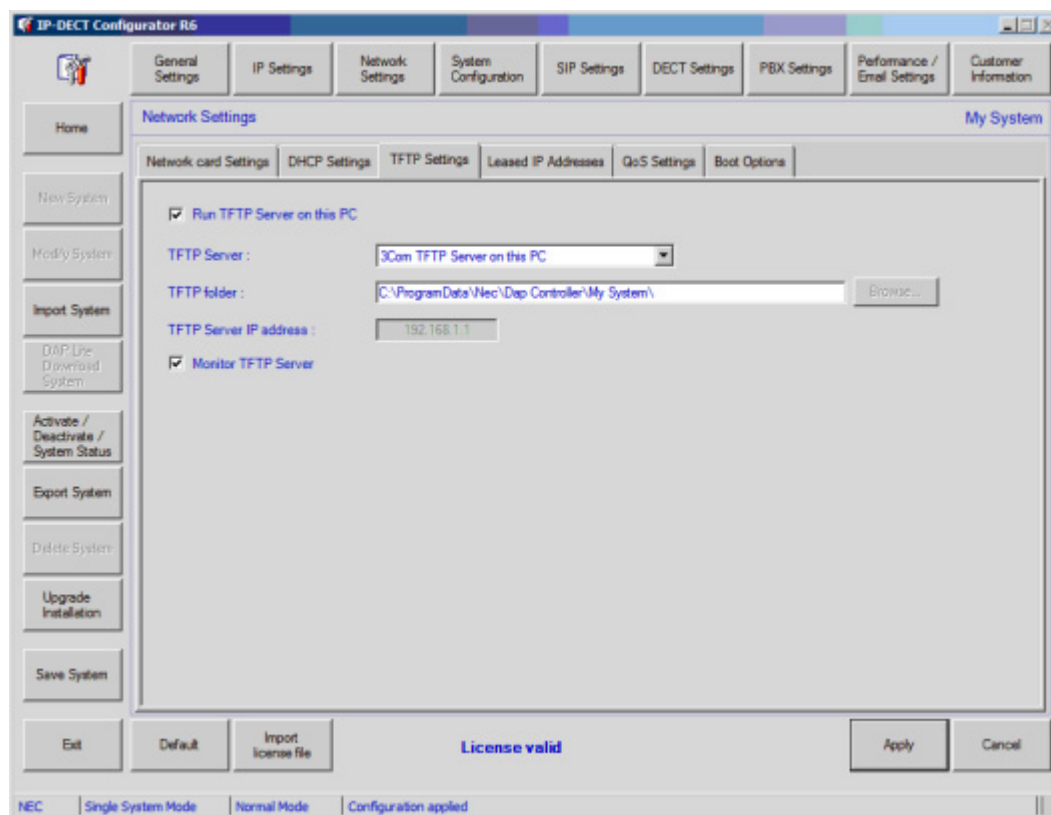


Figure 11-10 TFTP Settings

- **Run TFTP Server on this PC** - If this box is checked, a TFTP Server will be running on your PC as "Service". The settings for the TFTP Server are automatically set correct for your configuration. Note that a TFTP Server is needed when a DAP starts up, unless the configuration file is stored in the DAP.
- **TFTP Server** - Select the TFTP Server that you want to use for the IP DECT Configuration. If you select the "3Com Tftp Server on this PC" it enables the TFTP server that is part of the DAP Controller/Manager software package. When enabled, it runs as "Service" under MS Windows. The settings are stored in the file **3CTftpSvc.ini**.
- **TFTP Folder** - Automatically filled in. The TFTP folder is the folder where all system information is stored. Default folder is: **C:\Documents and Settings\All Users\Application data\Nec\DAP Controller\<system name>**. When you are using Windows 7 or Windows 2008, the directory is **C:\ProgramData\Nec\DAP Controller\<system name>**.
- **TFTP Server IP Address** - This is the IP address of the machine where

the TFTP server is running. When you have chosen to use the built-in TFTP server, you cannot change this IP address because it is the IP address of your machine.

- **Monitor TFTP Server** - This allows you to monitor the TFTP activity of the built-in TFTP server. You see the results in the System Status Window, which is opened when you click the button "Activate / Deactivate / System Status". See section [3.2 System Status Window on page 10-6](#).

4.4 Network Settings, Tab "Leased IP Addresses"

Please click the tab: **Leased IP Addresses**, see [Figure 11-11 Leased IP Addresses](#). Now you see a list of Leased IP addresses in the Built-in DHCP Server.

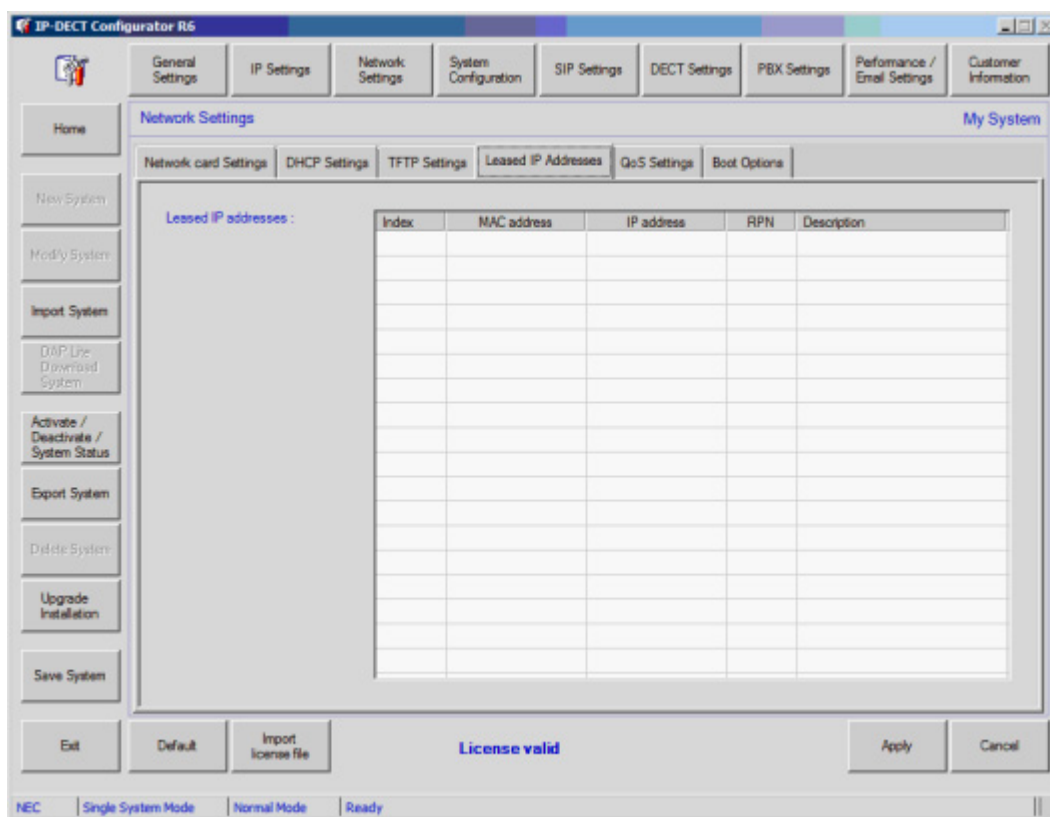


Figure 11-11 Leased IP Addresses

In this window, you can delete/change/add the relationship between MAC addresses and leased IP addresses. You have access to these settings by means of right mouse clicking a line in the Leased IP Addresses window.

4.5 Network Settings, Tab "QoS Settings"

Please click the tab: **QoS Settings**, see [Figure 11-12 QoS Settings](#). Now the following fields can be edited:

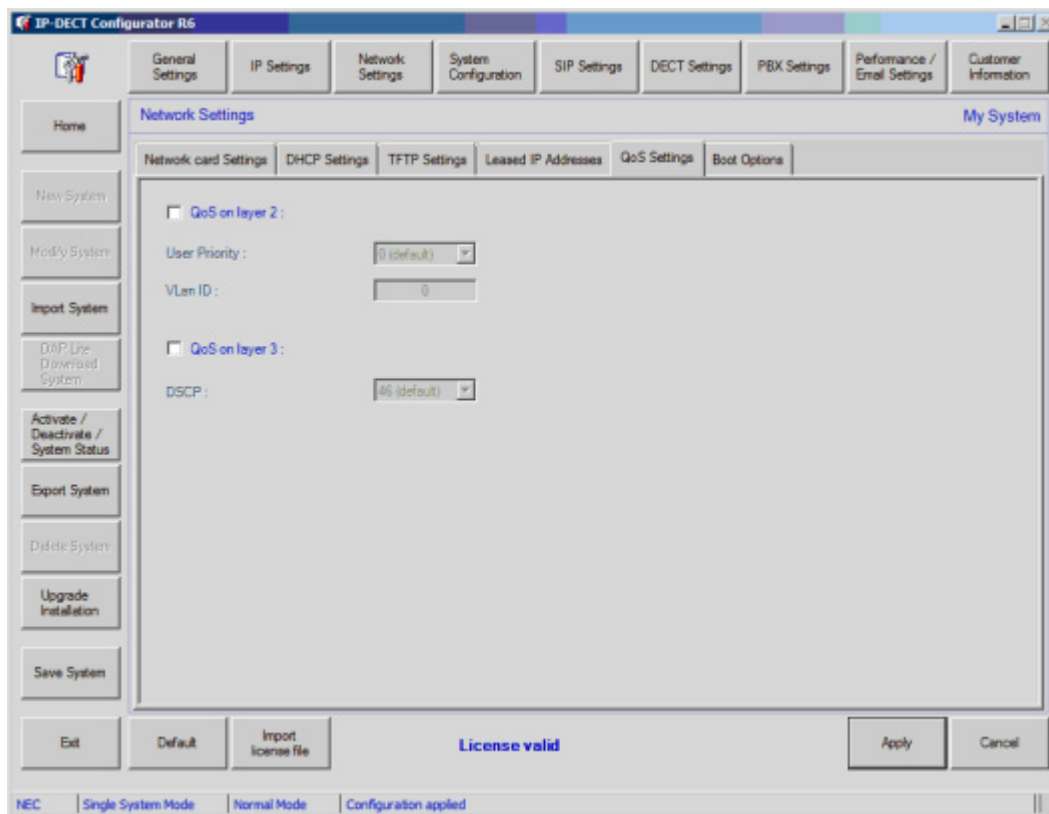


Figure 11-12 QoS Settings

- **QoS on Layer 2** - When you check this checkbox, the IEEE802.1p/q field in the layer 2 data package will be used.
If enabled, you must specify the Priority level for Layer 2 (IEEE802.1p) and the VLAN ID (IEEE802.1Q). The Priority value is a three bit value which must be entered as decimal value 0 ... 7, where 7 is the highest priority.
- **User Priority** - The Priority value is a three bit value which must be entered as decimal value 0 ... 7, where 7 is the highest priority.
- **VLAN ID** - Here you can specify a VLAN ID. Note that "0" means no VLAN specified.
- **QoS on Layer 3** - Here you can enable Quality of Service on Layer 3.
- **DSCP** - If you have enabled QoS on layer 3, you must specify the

DiffServCodePoint (DSCP) value in decimal, in the range 0 ... 63. Note that this is not the AF (Assured Forwarding) class selector/service level or EF (Expedited Forwarding) class selector/service level. This means that if you want to apply the "EF" class selector/service level (53), you should enter the DSCP decimal value "46" (binary 101110).

4.6 Network Settings, Tab "Boot options"

Please click the tab: **Boot Options**, see [Figure 11-13 Boot Options](#). Now the following fields can be edited:

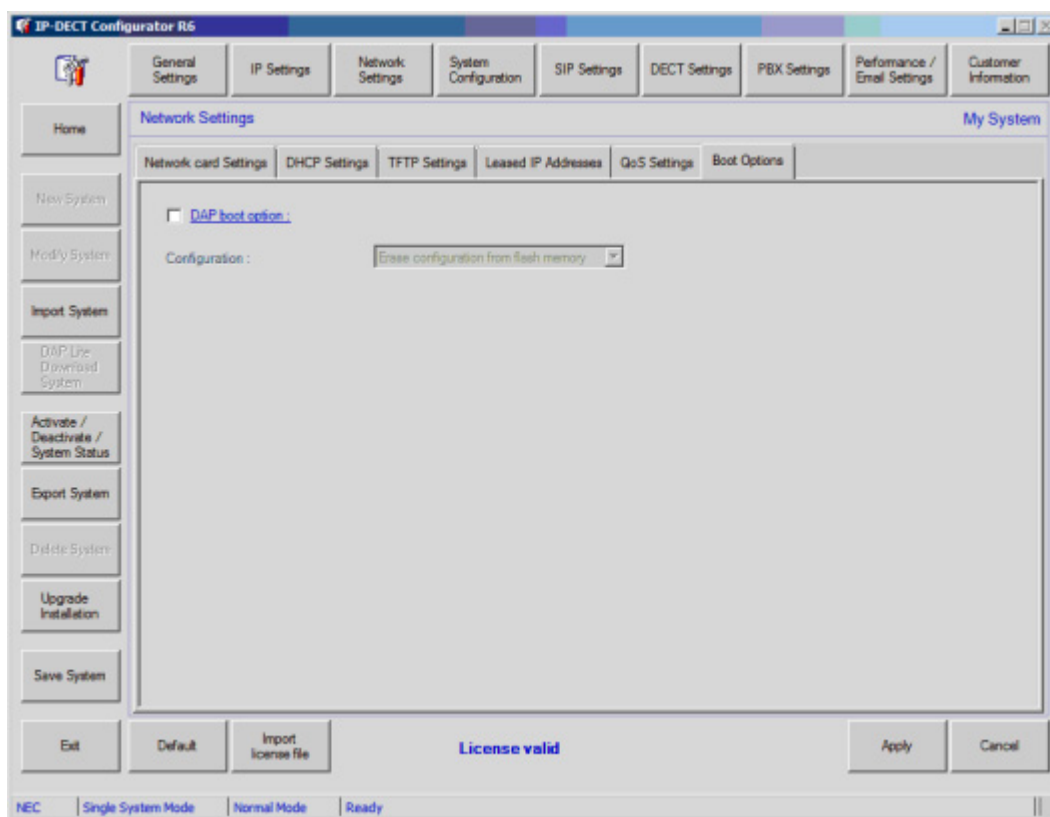


Figure 11-13 Boot Options

- DAP Boot options - This allows you to store the IP address data and Configuration data into Flash memory in the DAP. When stored, a DAP does not need a DHCP/TFTP server anymore. Note that you can "**Store**" or "**Erase**" data.
 - ✎ *Data is stored when you have selected to store data AND when the DHCP server issues an "Infinite" lease time.*

When finished, click **Apply** and continue with clicking button **System Configuration**.

SECTION 5 SYSTEM CONFIGURATION

When you click the **System Configuration** button, [Figure 11-14 System Configuration](#) displays.

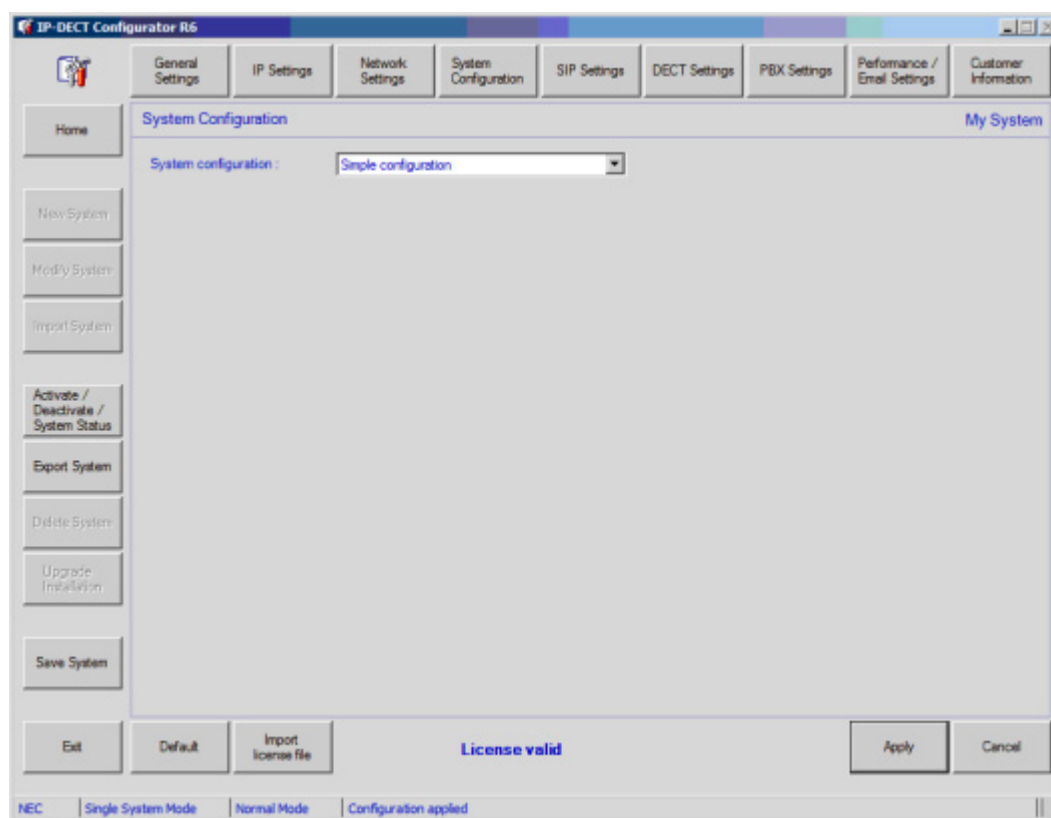


Figure 11-14 System Configuration

You can select the type of system that you want to use. Please consult [Network Configurations](#) for more information. Once you have decided which network configuration you need, continue with the information in this chapter and setup the configuration as needed.

When you click the pull down icon, you will see the following options as shown in [Figure 11-15 System Configuration Options](#).

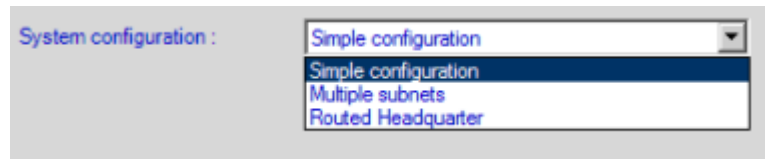


Figure 11-15 System Configuration Options

5.1 Simple Configuration

A simple configuration consists of one network segment. All IP DECT components are in that segment, including the PBX.

5.2 Multiple Subnets

This configuration allows you to have the IP DECT system over various subnets. A number of configurations are possible. You will need this configuration window to setup:

- A Head Quarter with Branch Office
- A Routed Head Quarter with Branch Office
- A Routed Head Quarter with a Routed Branch Office

Consult [Network Configurations](#) for more information.

The window **Multiple Subnets** offers the possibility to specify a certain RPN range per Branch Office Subnet. Note that you should set the RPN range wide enough to allow future system expansion. [Figure 11-16 Multiple Subnets](#) displays.

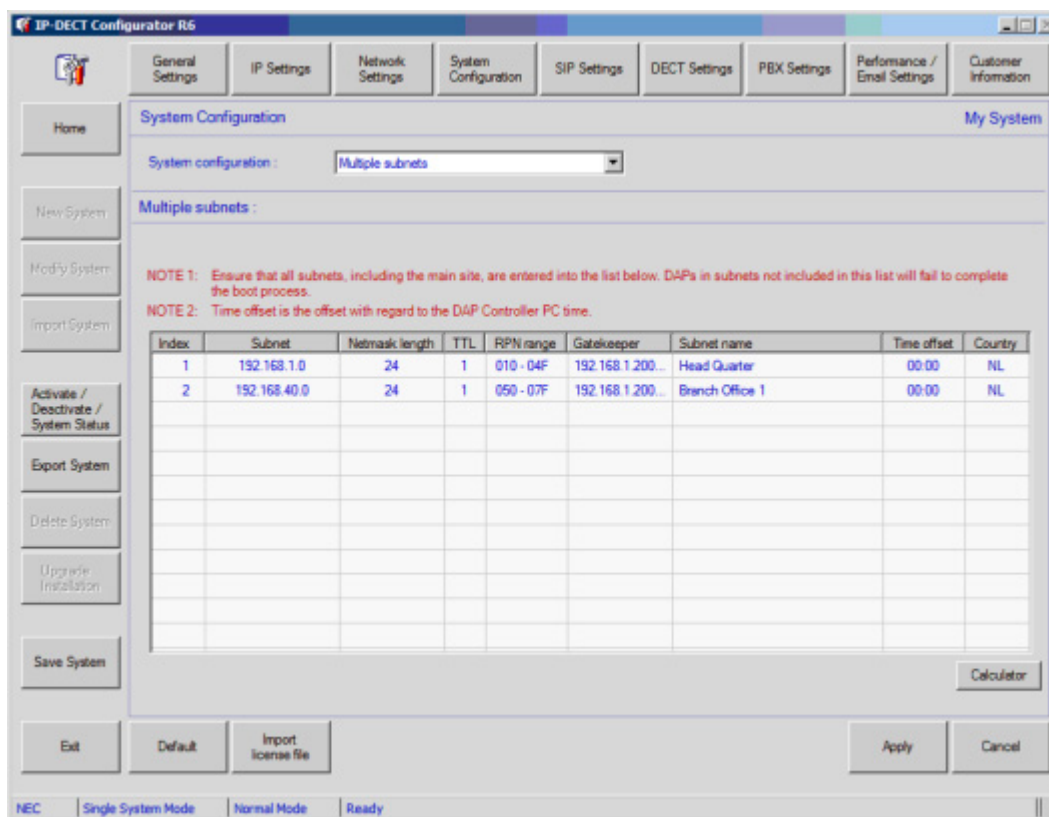


Figure 11-16 Multiple Subnets

In this window you can right mouse click a line in the shown table. Then you can add, edit or delete a Branch Office configuration. The following items must be specified:

- **Subnet** - In almost all configurations, this is the subnet address. It is the first address in the subnet range, e.g. 192.168.1.0/24.

However, note that this subnet can also be an Aggregated Subnet. An "Aggregated Subnet" is a Virtual network definition which determines the network boundaries for an IP DECT Network in which seamless handover is possible AND which is running over more than one IP subnet. An Aggregated subnet is a kind of "virtual" subnet that combines several real subnets.

This is used when your IP DECT system is operational on one location on more than one subnet, with seamless handover.


All DAPs within the Aggregated Subnet allow seamless handover between each other, although they are spread over different real subnets with Routers in between.

So, if you have IP DECT running on more than one IP subnet, where seamless handover is required, you must calculate the Aggregated subnet and fill it in, in this window

Example of an Aggregated Subnet:

There are two subnets in which IP DECT is installed. The Router supports IP Multicast and there is seamless handover between the DAPs in different IP subnets. One subnet is 192.168.1.0/24 and the other is 192.168.4.0/24. The aggregated subnet is 192.168.0.0/21. This covers both subnets.

All subnet addresses outside the Aggregated subnet, will be regarded as Branch Offices.


 *The Aggregated Subnet, together with the Aggregated Subnet Mask are only applicable for IP DECT. So, never use Aggregated Subnet mask on your Network card or other network devices.*

- **Mask Length** - This is the subnet mask length, the number of bits used to identify the network part.


In general, this will be a real netmask length, applicable for one network segment.

Example:

When your subnet mask is 255.255.255.0, it means 24 bits for the network part and 8 bits to identify the host part. So, in this example you must fill in 24.

 *The Mask Length can be the Aggregated subnet mask length. See the bullet above (Subnet) where the Aggregated subnet is explained.*

- **RPN range** - Lowest RPN and highest RPN in this Branch Office.

 *Make sure that you enter all subnet. DAP in subnets, not included in this list will fail to complete the boot process.*

- **Time to Live value** - The Time to Live value is used for the Multicast traffic. If the Time to Live for the Multicast is set to "1", Router(s) will not forward multicast traffic for the associated Multicast Group. If the Time to Live is higher than "1", Router(s) will forward multicast traffic for the associated Multicast Group (depending on settings in a Router).

If you are using an Aggregated subnet (see bullet "Subnet" above), multicast routing is required between the different Subnets and therefore the TTL must be set to a value higher than 1 (advised 32).

If the subnet that you have filled in, is a real subnet, not Aggregated, you must make sure that the Time to Live is always 1.

- **Gate Keeper** - This is the Proxy address for the DAPs in this Subnet.
- **Subnet name** - Can be any given name. It is used to identify the Branch Office.

- **Time Offset** - Self explanatory
- **Country** - This is important to make sure that the frequencies and tones are according to the country requirements

5.3 Routed Head Quarter

In this configuration ([Figure 11-17 Routed Head Quarter](#)), there are more than one network segments in the Head Quarter. The routers in this configuration must forward IP Multicast packages.

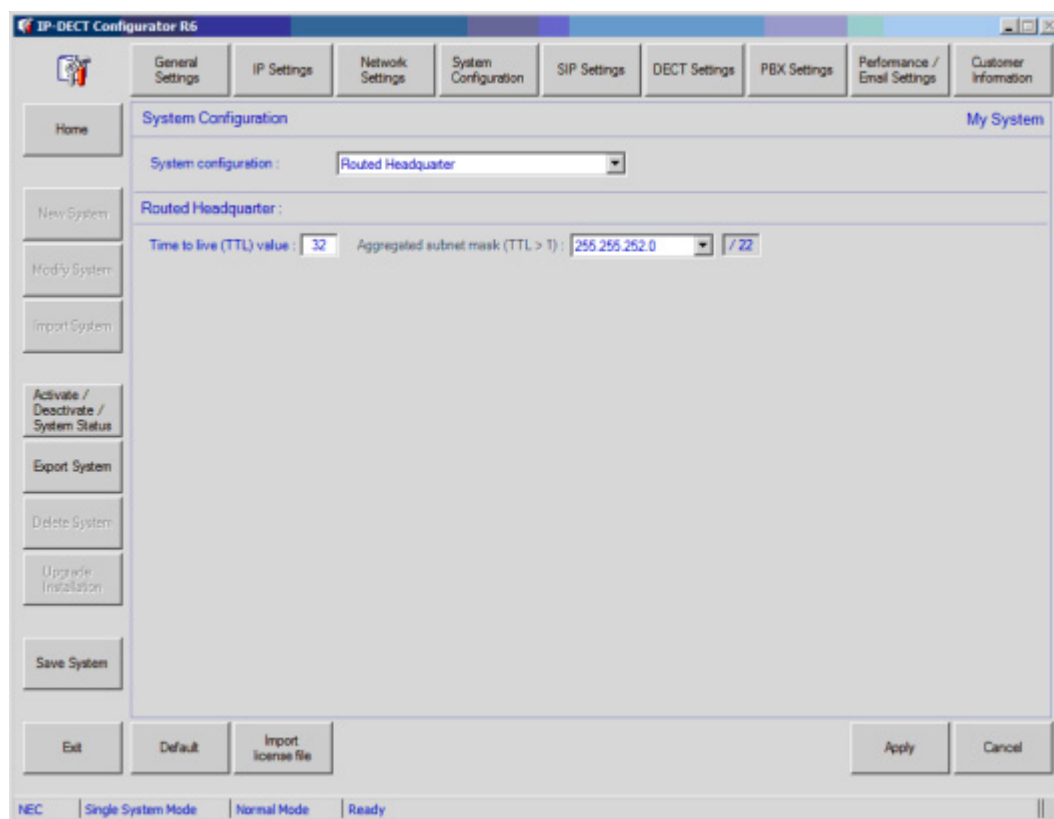


Figure 11-17 Routed Head Quarter

The following settings can be entered/changed:

- **Time to Live value** - The Time to Live value is used for the Multicast traffic. If the Time to Live for the Multicast is set to "1", multicast traffic will not be forwarded by a Router. If the Time to Live is higher than "1", multicast packages might be forwarded by the Router, depending on settings in the Router.

Because you have selected the Router Head Quarter configuration, the Time to Live will always be higher than one. Advised value is 32.

- Aggregated Subnet mask - The "Agg. subnet mask" is the subnet mask for the DAPs to determine the network boundaries for an IP DECT Network in which seamless handover is possible. It should cover the network segments that are connected together using routers that supports IP Multicast. If there are DAPs outside this Aggregated Subnet Mask, the DAP(s) is/are regarded as in a Branch Office.

If the IP addresses are in the same Aggregated Subnet, according to this mask, the system assumes that they are in the same subnet. The term "Aggregated" means that the subnet consists of smaller subnets which are connected over a router, but according to the subnet mask, all behaving as one subnet. This is applicable for the "Routed Head Quarter" network solution either with or without Branch Offices, see [5.3 Routed Head Quarter](#) and [Section 5 Routed Head Quarter with Branch Offices on page 6-8](#).

SECTION 6 SIP SETTINGS

6.1 SIP Settings, Tab "General Settings"

Please click the tab: **General Settings**, see [Figure 11-18 SIP Settings - General Settings](#). Now the following fields can be edited:

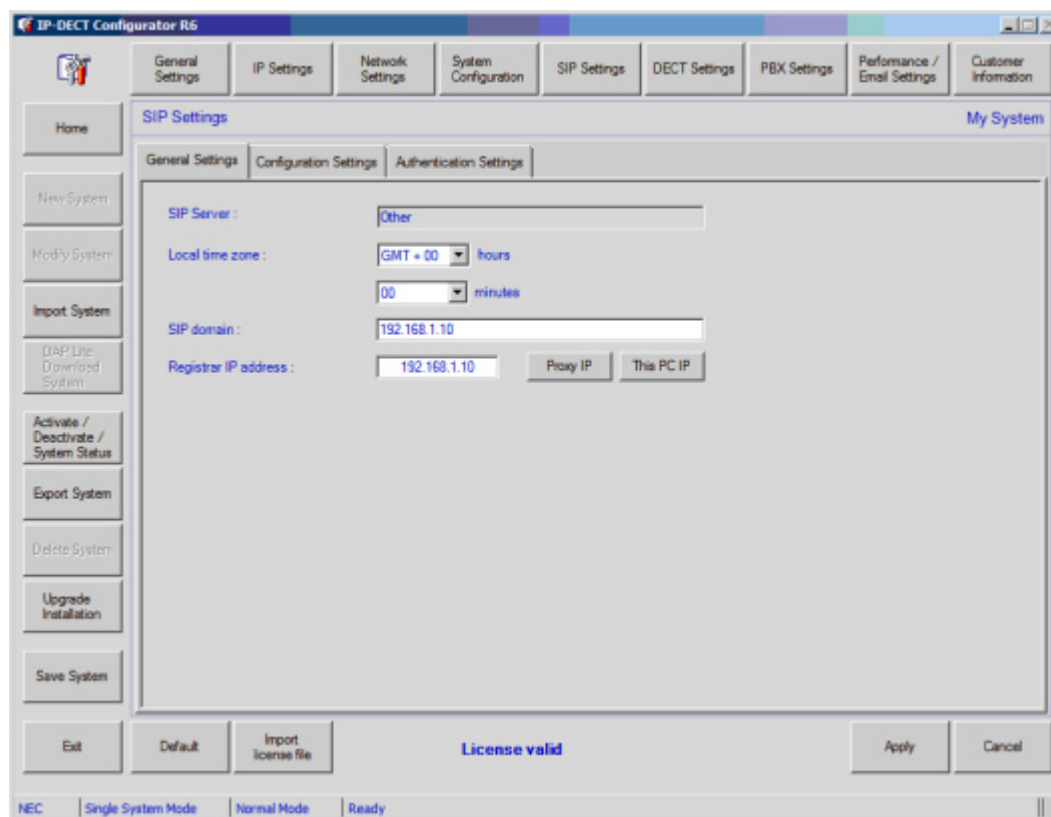


Figure 11-18 SIP Settings - General Settings

- **SIP Server** - This is derived from the setting in Section 9.2 General Settings. You cannot change the SIP server type here.
- **Local time zone** - Specify your time zone. Normally this setting is OK. You only need to change this setting if you want to deviate from the Windows time zone settings.
- **SIP Domain** - Here you must specify the Proxy IP Address (IP4, dotted format) or host name. Note that if you do not specify an address here, the value of "Proxy IP address or host name" is used.

When you have entered a Domain name in the "IP Setting" window (see [Section 3 IP Settings](#)) the Domain names specified there will have priority over the Domain name that you specify here. The Domain name that you specify here is regarded as default Domain name.

- **Registrar IP Address** - IP address of the Registrar server.

6.2 SIP Settings, Tab "Configuration Settings"

Please click the tab: **Configuration Settings**, see [Figure 11-19 SIP Settings - Configuration Settings](#). Now the following fields can be edited:

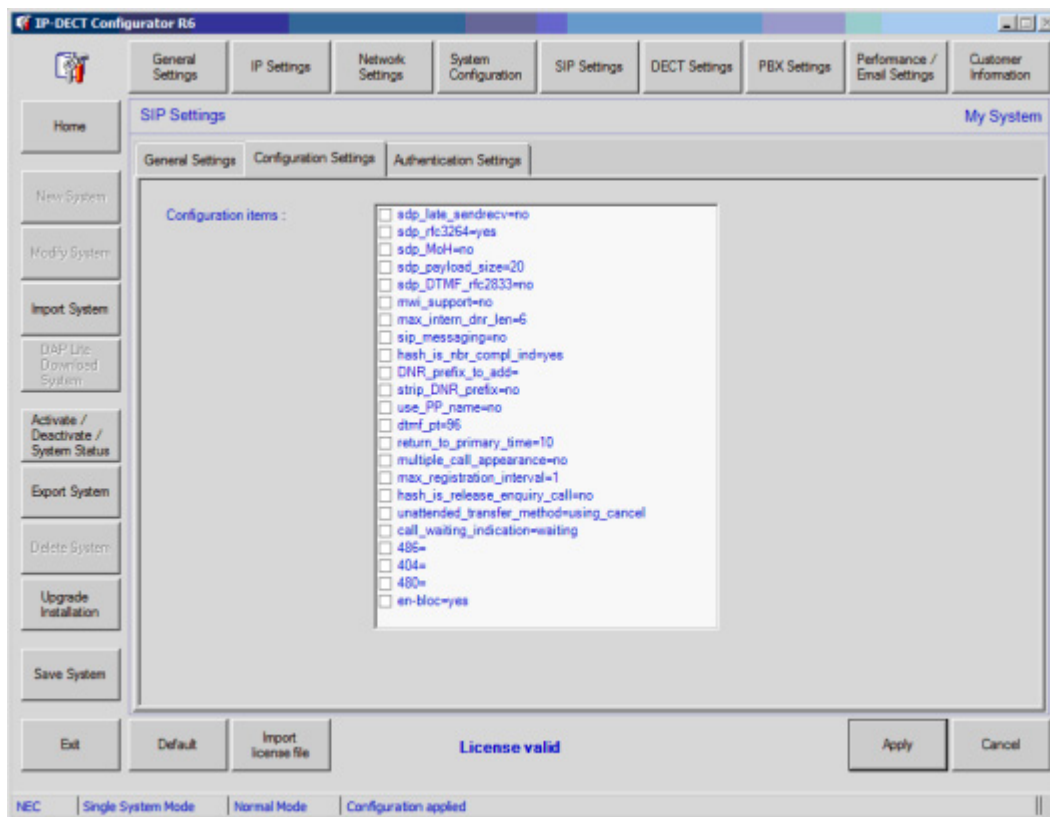



Figure 11-19 SIP Settings - Configuration Settings

The following items can be entered or changed.

- ✎ *The displayed Configuration items depend on the SIP Server selection. In the screen capture and overviews below all possible configuration items are mentioned. For your type of SIP Server, the number of Configuration items may be less because the items that are not relevant for certain SIP server are not displayed.*
- **sdp-late-sendrecv** - Enables the ability of the IP DECT system to issue an initial Invite without SDP (Session Description Protocol) offer.
- **sdp_rfc3264** - Enables "Hold" according to RFC3264.
- **sdp_MoH** - When enabled, no local tone is generated when the IP DECT handset is on "hold" (recvonly mode).
- **sdp_payload_size** - Offered payload size in the SDP (Session Description protocol) offer (in ms). However, generally the proposed payload size of the opposite party is used.
- **sdp_DTMF-rfc2833** - When enabled, DTMF digits are sent according to rfc2833 (in RTP). Otherwise the DTMF digits are sent as SIP "INFO" messages.

- **mwi support** - Message waiting indication supported, yes or no.
- **b2b_ua - Back-to-Back User Agent** - Necessary for an un-attended transfer in an iS3000 SIP server configuration. Must be set to "yes" for iS3000. Must be set to no in all other cases.
- **max_int_dnr_length** - Extension numbers longer than specified here are considered as external numbers. Note that this only applies to numeric extension numbers.
- **sip_messaging** - This option allows you to enable SIP Instant Messaging according to RFC3428.

 *When you enable SIP Instant Messaging, the LRMS messages send from a handset will always be send as SIP Instant Message and therefore not sent via the DAP Controller anymore. This means that when SIP Messaging is enabled, you cannot sent messages to the e.g. the Messenger@Net anymore!*

- **transport protocol** - Use the default protocol UDP. Only for iS3000 other protocols are supported.
- **Maximum Registration Interval=1** - This is the SIP registration interval in minutes. This is not the registration interval per handset.

When there is only one subscription in the DAP, the registration interval for that subscription will be the time specified here. When there are two subscriptions in the DAP, the registration interval for each of the subscriptions will be 2/<time specified>. So it will be 2/1 minute. This means that each subscription will register each two minutes.

- **Hash_is_nbr_complete_ind** - The hash button can be used to indicate number complete or can be used as part of the dialed number.
- **DNR_Prefix_to_add=** - If you want to add digits to the subscribed number, you can specify them here.
- **Strip_DNR_Prefix** - This feature is exactly the same as the "Strip Prefix" check box in the window "IP Settings", see [Section 3 IP Settings](#).
- **Use_PP_name** - If active, the portable name is send as calling line name to the opposite party. Note that this feature is only supported on SIP extensions that supports this functionality. Use this on your own risk.
- **diversion_status** - In this parameter, you must enter the prefix that is used to activate follow-me. The prefix should have been defined in the PBX as well and will be *21 in many countries. When you have entered the prefix, IP DECT knows when a follow-me is set on an extension and will therefore generate the diversion dial tone when going off-hook. Note that this feature only works for the iS3000
- **dtmf_pt** - This parameter allows you to specify the dtmf payload type for RFC2833 implementation. Default is 96. The range is 96 ...127.
- **Return_to_primary** - This parameter is used for a configuration with

Proxy redundancy for SIP. See [SIP Proxy Redundancy on page 14-1](#).


- **multiple_call_appearance** - When the handset is busy and a second call comes in, you will hear a ticker tone and the display shows "waiting <cli>". By means of the * button, you can toggle between the two calls. It behaves in a similar way as having a call on hold. Please note that the SIP Proxy must be able to support multiple call to one extension number as well.
- **Hash_is_release_enquiry_call** - When you are in an enquiry call and you end up on a device like a voice mail server, you cannot hangup the phone without losing your call. In that case you can press the # key to end your enquiry call but keep your original call.
- **Unattended_transfer_method** - There are three options: Proxy, Cancel, Replace. The following options should be chosen for the related PBX types.

Proxy: use for iS3000 type of PBXs

Cancel: most commonly used for a wide range of PBX types.

Replace: used for Alcatel PBX types.

- **Call_waiting_indication** - Here you can specify the call waiting indication text which is displayed when there is a call waiting.
- **486=** - Here you can enter the text that is displayed when the SIP Proxy sends error code 486
- **404=** - Here you can specify the text that is displayed when the Proxy sends error code 404.
- **480=** - Here you can specify the text that is displayed when the Proxy sends error code 480.

 *This window does not show a field for the SIP Proxy address. The SIP Proxy IP address must be specified in the "IP Configuration" window. See [3.4 IP Settings, tab "Proxy IP Configuration"](#).*

In the following bullet list, with hyphenated sub list, the parameters are explained.

6.3 SIP Settings, Tab "Authentication Settings"

Please click the tab: **Authentication Settings**, see [Figure 11-20 SIP Settings - Authentication Settings](#). Now the following fields can be edited:

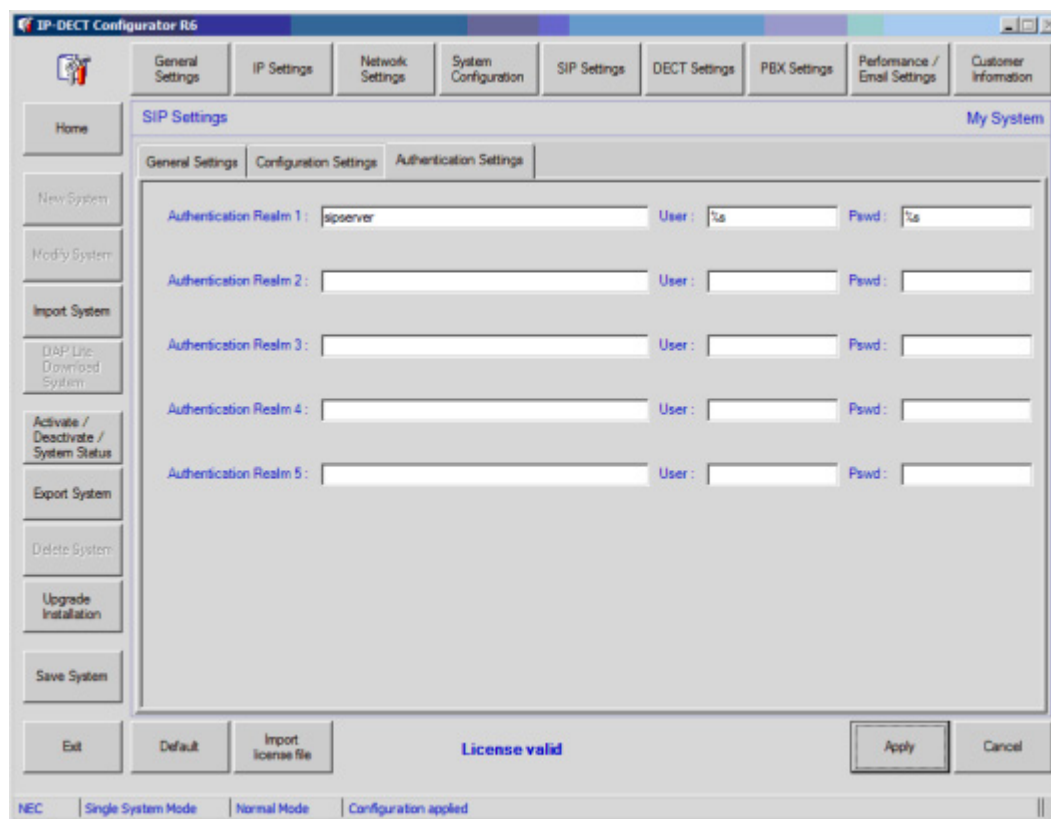



Figure 11-20 SIP Settings - Authentication Settings

○ **Authentication Realm 1 . . . AuthenticationRealm 5**


Up to 5 authentication realms can be specified. Note that if the Proxy requests for authentication, it issues the Realm name. On receiving the Realm name, the IP DECT system compares the received Realm name with the ones in this list. If the Realm name matches, the "username" and the "Password" are sent to the Registrar for authentication check.

A Realm name must be unique, do not enter a same Realm name in more than one field.

 You can do authentication based on the User Name in the handset and on entering a password into the handset. To achieve this functionality, do not enter a Realm name that matches the Realm name of the Proxy. If IP DECT cannot find a Realm name match, it will copy the Realm name that comes from the Proxy back to the Proxy again and will request for handset name authentication. This mechanism works for the G355, G955 and I755 handset only with the latest software in the handset.

○ **User**

The "user" is the name for login on the Proxy/Registrar server.

 You can fill in an actual username OR a %s . When you enter %s , the IP DECT system sends the extension number of the handset making a call. This makes the username extension number specific.

○ **Password**

Password for authentication in the Proxy/Registrar. When you enter %s as password or part of the password, IP DECT converts that to the extension number.

When finished, click **Apply** and continue with clicking button **DECT Settings**.

SECTION 7 DECT SETTINGS

7.1 DECT Settings, Tab "DECT Settings"

Please click the tab: **DECT Settings**, see [Figure 11-21 DECT Settings](#). Now the following fields can be edited:

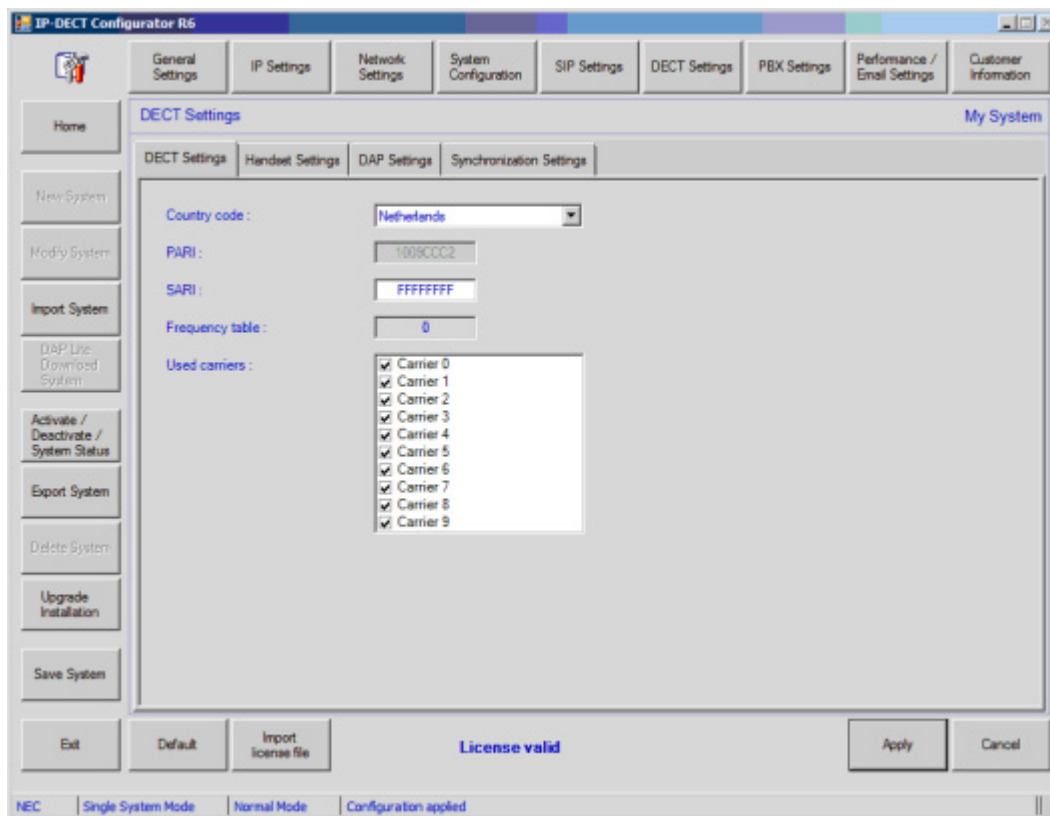



Figure 11-21 DECT Settings

- **Country Code** - The Country code specifies the tone plan for IP DECT and also selects the correct frequency range and transmitter output power.
- **PARI** - Primary Access Rights Identifier. This is the Unique DECT System Identifier. It is an 8 digit hexadecimal string. It is a worldwide Unique Identifier which you should have received together with your DECT system.
- **SARI** - The SARI is the Secondary Access Rights Identifier, which is only needed if you use Multi-Site subscriptions. If you do not use multi-site Subscriptions, leave this field to the default "FFFFFFFF".
- **Frequency Table** - This shows which DECT frequency range is used. This differs per part of the world.
 *You cannot change the setting here, it is a result of the country that you have selected.*
- **Used carriers** - By means of this field you can enable/disable the DECT carriers. Leave all carriers enabled to make sure maximum bandwidth is available.

7.2 DECT Settings, Tab "Handset Settings"

Please click the tab: **Handset Settings**, see [Figure 11-22 DECT Settings - Handset Settings](#). Now the following fields can be edited:

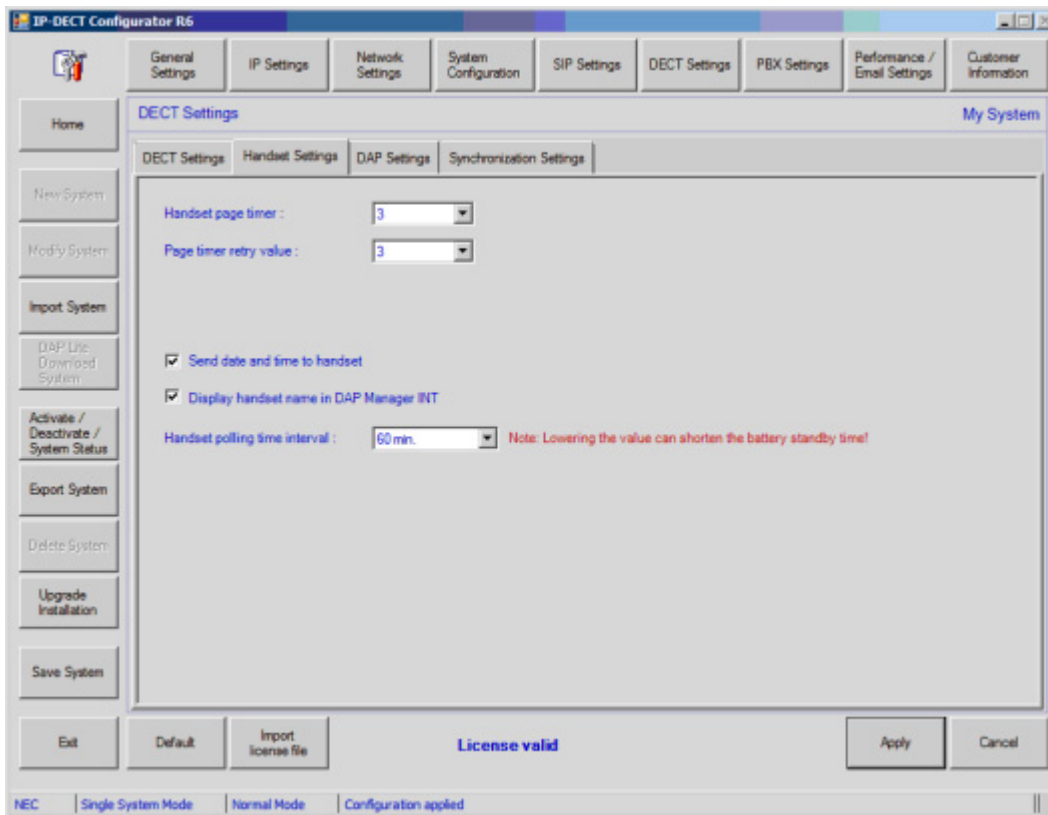


Figure 11-22 DECT Settings - Handset Settings

- **Handset Page Timer** - The Page Timer specifies the time in seconds between two page requests (retries).
- **Page timer retry value** - The Page Retry Value specifies the maximum number of paging retries that are issued, if paging a handset fails.
- **Send date and time to handset** - Self explanatory.
- **Display handset name in DAP Manager INT** - When enabled, the handset name (if present in the handset) will be displayed in the DAP Manager, in the Subscriptions window, in the Comment field. The handset name will be displayed between brackets.
- **Handset Polling time interval** - This is a mechanism to check if the handset is still reachable. Here you specify the polling interval time. If the handset does not respond, it will be switched absent in the IP DECT system.

7.3 DECT Settings, Tab "DAP Settings"

Please click the tab: **DAP Settings**, see [Figure 11-23 DECT Settings - DAP Settings](#). Now the following fields can be edited:

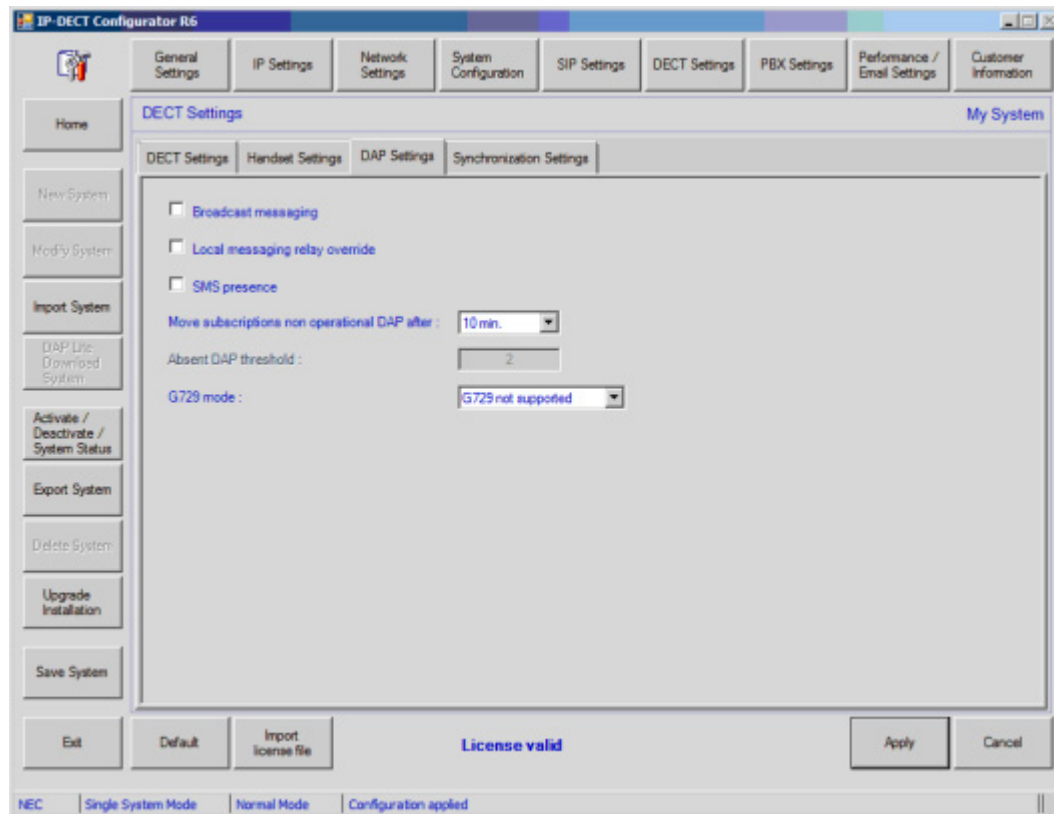


Figure 11-23 DECT Settings - DAP Settings

- **Broadcast Messaging** - This enables broadcast messaging.
- **Local Message relay override** - When "Local Message Override" is not checked, and the TCP/IP DECT Messaging port (default 28001) is in state "Connected" (from e.g. a Messaging device) it is not possible to do handset-to-handset messaging anymore without intervention of an external messaging system. However, if you check the "Local Message override" check box, handset-to-handset messaging remains possible even if the TCP/IP port is in the state "connected". This setting can be required for the messaging functionality of "Business Connect" however, it should not be checked in case of the Messenger@Net.
- **SMS Presence** - Send the absent/present status to dedicated applications via DMLS.

- **Move subscriptions non operational DAP after** - When a DAP is down and the DAP Controller is up- and-running the subscription records from that DAP will be moved to other DAPs. The time interval can be specified here.
- **Absent DAP Threshold** - When the number of absent DAPs is more than 2, the subscription data will NOT be moved to other DAPs.
 - ✎ *This is a fixed system parameter, and cannot be changed.*
- **G729 mode** - The following items can be selected:
 - ☐ **G.729 not supported** = never use G.729
 - ☐ **Use G729 when required** = Setting as in previous versions of IP DECT. G.729 used in case of connection to Branch Office DAPs.
 - ☐ **Preferred use of G.729** = IP DECT will always issue G.729 as preferred codec over G.711.
 - ☐ **Only use G.729** = Do not use this setting!
 - ✎ G.729 voice compression (G7A unit installed in AP300/AP400) could be the answer for applying DECT in networks with limited bandwidth. The downside however is that the voice quality will be less compared to uncompressed voice. But under more demanding circumstances like environments with background noise, the voice quality may become unacceptable if used in combination with G.729. Therefore we advise not to apply G.729 on sites with a background noise.

When finished, click **Apply** and continue by clicking button **PBX Settings**.

7.4 DECT Settings, Tab "Synchronization Settings"

When you see a tab called "Synchronization Settings", it indicates that you have a license for IP DECT in an environment with a lot of metal causing reflections. The license is offers additional functionality to reduce the effects of the reflections. However, it is only available on "Project Base" which means that it has to be installed by special maintenance engineers. Therefore the Synchronization Settings window is not explained here.

SECTION 8 PBX SETTINGS

8.1 PBX Settings, Tab "Handset Sharing"

When you click the **Handset Sharing** tab, [Figure 11-24 PBX Settings - Handset Sharing](#) displays.

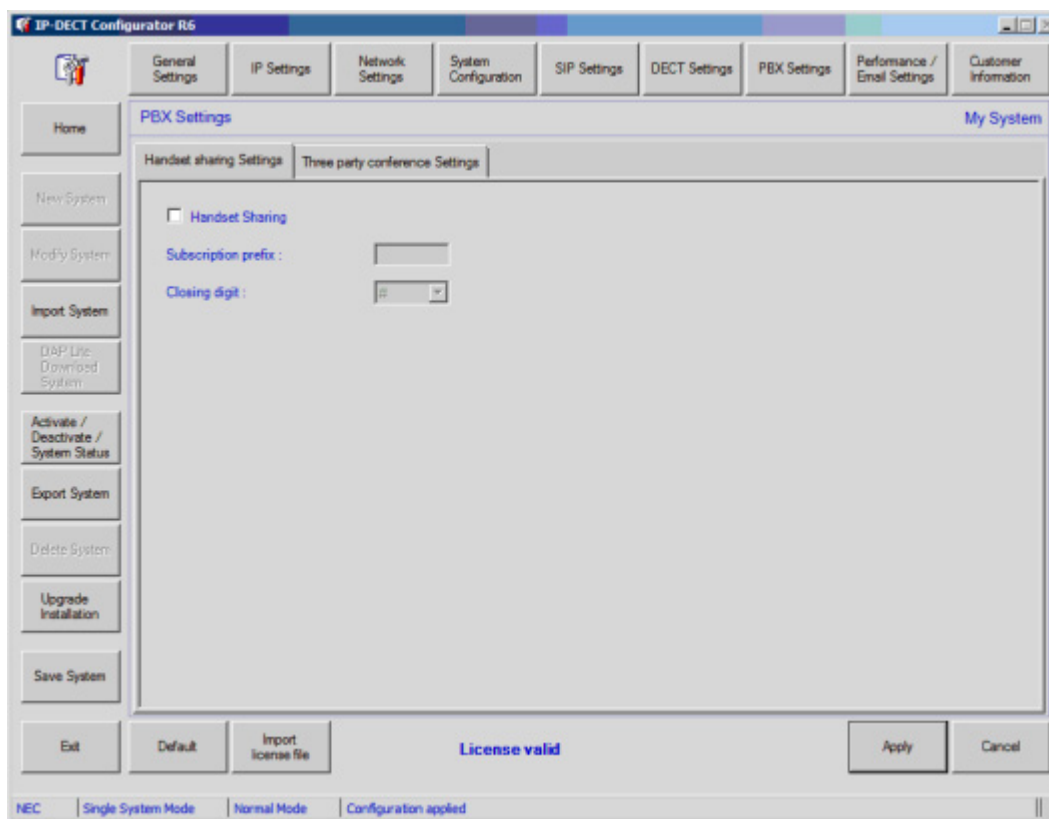


Figure 11-24 PBX Settings - Handset Sharing

- **Handset sharing** - Checking this box, enables Portable sharing, see Chapter 15 "PORTABLE SHARING".
- **Subscription prefix** - First digit(s) of the subscribed number. If the first digit(s) of a subscription matches with the digit(s) defined here, the handset is enabled for portable sharing.
- **Closing digit** - Digit that must be entered on the handset after entering the extension number at login. Default is "#". Normally there is no need to change this digit.

8.2 PBX Settings, Tab "Three party conference Settings"

When you click the **Three party Conference Settings** tab, [Figure 11-25 PBX Settings - Three Party Conference Settings](#) displays.

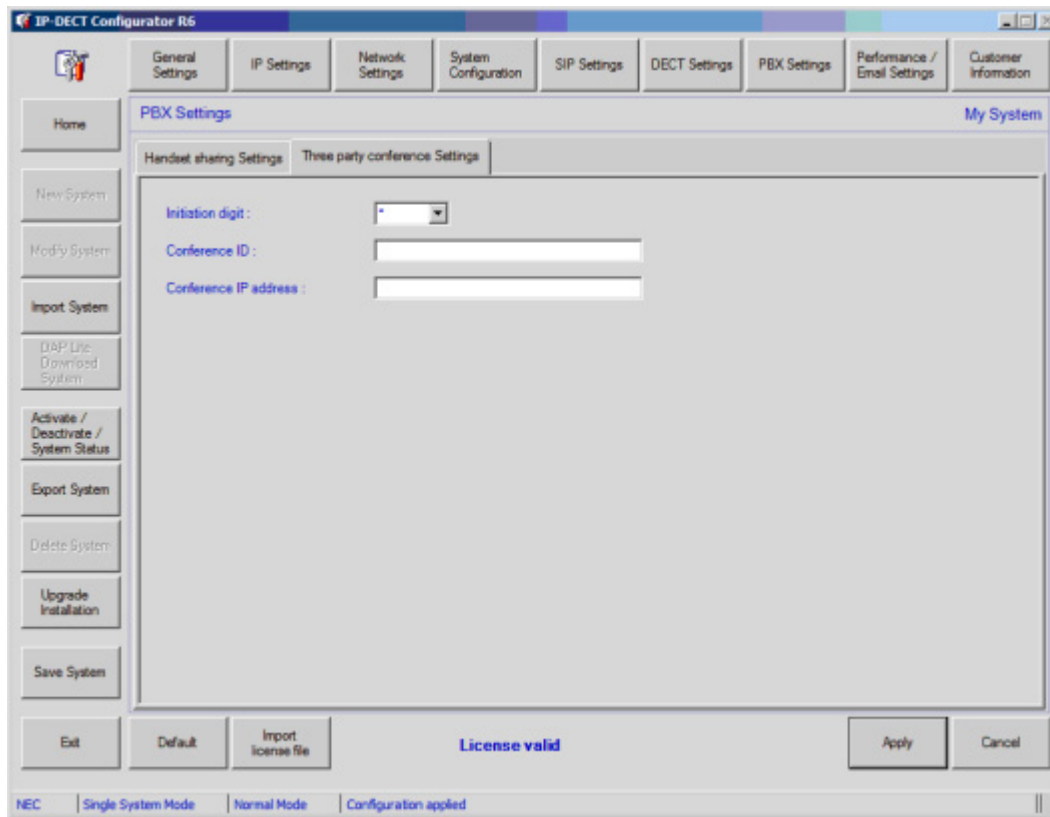


Figure 11-25 PBX Settings - Three Party Conference Settings

The following items can be set/changed:

- **Initiation digit** - Digit that must be dialed to start the three party conference.
- **Conference ID** - The unique ID for the conference.
- **Conference IP Address** - The IP address of the Conference server. (Used for RTP Speech path.)

When finished, click **Apply** and continue with clicking button **Performance / Email Settings**.

SECTION 9 PERFORMANCE / E-MAIL SETTINGS

9.1 Performance / E-mail Settings, Tab "PCR Settings"

When you click the **PCR Settings** tab, [Figure 11-26 Performance Email Settings - PCR](#) displays.

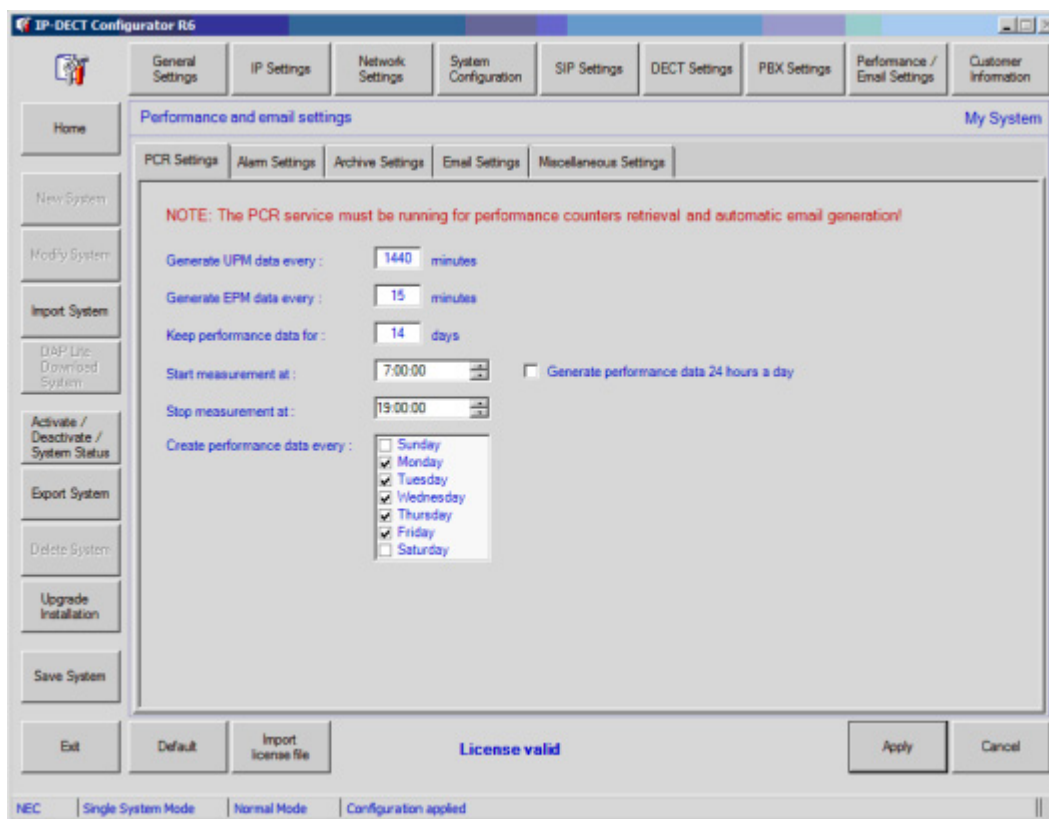


Figure 11-26 Performance Email Settings - PCR

The following parameters are available:

- **Interval UPM generation every** - With this interval, User Performance Measurement files are generated. Default value is 1440 minutes (one day)
- **Interval EPM generation every** - With this interval, Equipment Performance Measurement files are generated. Default value is 15 minutes.
- **Keep Performance data for . . . days** - Number of days that the performance data should be kept on the Hard Disk.
- **Start measurement at** - Each day performance measurement should take place, the performance measurement will start at the time specified here.
- **Stop measurement at** - Each day performance measurement should take place, the performance measurement will stop at the time specified here.

- **Create Performance counters every** - Specify the days that performance counter retrieval should take place.

9.2 Performance / E-mail Settings, Tab "Alarm Settings"

When you click the **Alarm Settings** tab, [Figure 11-27 Performance/E-mail Settings - Alarm Settings](#) displays.

:

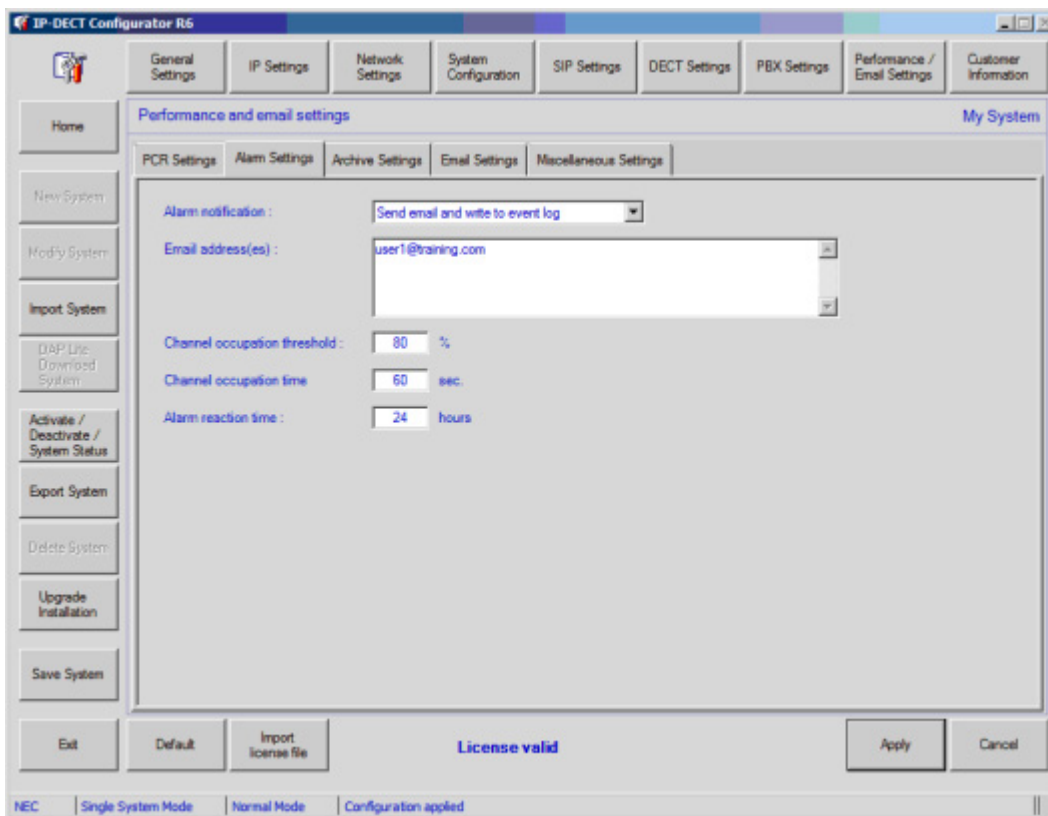


Figure 11-27 Performance/E-mail Settings - Alarm Settings

Emails can be sent automatically when a DAP goes down or when the channel occupation threshold is exceeded for more than a number of seconds. Note that this will only work when the DAP Controller/Manager is up-and-running. The PCR service must be running on the DAP Controller/Manager PC.

- **Alarm Notification** - Alarm notifications can be sent as an e-mail and/or to the **Windows Event Log**. See [Figure 11-28 Alarm Notification](#). Please note that it is possible to convert the events, written to the event log, into SNMP Traps (consult the Advanced Data Manual.).

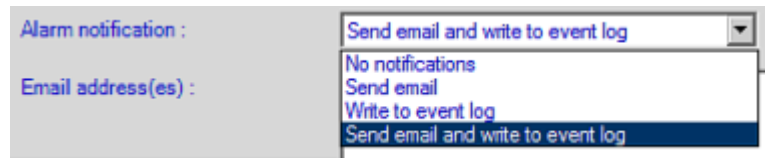


Figure 11-28 Alarm Notification

- **E-mail addresses** - Enter the destination email address(es). Note that you can enter more than one email address. Separate the individual addresses with a ; (semi colon).
- **Channel occupation Threshold** - If the channel occupation is higher than this percentage of the available channels for a specified time period, an email is generated. The threshold is specified in percentage, the time is specified in minutes.
- **Channel occupation time** - If the channel occupation is higher than a percentage of the available channels for a specified time period, an email is generated. The time is specified in minutes.
- **Alarm reaction time** - Time interval for sending emails. Default 24 hours, which means that the time interval between two emails will be 24 hours. Note that this is not a repetition timer. Once an email is send, it will not be repeated anymore.

9.3 Performance / E-mail Settings, Tab "Archive Settings"

When you click the **Archive Settings** tab, [Figure 11-29 Performance/E-mail Settings - Archive Settings](#) displays.

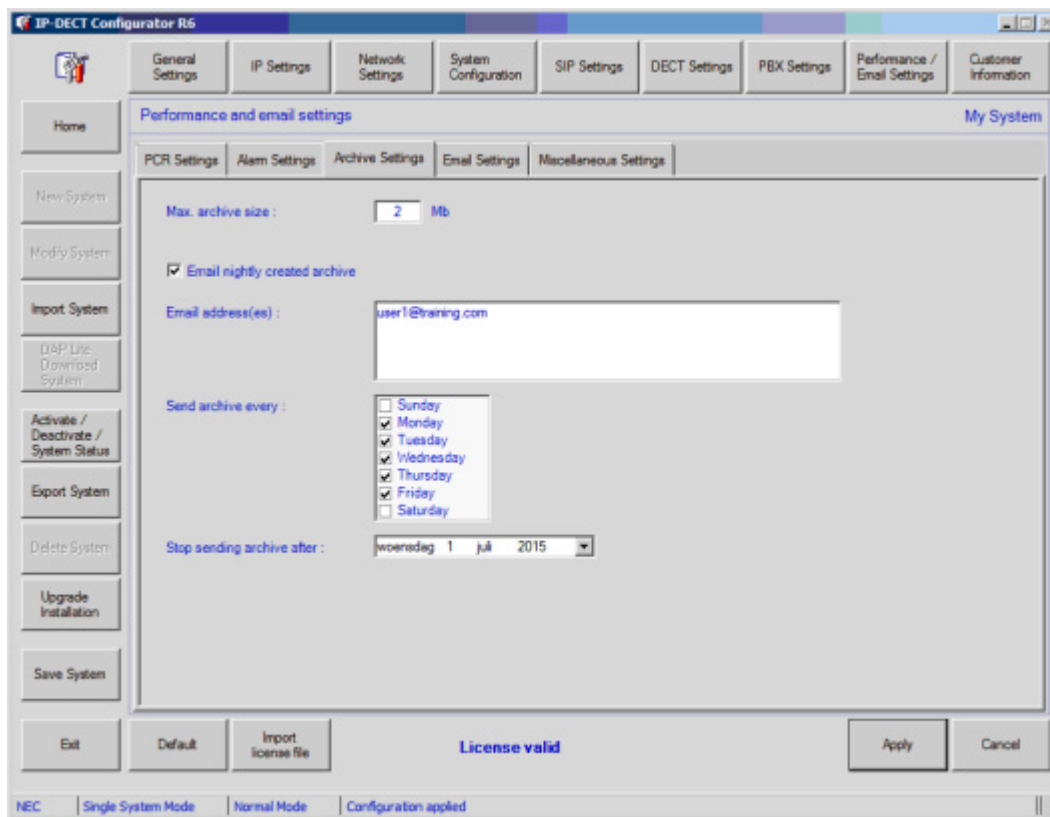


Figure 11-29 Performance/E-mail Settings - Archive Settings

The following parameters can be adjusted:

- **Max. attachment size** - This is the maximum attachment size. If the archive is larger than the size specified here, it will be chopped into pieces of the specified size.
- **E-mail nightly created archive** - This enables automatic sending an email with the nightly created archive file as attachment.
- **E-mail address(es)** - Enter the destination email address(es) as destination for the nightly created archive. Note that you can enter more than one email address separated by ; (semi colon).
- **Send archive every** - Specify the days that the Archive should be send.
- **Stop sending archive after**- After this date, archives are not automatically sent anymore

9.4 Performance / E-mail Settings, Tab "E-mail Settings"

When you click the **E-mail Settings** tab, [Figure 11-30 Performance/E-mail Settings - E-mail Settings](#) displays.

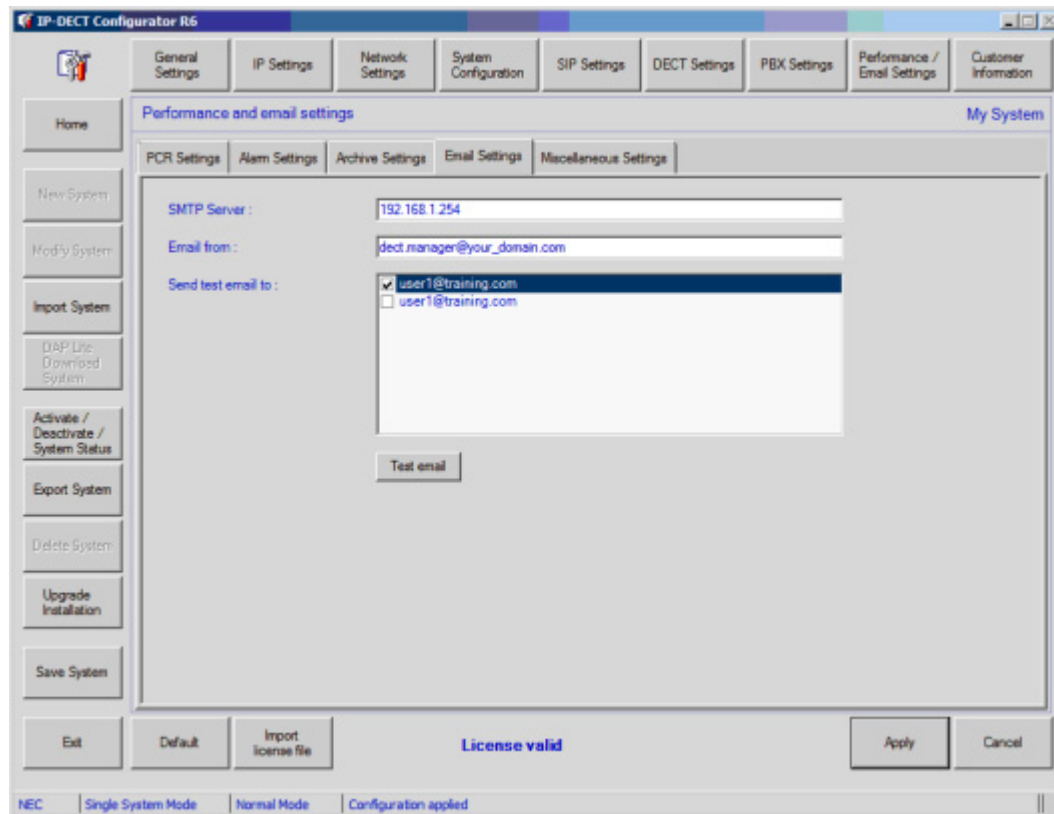


Figure 11-30 Performance/E-mail Settings - E-mail Settings

The following items are available:

- **SMTP Server** - Enter the DNS name or the IP address of the SMTP mail server.
- **E-mail from** - Enter the originators email address. Note that normally the SMTP server does not check the originators email address, which means that you can enter any email address here.
- **Send test e-mail to** - Select the addresses to which an e-mail should be send. Please note that these addresses come from the Alarm Settings and Archive settings.
- **Test e-mail** - Click this button to send an email to the addresses that have checked checkboxes.

9.5 Performance / E-mail Settings, Tab "Miscellaneous Settings"

When you click the **Miscellaneous** tab, [Figure 11-31 Performance/E-mail Settings - Miscellaneous Settings](#) displays.

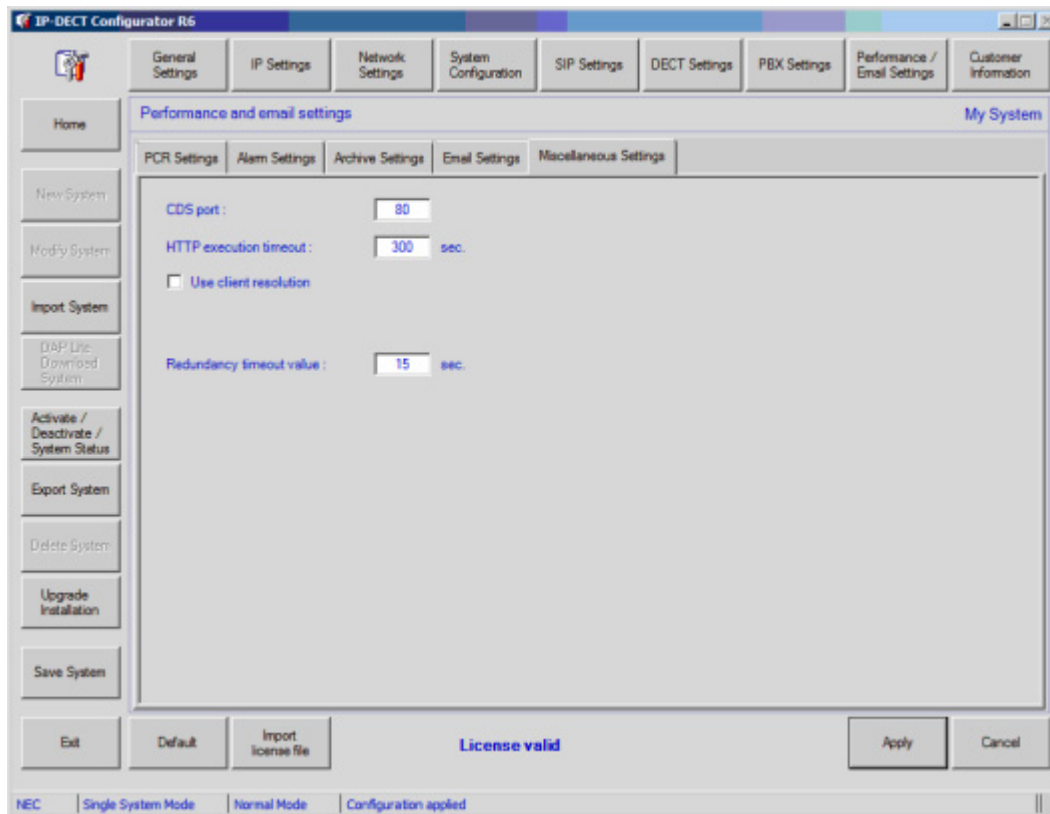


Figure 11-31 Performance/E-mail Settings - Miscellaneous Settings

- **CDS port** - Here you can change the port number of the CDS. The CDS takes care of showing the WEB pages. When you change the port here, the port of the WEB server for CDS is changed. This means that you must enter the new port number in the URL that you use to reach the WEB page.
- **HTTP execution time out** - This is a guarding timer for the ASP scripts. E.g. if the ASP web pages try to send an archive and it takes longer than the time specified here, it will be terminated.
The time is specified in seconds.
- **Use client resolution** - If you check this box, you cannot scroll anymore through lists but the available information is chopped up into pages. You can select pages using tabs. If this box is unchecked, information is

presented in a way that you can scroll through it using the scroll bar. Note the information is still chopped up into pages, but the pages contain (much) more information.

- **Redundancy Time out value** - This value is the polling time from the DAPs to the DAP Controller. When it times out, the DAPs will try to connect to another redundant DAP Controller

When finished, click **Apply** and continue by clicking button **Customer Information**.

9.6 Customer Information

When you click the **Customer** button, [Figure 11-32 Customer Information](#) displays.

The screenshot shows the 'IP-DECT Configurator R6' application window. The 'Customer Information' tab is selected in the top menu bar. On the left, there is a vertical toolbar with buttons: Home, New System, Modify System, Import System, DAP Lic. Download System, Activate / Deactivate / System Status, Export System, Delete System, Upgrade Installation, Save System, Exit, Default, and Import license file. The main area contains the following fields:

- Customer name : [text box]
- Address : [text box]
- Contact person : [text box]
- Phone number(s) : [text box]
- Email : [text box]
- Comments : [text area]
- System created on : 1-1-0001 0:00:00
- Last modified on : 1-1-0001 0:00:00

At the bottom, there is a 'License valid' status indicator and 'Apply' and 'Cancel' buttons. The bottom status bar shows 'NEC | Single System Mode | Normal Mode | Configuration applied'.


Figure 11-32 Customer Information

In this window, you can enter customer information. It is only for administrative purposes. The system does not use this information.

When finished, click **Apply**. Continue with [9.7 Save System and Start System](#).

9.7 Save System and Start System

When you have finished with setting up the configuration, you must do the following:

 *If you use another TFTP server or DHCP server than the build in TFTP/DHCP server, consult [Using Other TFTP Server on page 15-1](#) first.*

1. Click the **Save System** button (left side of the DAP Configurator window), to save the changes you have made.
2. If the firmware file is not yet in the TFTP directory, copy the firmware file(s) **4910bvxx.dwl (AP300)** and/or **4920bvxx.dwl (AP400)** into the TFTP directory. When having AP400, also copy the **Loader** file **49920111.dwl** into the TFTP directory. This directory will normally be the following directory: **C:\Documents and Settings\All Users\Application Data\Nec\DAF Controller\<system name>**.

When you are using Windows 7 or Windows 2008, the directory is:
C:\ProgramData\Nec\DAF Controller\<system name>.

3. Activate the system, using the **Activate / Deactivate / System** Button.
4. Check the **System Status** in the System Status Window.
5. Check that the DAPs become operational.

For more information, see [Section 3 System Control Section on page 10-5](#).

9.8 Finishing Advice

When the system is running correctly, generate a **visadm.txt** file (in the WEB Page **<http://<DAP Controller IP Address>/cds/perfform.aspx>**) and analyze the file, using the **SyncAnalyser** tool.

If necessary, re-arrange the synchronization structure.

9.9 License Handling

9.9.1 Install a New License File

You can easily install a new license file by means of **Import license file** which is available at the bottom side of the DAP Configurator. See [Figure 11-33 Import License](#).

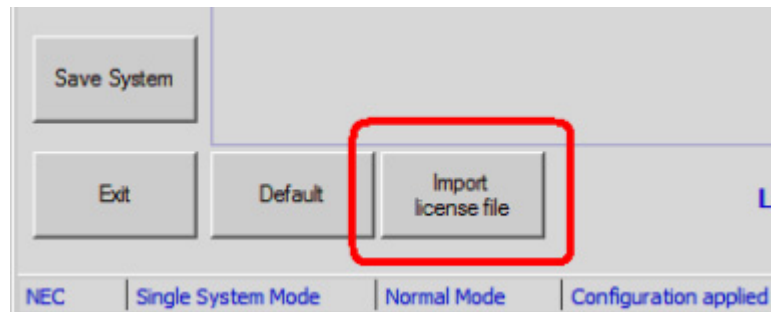


Figure 11-33 Import License

- ✎ The license file should have a file extension: **.txt**

9.9.2 Reading out the Licenses

You can read out the license data by means of the **License** button in the **General Settings** window. See [Figure 11-34 License](#).

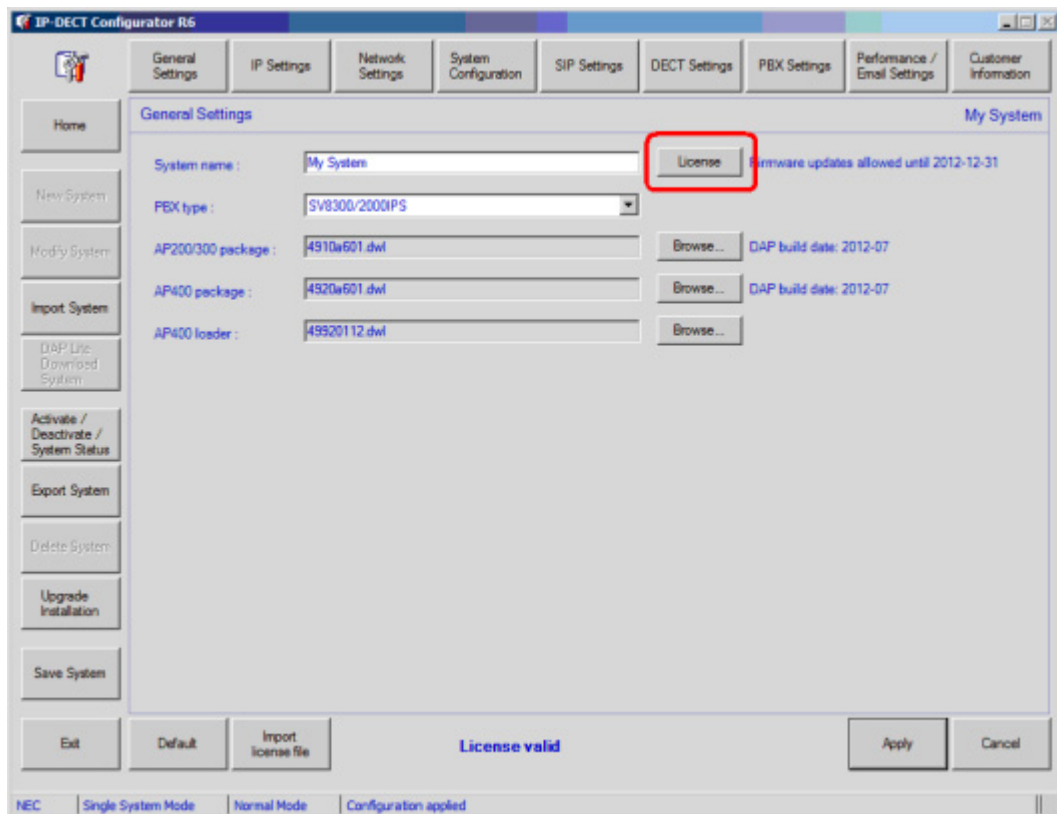


Figure 11-34 License

When you click the button, you will see the licenses presented as shown in [9.9.3 License Information Window](#).

9.9.3 License Information Window

[Figure 11-35 License Information Window](#) provides two examples of the License information window.

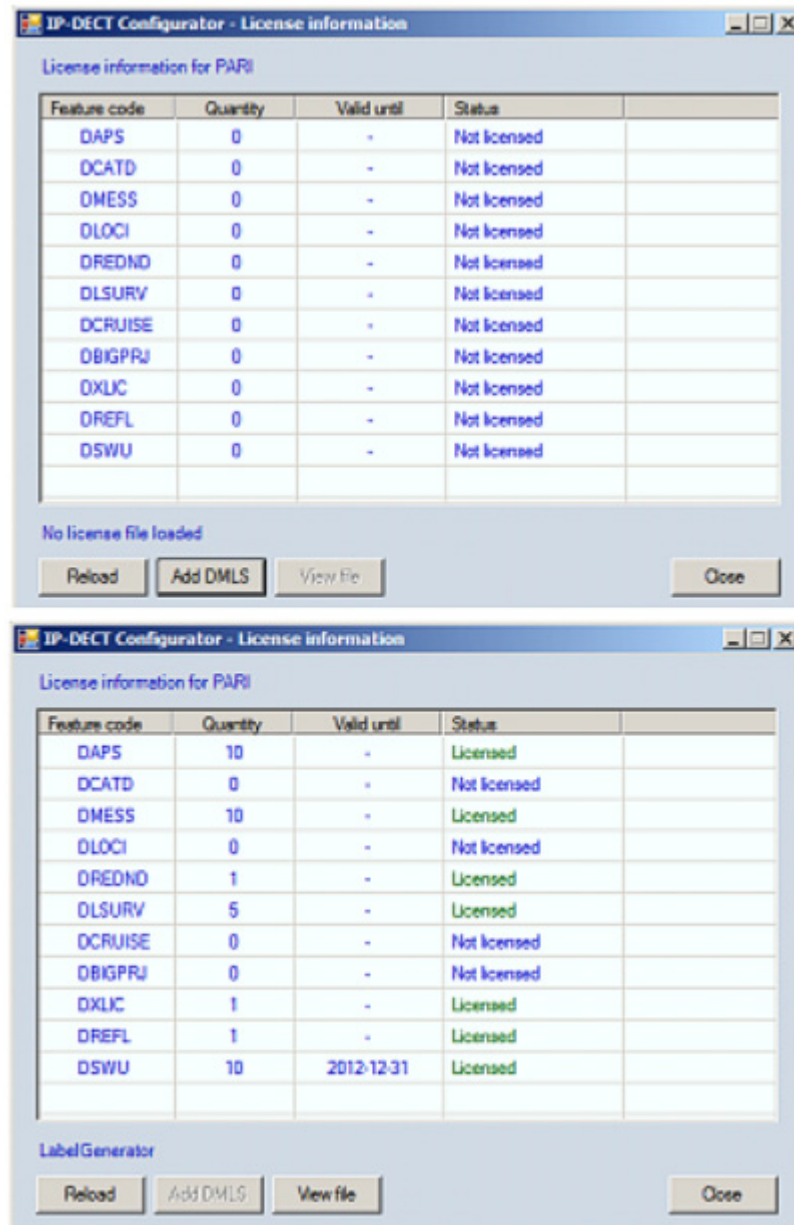


Figure 11-35 License Information Window

Table 11-1 License Items provides an explanation of the various license items shown in Figure 11-35 License Information Window.

Table 11-1 License Items

Item	Explanation	License Type
DAPS	Number of DAPS allowed	Number of DAPS in steps of 10
DCATD	<i>For future use:</i> CAT -iq Data allowed	0=no 1=yes
DMESS	DECT Messaging allowed on DMLS	Number of DAPS in steps of 10
DLOCI	DECT Messaging and Location allowed on DMLS	Number of DAPS in steps of 10
DREDND	DAP Controller Redundancy (Central DAP Controller)	0=no 1=yes
DLSURV	Survivability (Local DAP Controllers)	0...10
DCRUISE	Special functionality for Cruise Lines	0=no 1=yes
DBIGPRJ	Special functionality for configurations with more than 256 DAPS in one system with seamless handover.	0=no 1=yes
DXLIC	License for using the NEC ATEX (ATmospheresEXplosives) handsets.	0=no 1=yes
DREFL	Reflective environment license. Allows additional settings for reflective environments.	0=no 1=yes
DSWU	DECT Software upgrade license.	Number of DAPS + expiry date

- ✎ Please note that the licenses DAPS, DMESS, DLOCI and DSWU are based on the number of DAPs.
- ✎ Licenses that are based on the number of DAPs must always have the same number of DAPs as licensed in the first item: DAPS. So, if the number of DAPS is 40, the other licenses (if required) that are based on the number of DAPs should be forty as well. They cannot be less than the number of DAPs.
- ✎ When you have a DMLS license for the DAP Controller License mechanism, the license information is automatically copied into the DMLS, when the DMLS starts up (make sure that you have the latest DMLS.)

When you have a DMLS license for the DMLS itself, (to import into the DMLS directly), you can enter that license into the DAP Controller, by means of the button **Add DMLS**.

THIS PAGE INTENTIONALLY LEFT BLANK

Redundancy (General)

SECTION 1 **GENERAL**

Redundancy in IP DECT can be necessary for the following functions:

- ☐ Voice
- ☐ Roaming
- ☐ Messaging

It is important to determine which type of redundancy is required for your system.

In the following sections the redundancy for the functions is explained.

1.1 Voice Redundancy

To make voice connection redundant, Proxy Redundancy is required.

Proxy redundancy has already existed for many years. When a SIP connection between a DAP and a Proxy goes down or fails, the DAP can select another (redundant) Proxy. In the DAP, you can set up a list of Proxy IP addresses with Priorities. For more information about this type of redundancy, please consult [SIP Proxy Redundancy on page 14-1](#).

1.2 Roaming Redundancy

Handset roaming requires that the subscription record of the handset is always reachable in one of the DAPs in the network. If not, the handset is not usable. In two cases, roaming redundancy can be required:

- DAP goes down - When a DAP goes down, the subscription records in such a DAP are not reachable anymore, and therefore the Handsets having a subscription record in that DAP, will not be operational anymore. When the DAP

Controller is up-and-running in the network, it will take care that the subscriptions records will be put in another DAP (after a short time). From that time on, the handsets are operational again. This offers a high availability of the handsets. But, this means that the DAP Controller must be up-and-running. To make this mechanism even more reliable, the DAP Controller can be made redundant. (See [DAP Controller Redundancy on page 13-1](#)).

- Moving between Branch Office locations - In a Branch Office configuration, the subscription record (in a DAP) moves with the handset to another Branch Office (when the handset moves to the other Branch Office). The DAP Controller takes care of this functionality. To make this mechanism more reliable, the DAP Controller can be made redundant. (See [DAP Controller Redundancy on page 13-1](#)).

1.3 Messaging Redundancy

DECT Messaging (LRMS) always goes via the DAP Controller. When there is only one DAP Controller, it is a single point of failure for messaging. In certain environments, messaging is an important functionality and must be highly reliable. Therefore it can be necessary to have a Redundant DAP Controller configuration. The DAP Controller can be made redundant, by means of adding second DAP Controller in the IP DECT System.

When LRMS is required in individual Branch Offices, you can install a Local DAP Controller in the Branch Office, that takes care of the DAP Controller functionality in case the connection to the Central DAP Controller(s) fail. Each Branch Office can have its own Local DAP Controller. ([DAP Controller Redundancy on page 13-1](#)).

DAP Controller Redundancy

SECTION 1

 *DAP Controller Redundancy is licensed!*

GENERAL

DAP Controller Redundancy means that you will have one or more redundant DAP Controller(s) in your network. If the main DAP Controller goes down, another DAP Controller takes over the functionality.

Please note the following various possible configurations.

- ☐ Central DAP Controllers - A Central DAP Controller controls the entire IP DECT system, so the main site and, if present, Branch Offices. As Central DAP Controller, there is always a Primary DAP Controller and there can be a Secondary DAP Controller for redundancy. As a matter of fact, the Secondary DAP Controller will take over when the Primary fails or is not reachable anymore.

The maximum number of Central DAP Controllers is two.

For additional redundancy in Branch Office locations, there can be Local DAP Controllers, see next bullet.

- ☐ Local DAP Controllers - A local DAP Controller is located in a Branch Office, and controls its own Branch Office in case the Central DAP Controller(s) cannot be reached anymore.

A Local DAP Controller never controls another Branch Office other than its own. So, it operates in a Survivability mode for the Branch Office.

The maximum number of Local DAP Controllers is 10.

The distinction between a Central and a Local DAP Controller is determined by the configuration that you setup in the "DAP Configurator" in the Primary DAP Controller.

In [Figure 13-1 DAP Controller Redundancy Configuration](#), you see the DAP Configurator screen in which you must setup the configuration. Please note that you assign the Central and the Local DAP Controllers here with the associated priority.

So, for the Central DAP Controller(s), you specify a Primary (index 1) and if required, a Secondary (index 2) DAP Controller.

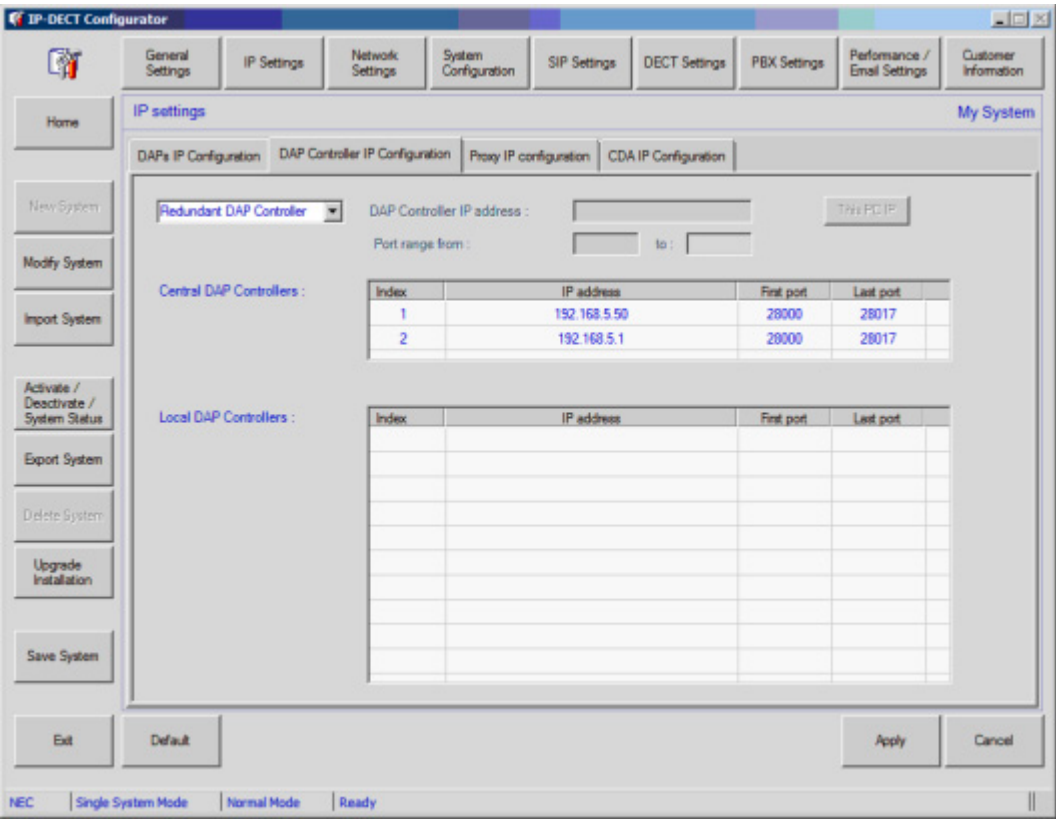


Figure 13-1 DAP Controller Redundancy Configuration

A special "service" (Redundancy Service) in the DAP Controller takes care of the redundancy tasks.

All configuration actions are done by means of the DAP Configurator in the Primary DAP Controller. When done, the configuration must be exported from the Primary to the other DAP controller(s)

SECTION 2 **DAP CONTROLLER REDUNDANCY IN MESSAGING CONFIGURATION**

DAP Controller Redundancy in a messaging configuration, means that you have two DAP Controllers and two DMLS services. Please note that in this description, we assume that we have Central DAP Controllers (Primary and Secondary), and no

Local DAP Controllers. However, there could be a Local DAP Controller as well. (The characteristics of the Local DAP Controller are explained in one of the following subsections.).

The Messaging Application could have been duplicated as well, or it can have an IP connection to each of the DMLS services.

In [Figure 13-2 Example of a Redundant IP DECT configuration with Messaging](#), there is only one IP DECT system, with two DAP Controllers, the Primary and the Secondary. As you can see, there are two options: one messaging system with two connections to the DMLS services, or duplicated Messaging Applications.

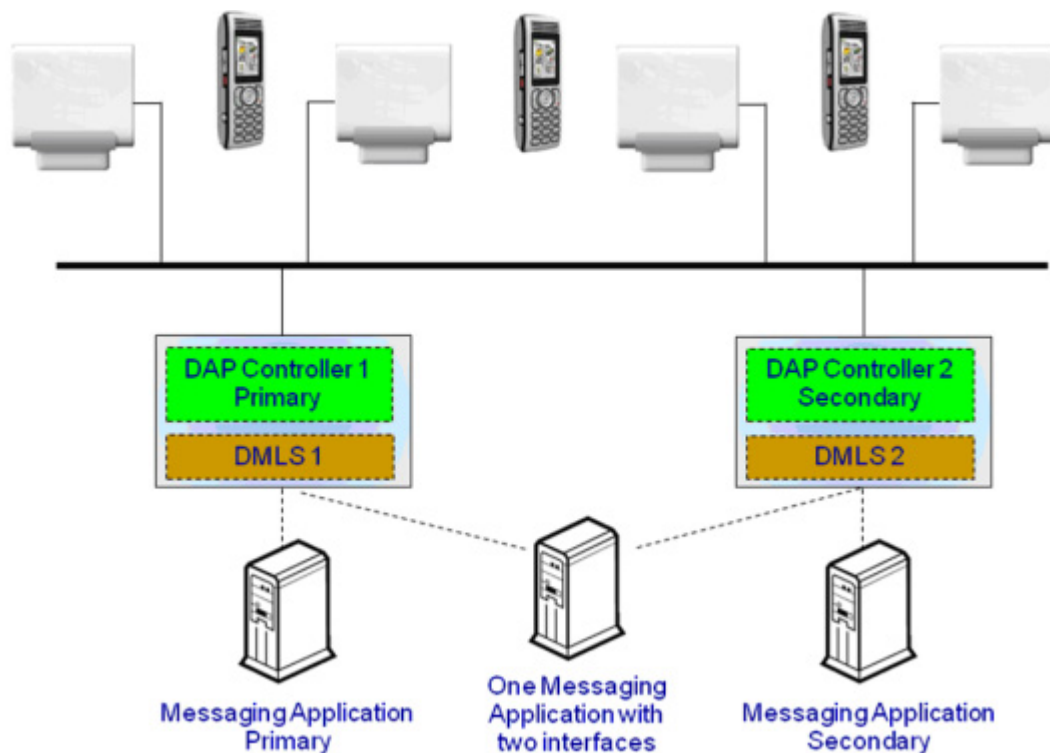


Figure 13-2 Example of a Redundant IP DECT configuration with Messaging

- ✍ *The Duplicated Messaging Application must be capable to run in redundant mode as well, one operational, one standby. Or in case of one Messaging Application, it must be capable to handle two IP interfaces and detect which interface is operational.*
- ✍ *In all cases, the Messaging application should check which DAP Controller and therefore which DMLS is up and running.*

Message to the handsets when Primary DAP Controller is active

[Figure 13-3 Messaging when Primary DAP Controller Active](#), shows that, when the Primary DAP Controller is active, the Messaging Application will send the message to the DMLS (DMLS 1) that is connected to the Primary DAP Controller. The DMLS will send the message to the Primary DAP Controller. The Primary DAP Controller will issue a paging request via all DAPs in the system, to page the handset. When the handset responds, the message is sent to the handset.

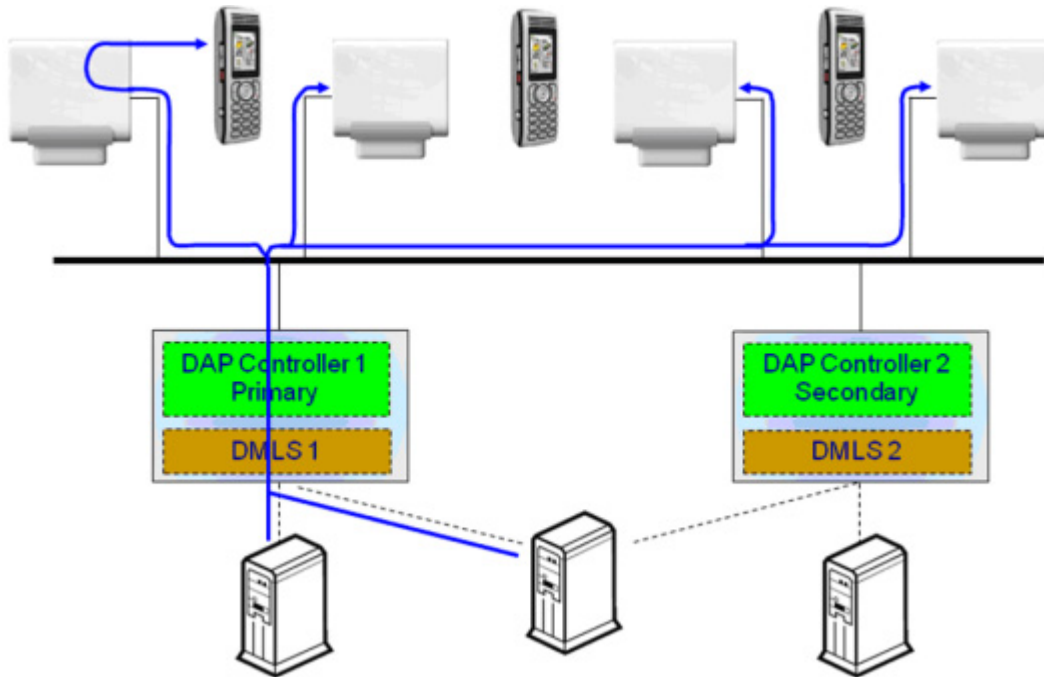


Figure 13-3 Messaging when Primary DAP Controller Active

Message to the handset when Primary DAP Controller is down

[Figure 13-4 Messaging when primary DAP Controller down](#) shows that, when the Primary DAP Controller is down, the Messaging Application will send the message to the DMLS (DMLS 2) that is connected to the Secondary DAP Controller. The DMLS will send the message to the Secondary DAP Controller. The Secondary DAP Controller will issue a paging request via all DAPs in the system, to page the handset. When the handset responds, the message is sent to the handset.

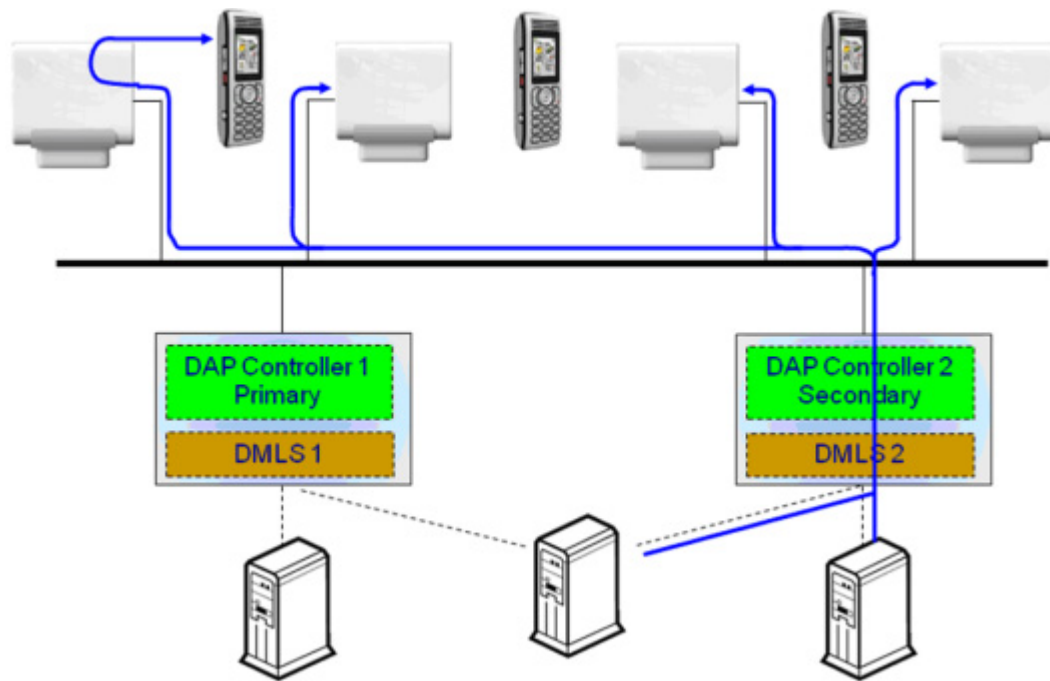


Figure 13-4 Messaging when primary DAP Controller down

Message from the handset when Primary DAP Controller is active

Figure 13-5 Message from handset when Primary DAP Controller is active shows the path of a message from a handset. It will go from the handset to the Primary DAP Controller. Only if the Primary DAP Controller is down or not reachable, the DAP will send the message to the Secondary DAP Controller (not shown in the figure.)

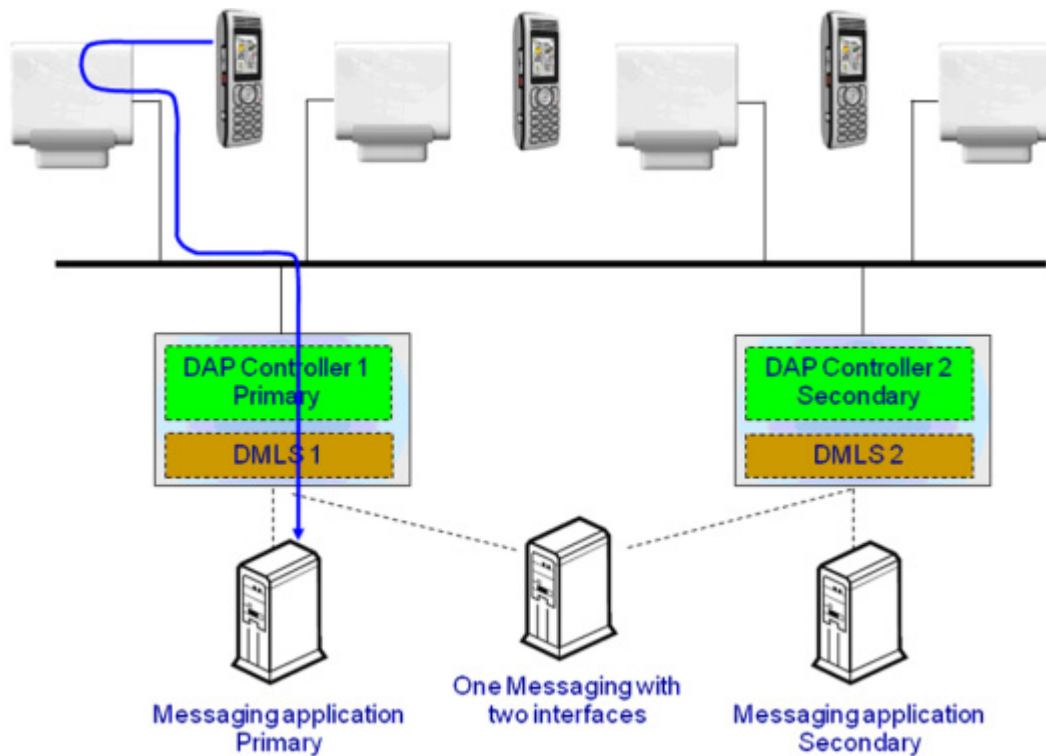


Figure 13-5 Message from handset when Primary DAP Controller is active

Please note that the DAP determines where to send the message to: the Primary or the Secondary DAP Controller. The DAP checks if the Primary DAP Controller is up-and-running. If it is up-and-running, it will send the message to the Primary DAP Controller. If not running, it will send the message to the secondary DAP Controller.

SECTION 3 **DAP CONTROLLER REDUNDANCY - HOW DOES IT WORK**

In the DAP Controller Redundancy, there is a Primary DAP Controller and a Secondary DAP Controller. Please note that in an operational configuration, both DAP Controllers are up-and-running. The Primary DAP Controller contains the actual and up-to-date configuration. The Secondary DAP Controller keeps itself updated with the configuration data from the Primary by means of a Presence Check and info exchange. See [Figure 13-6 DAP Controller Redundancy](#).

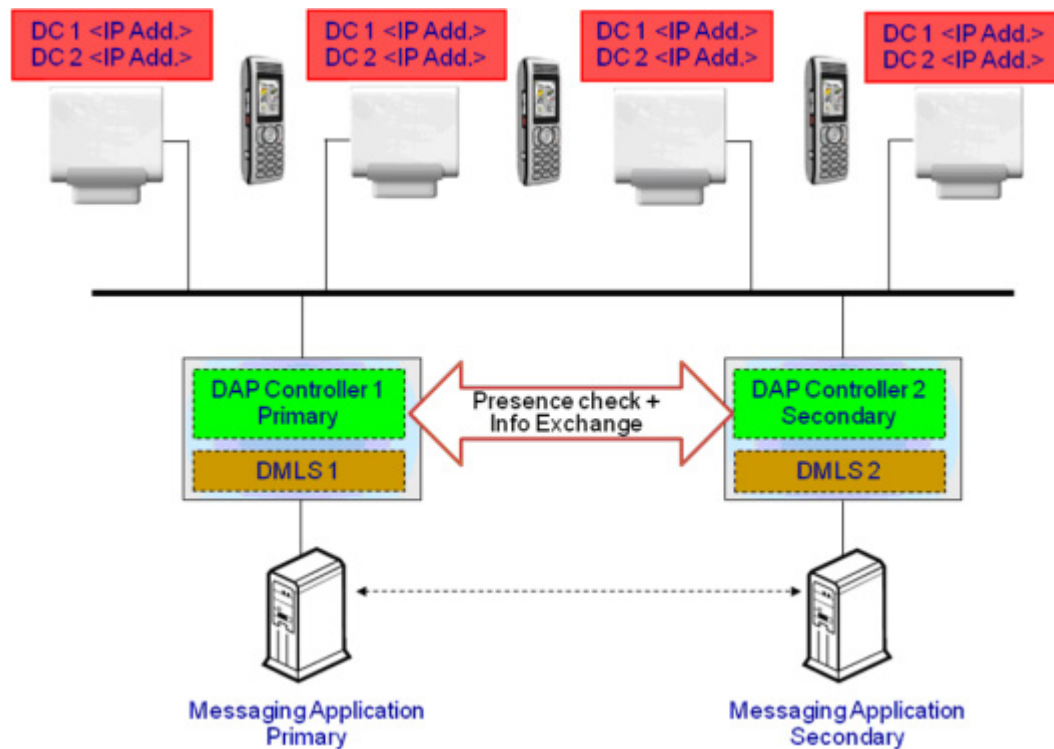


Figure 13-6 DAP Controller Redundancy

☐ **Three DAPs select to which DAP Controller they will connect**

The DAPs select to which DAP Controller they will connect, based on the priorities in the list of DAP Controllers. A DAP will try to connect to the DAP Controller that is first in the priority list (Primary DAP Controller). If that fails, it will try to connect to the second DAP Controller in the list (Secondary DAP Controller). If that fails it will try to connect to the Local DAP Controller that is in the list (see the screen capture in [Section 1 General](#)).

☐ **The Messaging Application**

In the Messaging Application configuration, most likely, one of the Applications is operational, the other stand-by. The Messaging Application is able to detect if Primary DMLS/DAP Controller is active or not. If operational, the primary Messaging Application will be active. If the Primary DMLS/DAP Controller is not active, the Messaging Application detects that, and will make the secondary Messaging Application active.

☐ **When the Primary DAP Controller is down**

If the Primary DAP Controller is down, the DAPs will notice that the DAP Controller, is not operational anymore, and therefore, the DAPs will try to

connect to the Secondary DAP Controller, based on the on-board priority list of DAP Controllers. See [Figure 13-6 DAP Controller Redundancy](#). The Secondary DAP Controller detects that the Primary is not reachable anymore, and will not allow to do any manual changes in subscriptions anymore.

□ When the Primary DAP Controller becomes operational gain

When the Primary becomes operational again, the following will happen:

- The DAPs continuously poll the Primary DAP Controller to check if it is back again. Because of that, they will detect that the Primary DAP Controller is up again. Then they will "lock" on the Primary DAP Controller.

Then the Primary DAP Controller will retrieve the configuration data (subscription data etc.) from the DAPs, to make the system consistent again. ‘

- The Secondary DAP Controller polls the Primary DAP Controller continuously. When it detects that the Primary DAP Controller is back again, it will request for configuration data from the Primary DAP Controller. The Primary DAP Controller already received the latest configuration data from the DAPs, and is up-to-date. The Secondary DAP Controller will get the configuration data from the Primary, and then the IP DECT System is consistent again.

□ What happens when there is a change in the configuration data in the Primary DAP Controller

When there is a change in the configuration data in the Primary DAP Controller (e.g. a handset is subscribed, the Redundancy Service in the Primary DAP Controller sends a notification to all other DAP Controllers (Secondary and Local DAP Controllers).

SECTION 4 LOCAL DAP CONTROLLERS

Besides the Central DAP Controllers, there can be Local DAP Controllers. A Local DAP Controller is located in a Branch Office and takes care of the DAP Controller functionality in the associated Branch Office only, in case the Central DAP Controllers (Primary and/or Secondary) are not reachable anymore. It performs a kind of Survivability task.

There can be up to 10 Local DAP Controllers. The DAPs in the Branch Office will check if the Central DAP Controllers are reachable. If not, they will check if the Local DAP Controller is reachable, and they lock on the local DAP Controller.

[Figure 13-7 Example of DAP Controller Redundancy with two Central DAP Controllers and two Local DAP Controller](#) shows a configuration with mixed DAP Controllers, Central and Local. Although capable to send/receive messages, the Local DAP Controllers are not used for messaging in this example. However, if the Messaging Application supports it, the Messaging Application could connect to a Local DAP Controller, to assure that messaging works to the Branch Office.

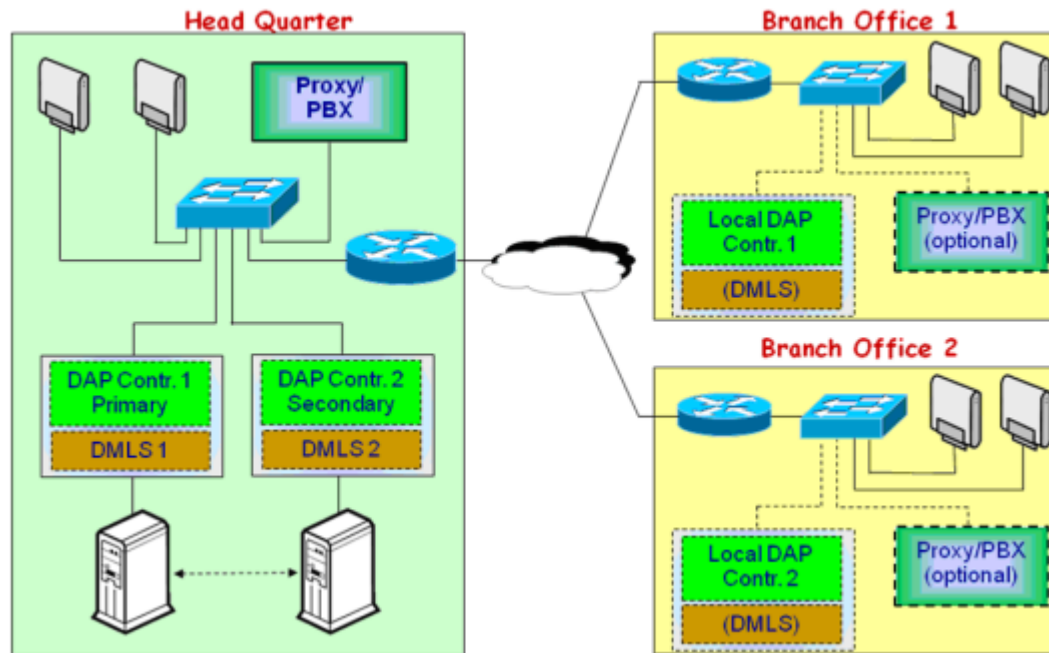


Figure 13-7 Example of DAP Controller Redundancy with two Central DAP Controllers and two Local DAP Controller

SECTION 5 SECONDARY DAP CONTROLLER IN BRANCH OFFICE LOCATION

As a matter of fact, the Secondary DAP Controller does not necessarily have to be located in the Head Quarter, but can be located anywhere else, e.g. in a Branch Office. See [Figure 13-8 Example of DAP Controller Redundancy with Secondary DAP Controller in the Branch Office](#).

In this configuration the Secondary DAP Controller controls the entire IP DECT system when the Primary DAP Controller fails. The Messaging Application can connect to the Secondary DAP Controller, via the IP network.

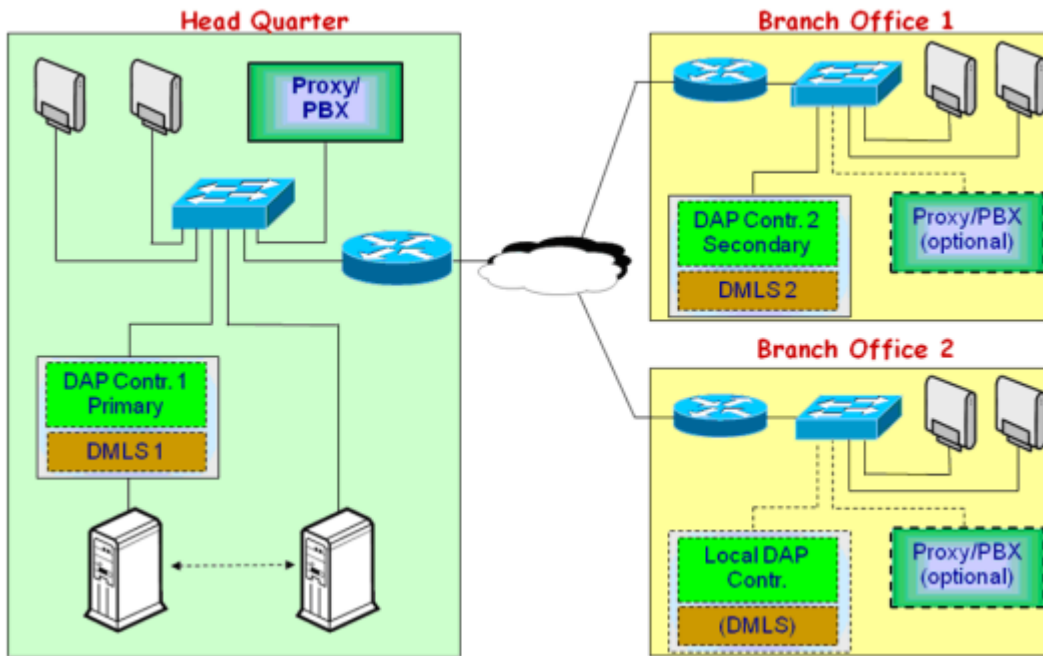


Figure 13-8 Example of DAP Controller Redundancy with Secondary DAP Controller in the Branch Office

SECTION 6 HOW TO SET UP

6.1 Setting up the Redundant Configuration

1. Make a drawing of the redundant configuration. Determine if you need to have a Secondary DAP Controller and determine if you need to have one or more Local DAP Controllers, and where in the network.
2. If not yet done, open the DAP Configurator and go to "IP Settings" ' "DAP Controller IP Configuration".
3. Select Redundant DAP Controller. See [Figure 13-9 Redundant DAP Controller](#).

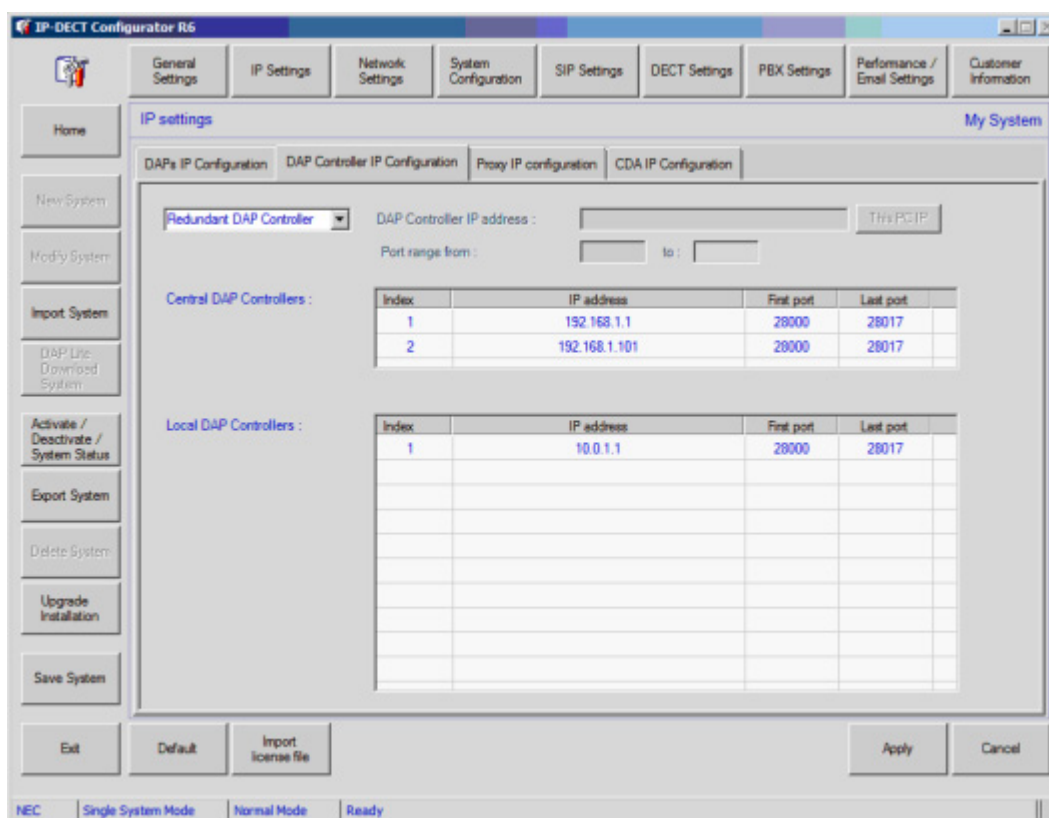


Figure 13-9 Redundant DAP Controller

4. In the list of **Central DAP Controllers**, enter the IP address of the Central, Primary DAP Controller in the row **Index 1**.
5. If you have a secondary DAP Controller, enter the IP Address of the Secondary DAP Controller under **Index 2**.
6. If you have one or more "Local DAP Controllers", enter the IP addresses in the table of the Local DAP Controllers.
7. When done, click the **Apply** button and after that, the **Save System** button.
8. Finish all other settings for the Primary DAP Controller. When done, click **Export System** and save the configuration in a file.
9. Install the other (Central and or Local) DAP Controllers and Import the Configuration file from the Primary DAP Controller.
10. Now you can start the DAP Controllers and the Redundant configuration should work.

11. Check that the "Redundancy" service called **Redundant DAP Controller** is running as a service under Windows, and check that the "Redundant DAP Controller" service is set to **Automatic**.

SECTION 7 DECT MANAGEMENT

- ☐ **At the Primary DAP Controller** - Normally you will do DECT Management on the Primary DAP Controller, and you will have full DECT Management functionality available.
- ☐ **At the Secondary DAP Controller** - When you open the WEB page on the Secondary DAP Controller with address **Localhost**, you will be redirected to the Primary DAP Controller and you will have full DECT Management functionality available. When the Primary DAP Controller is not up-and-running, you will not be redirected, but you will see the Secondary DAP Controller DECT Manager window in Read Only mode. When the Primary DAP Controller comes back again, you will automatically be redirected to the Primary DAP Controller.

SECTION 8 HOW TO CREATE AN ARCHIVE

When you open a WEB Page on the Secondary DAP Controller, you will see the WEB Page (DAP Manager screen) on the Primary DAP Controller. So, when you click the **Archive Button**, an Archive is created of the Primary DAP Controller, but stored on the Secondary DAP Controller!

When you want to make an Archive of the Secondary DAP Controller, you cannot do that via the WEB Page (DAP Manager), unless the Primary DAP Controller is down. So, you must use the button **Archive** in the DAP Configurator of the Secondary DAP Controller.

SECTION 9 ACTUAL STATUS INDICATION

In the top right corner of the DECT Manager WEB interface, the Redundancy status is displayed. The redundancy status is either Redundant or Stand Alone. See [Figure 13-10 Display Redundant Mode](#).

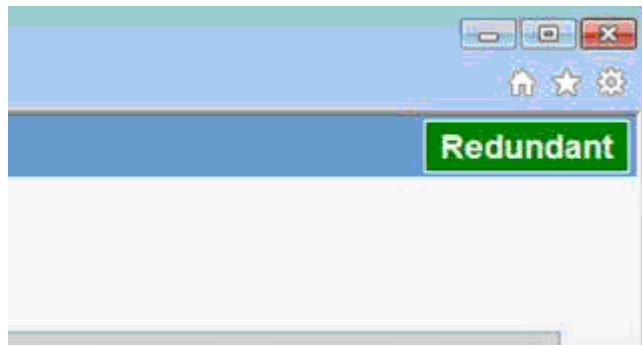


Figure 13-10 Display Redundant Mode

THIS PAGE INTENTIONALLY LEFT BLANK

SIP Proxy Redundancy

SECTION 1 IMPLEMENTATION

Redundancy means that a SIP User Agent (UA) can (automatically) register to a Proxy out of a list of Proxies. Selection criteria (like availability of the Proxies) determine which Proxy is chosen.

Complicating factors are related features like load-sharing, multi-tenancy and the fact that DAPs can fail.

The implementation is based on a Proxy List. Each Proxy has specific properties in the list like a priority level.

The following redundancy types are distinguished:

- ☐ **Fail Over** - All UAs of one DAP, should register at the same primary Proxy. In case the Proxy fails all UAs will register at the same secondary Proxy or when that fails to a tertiary Proxy, etc. When the primary Proxy is back, all UAs should re-register at the primary Proxy.

The first Proxy defined in the Proxy List is the primary Proxy, the second one the secondary Proxy, etc.

At a certain interval, the DAP checks if the primary Proxy is back again. This is the return-to-primary timer. The time period is specified in minutes.

- ☐ **Alternating** - Two different Proxies are each other's standby. Either one of the Proxies is active. If one fails, the other one becomes active. Therefore there is no primary nor secondary Proxy.

The Proxy List contains just a list of Proxies and there is no priority. Also, there is no timer needed to check if the other Proxy is back again.

Because no timer is needed, the "**return-to-primary timer**" is set to 0 minutes, which means "**disabled**".

- ☐ **Load-balancing** - Several Proxies are capable of handling all UAs.

When all Proxies are active, they try to divide the registrations. When one fails, others will accept the registrations of the failing Proxy.

Proxies in the Proxy List are associated with an extension number prefix, used as discriminator to determine the primary Proxy.

At a certain interval, the DAP checks if the primary Proxy is back again. This is the return-to-primary timer. The time period is specified in minutes.

SECTION 2 **SELECTION MECHANISMS**

The following algorithms are used for selecting the preferred Proxy:

- ☐ **Selecting the Primary Proxy** - The DAP searches from top to bottom in the proxy-list for the first Proxy that matches the DNR prefix; a Proxy without DNR prefix always matches. If also a domain name is assigned to this Proxy, the domain name is always used in each message, also when registered at an alternative Proxy.
- ☐ **Selecting the Alternative Proxy** - If the current or chosen Proxy does not accept the registration, the next Proxy that matches will be chosen with the same domain name (irrespective of the DNR prefix, an entry without domain name always matches); if not successful then restart at the top of the proxy-list until the current one is reached again; If this still fails then after a timeout the process starts all over again.

The following triggers will start searching for an alternative Proxy:

- ☐ **Registration Timer** - The DAP re-registers the registered handset with the oldest expiry time for every Proxy (with handsets registered at). The interval is not a fixed time but a computed value. If a Proxy is not operational (doesn't answer upon 2 registration attempts) all the handsets registered at that Proxy will try to re-register. If successful they will stay registered at that Proxy. If not they will register at the next Proxy configured for that handset. When also the next Proxy doesn't react, the search for an alternative Proxy will be postponed and picked up by the regular registration process.

In this scenario worst case it will take 1 minute + the number of handsets per DAP * 5 seconds before all handsets will be registered at the secondary Proxy (if this Proxy is up-and-running).

- ☐ **Return-to-Primary timer** - At the return-to-primary timer all handsets that are not active in a call and not registered to their primary Proxy will try to re-register at their primary Proxy again. If the registration is successful they will stay registered at the primary. Otherwise they will re-register at their current Proxy. Handsets that are active in a call or handsets of which the primary is not present have to wait for the next expiry of this timer before another attempt to re-register them at the primary will be done. Note that the value 0 means that the timer is disabled.

With some extra configurations effort it is even possible to give DAPs at different locations different configuration files and thus different Proxy lists.

The Proxy list must be entered in the DAP Configurator, in the **"IP Settings"** window.

SECTION 3 EXAMPLES

Below are some examples on how Proxy selection is done.

3.1 Example "Fail Over"

In this example the first Proxy is preferred. Each 4 minutes a primary check is done (based on the timer value in the return-to-primary timer), to check if the primary Proxy is back again.

Refer to [Figure 14-1 Example of Proxy settings required for the "Fail Over" example](#) to see the settings in the DAP Configurator **"IP Settings"** window.

The screenshot shows the 'IP Settings' window of the DAP Configurator. The 'Proxy IP configuration' tab is selected. Under 'Multiple gatekeepers', the 'Strip DNR prefix' checkbox is checked. A table lists two gatekeepers:

Index	IP address	Port	DNR prefix	Domain	PBX
1	192.168.1.1	5060			
2	192.168.1.2	5060			

Figure 14-1 Example of Proxy settings required for the "Fail Over" example

In this example, the timer settings in the DAP Configurator **"SIP Settings"** window can be set to 4 minutes. See [Figure 14-2 Example of Return to Primary Setting for "Fail Over" Example](#).

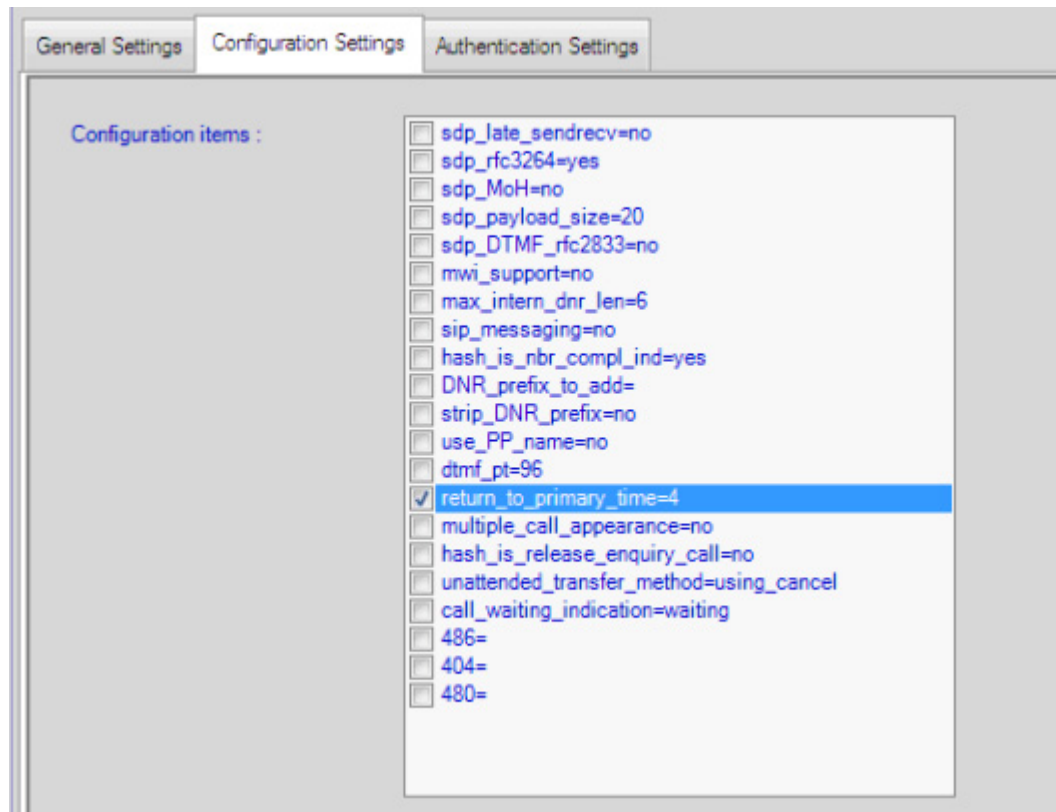


Figure 14-2 Example of Return to Primary Setting for "Fail Over" Example

After saving the configuration, the following lines (amongst others) should be present in the **dapcfg.txt** file:

```
[GK]
192.168.1.1 5060
192.168.1.2 5060

[XDS]
return-to-primary=4
```

3.2 Example "Alternating"

In this example, the first one that matches will be used until it fails. If it fails, the second one will be chosen. The second one remains selected until it fails.

The settings in the DAP Configurator "IP Settings" window can be seen in [Figure 14-3 Example of Proxy Settings Required for the "Alternating" Example](#).

☐ Single gatekeeper Proxy IP address :
 Proxy port number :

☒ Multiple gatekeepers
☐ Strip DNR prefix

Index	IP address	Port	DNR prefix	Domain	PBX
1	192.168.1.1	5060			
2	192.168.1.2	5060			

Figure 14-3 Example of Proxy Settings Required for the "Alternating" Example

The timer settings in the DAP Configurator "**SIP Settings**" window should be set to 0 seconds (to disable the timer), as shown in [Figure 14-4 Return to Primary Setting for "Alternating" Example](#).

General Settings Configuration Settings Authentication Settings

Configuration items :

- ☐ sdp_late_sendrecv=no
- ☐ sdp_rfc3264=yes
- ☐ sdp_MoH=no
- ☐ sdp_payload_size=20
- ☐ sdp_DTMF_rfc2833=no
- ☐ mwi_support=no
- ☐ max_intern_dnr_len=6
- ☐ sip_messaging=no
- ☐ hash_is_nbr_compl_ind=yes
- ☐ DNR_prefix_to_add=
- ☐ strip_DNR_prefix=no
- ☐ use_PP_name=no
- ☐ dtmf_pt=96
- ☒ return_to_primary_time=0
- ☐ multiple_call_appearance=no
- ☐ hash_is_release_enquiry_call=no
- ☐ unattended_transfer_method=using_cancel
- ☐ call_waiting_indication=waiting
- ☐ 486=
- ☐ 404=
- ☐ 480=

Figure 14-4 Return to Primary Setting for "Alternating" Example

After saving the configuration, the following lines (amongst others) should be present in the **dapcfg.txt** file:

```
[GK]
192.168.1.1 5060
192.168.1.2 5060

[XDS]
return-to-primary=0
```

3.3 Example “Load Balancing”

In this example, all extension numbers that start with 1 or 2 will have primary Proxy 192.168.1.1 and all other extension numbers will have primary Proxy 192.168.1.2.

When the primary Proxy for the extension numbers that start with 1 or 2 is unreachable, Proxy 192.168.1.2 will be used.

In this example, each 10 minutes a primary check is done to check if switching back to the primary Proxy is possible. This time is specified in the return-to-primary timer.

The settings in the DAP Configurator “**IP Settings**” window can be seen in [Figure 14-5 Example of Proxy Settings Required for the “Load Balancing” Example](#).

The screenshot shows the 'IP configuration' tab of the DAP Configurator. It features two radio buttons: 'Single gatekeeper' (unselected) and 'Multiple gatekeepers' (selected). Below the radio buttons is a checkbox labeled 'Strip DNR prefix' which is also unselected. To the right, there are input fields for 'Proxy IP address' and 'Proxy port number'. Below these fields is a table with the following data:

Index	IP address	Port	DNR prefix	Domain	PBX
1	192.168.1.1	5060	1		
2	192.168.1.1	5060	2		
3	192.168.1.2	5060			

Figure 14-5 Example of Proxy Settings Required for the “Load Balancing” Example

In this example, the timer settings in the DAP Configurator “**SIP Settings**” window can be set to e.g. 10 minutes, as shown in [Figure 14-6 Example of Return to Primary Setting for “Load Balancing” Example](#).

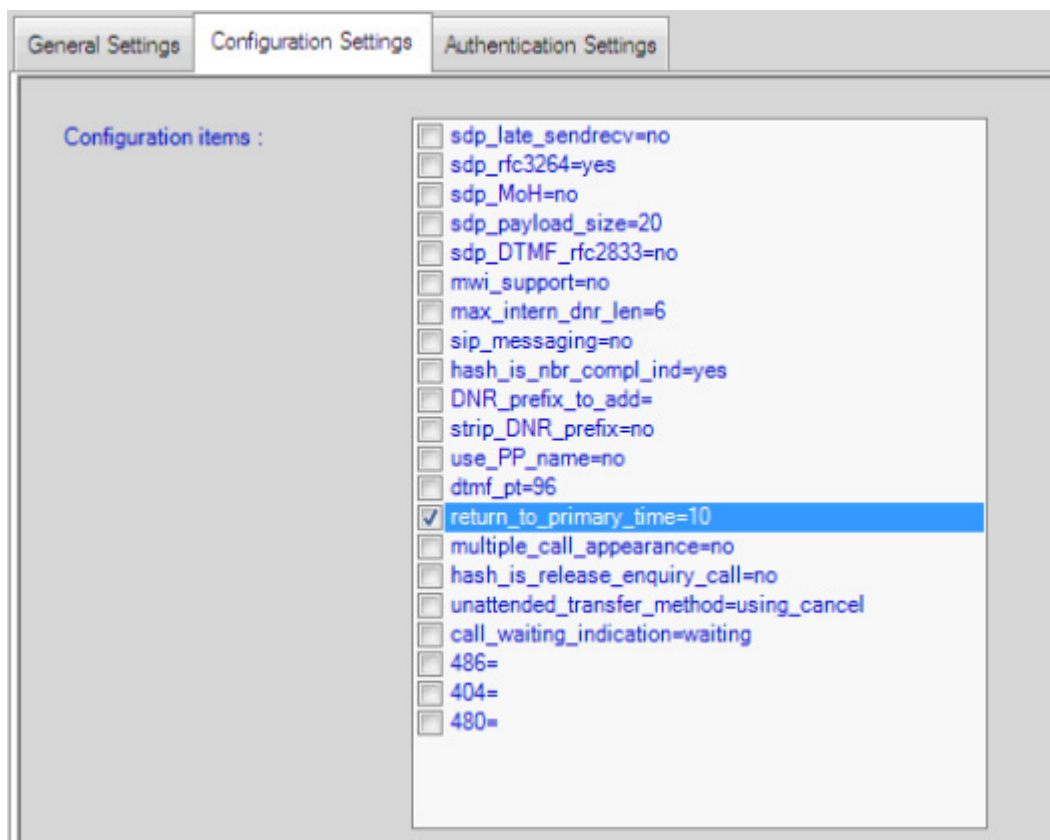


Figure 14-6 Example of Return to Primary Setting for "Load Balancing" Example

After saving the configuration, the following lines (amongst others) should be present in the **dapcfg.txt** file:

```
[GK]
192.168.1.1 5060 0 1
192.168.1.1 5060 0 2
192.168.1.2 5060
```

```
[XDS]
return-to-primary=10
```

3.4 Example "Using Different Domains"

In this example, extension number ranges are in different domains.

Extension numbers starting with a **1** will have:

- test1.com as domain name.

- Proxy 192.168.1.1 as primary.
- Proxy 192.168.1.2 as secondary.
- Proxy 192.168.1.3 as tertiary.

Extension numbers starting with a **2** will have:

- test2.com as domain name.
- Proxy 192.168.1.1 as primary.
- Proxy 192.168.1.3 as secondary.

Every 10 minutes a primary check is performed.

The settings in the DAP Configurator "**IP Settings**" window can be seen in [Figure 14-7 Proxy Settings Required for the "Using Different Domains" Example](#).

Index	IP address	Port	DNR prefix	Domain	PBX
1	192.168.1.1	5060	1	test1.com	
2	192.168.1.2	5060	1	test1.com	
3	192.168.1.1	5060	2	test2.com	
4	192.168.1.3	5060			

Figure 14-7 Proxy Settings Required for the "Using Different Domains" Example

The timer settings in the DAP Configurator "**SIP Settings**" window should be as shown in [Figure 14-8 Return to Primary Setting for "Using Different Domains" Example](#).

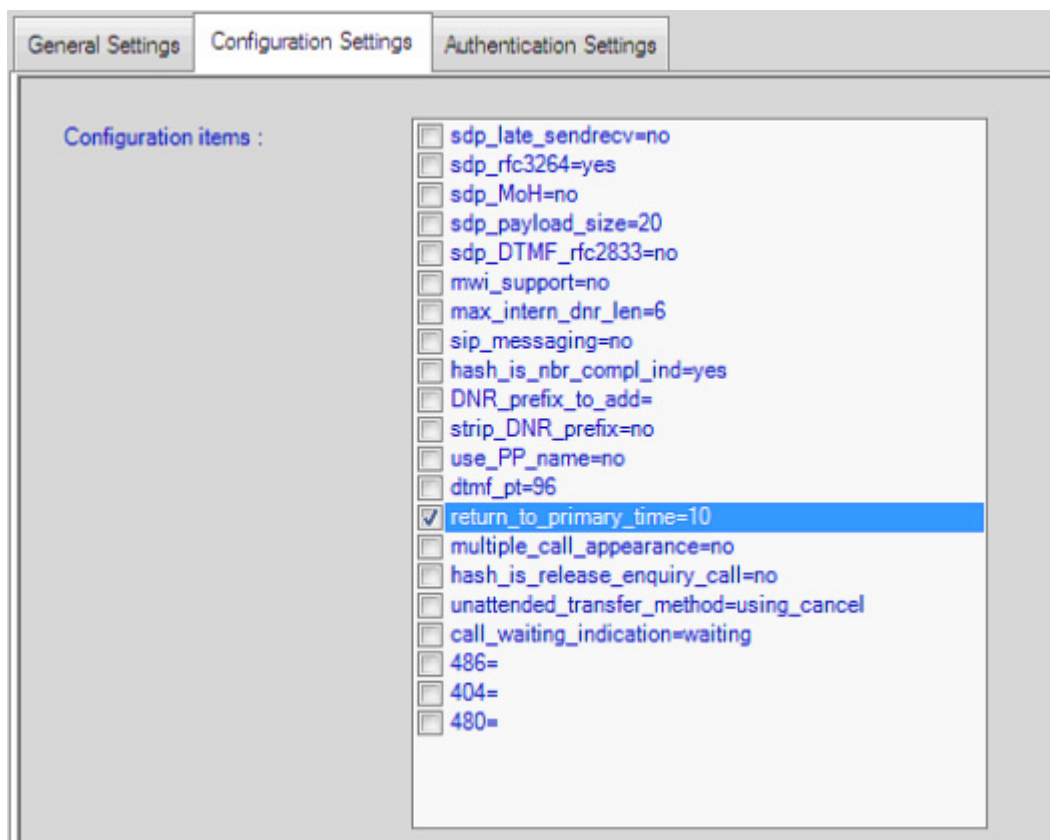


Figure 14-8 Return to Primary Setting for "Using Different Domains" Example

After saving the configuration, the following lines (amongst others) should be present in the **dapcfg.txt** file:

```
[GK]
192.168.1.1 5060 0 1 6 test1.com
192.168.1.1 5060 0 1 6 test1.com
192.168.1.1 5060 0 2 6 test2.com
192.168.1.3 5060
```

```
[XDS]
return-to-primary=10
```

Please note that there is a system type identifier as fifth field in the proxy definition line. In this example the system type identifier is 6, which means SIP Proxy.

The selection criteria for a change over to a secondary proxy in the list is primarily based on the domain specification. So, when the primary proxy fails, the system will select the next proxy in the list that has the same domain name.

THIS PAGE INTENTIONALLY LEFT BLANK

Using Other TFTP Server

SECTION 1 GENERAL

The previous sections assume that you are using the built in TFTP Server in the DAP Controller/Manager Software. That is the easiest way because paths etc. are automatically set correct. However, if you have chosen to use another TFTP server, paths must be set correct and files needs to be copied into the TFTP root directory. Consult the following section.

SECTION 2 PREPARE FILES FOR TFTP UPLOAD TO DAPS

The DAPs will only become operational if they can load the required files via TFTP. This requires that the DHCP server and the TFTP server are up-and-running with the correct configuration and it requires that the files for the DAP are available in the TFTP directory.

2.1 Copying Files to the TFTP Directory

1. Determine which TFTP Server you are using. There are four options:
 - ☐ 3com TFTP Server on this PC.
 - ☐ Windows TFTP Server on this PC.
 - ☐ Other TFTP Server on this PC.
 - ☐ Other TFTP Server running on other PC.
2. In the following steps you must copy the firmware file (and configuration file) to the upload directory of the TFTP Server. Therefore, you must know the path settings of the TFPT Server that you are using. [Table 1 Overview of TFTP Servers](#) provides an overview of the TFTP Servers and the path settings.

Table 1 Overview of TFTP Servers

TFTP Server	Default Path	Preferred Path
3com	C:\Documents and Settings\All Users\Application Data\Nec\DAPE Controller\<system name>\ OR for Windows 7 and 2008: C:\ProgramData\Nec\DAPE Controller\<system name>	C:\Documents and Settings\All Users\Application Data\Nec\DAPE Controller\<system name>\ OR for Windows 7 and 2008: C:\ProgramData\Nec\DAPE Controller\<system name>
Windows	C:\tftpdroot\	C:\tftpdroot\
Other	Unknown	C:\Documents and Settings\All Users\Application Data\Nec\DAPE Controller\<system name>\ OR for Windows 7 and 2008: C:\ProgramData\Nec\DAPE Controller\<system name>
Other on other PC	Unknown	Unknown

The two files that needs to be in the TFTP directory are:

- Firmware file: 4910bvxx.dwl (the one that you have specified in [Section 2 General Settings on page 11-1](#)).
 - The configuration file: **dapcfg.txt**.
3. Copy the firmware file to the TFTP directory of the TFTP Server that you are using. If you are using the 3com TFTP server that came with the IP DECT installation (default!) the default path equals the preferred path.

The dapcfg.txt file is by default stored in the directory:

C:\Documents and Settings\All Users\Application Data\Nec\DAPE Controller\<system name>\.

OR when you are using Windows 7 or Windows 2008, the directory is:

C:\ProgramData\Nec\DAPE Controller\<system name>. This is the default directory for the "3com TFTP" server that came with the installation of the IP DECT system. If you are using the "3com TFTP" server, no manual action is needed anymore. However, if you are using another TFTP server, copy the **dapcfg.txt** from the directory **C:\Documents and Settings\All Users\Application Data\Nec\DAPE Controller\<system name>** to the TFTP directory that your TFTP Server is using as upload directory. For Windows 7 or Windows 2008, the path is: **C:\ProgramData\Nec\DAPE Controller\<system name>.**

4. Make sure that the option "**Next Boot Server**" in the DHCP Server that you are using, points to the IP address of the PC where your TFTP Server is running.
5. The DAPs should be able to start-up now.

Opening DAP Manager Web Interface

You can open the DAP Manager window using Internet Explorer 6.0 or higher.

SECTION 1 OPENING THE DAP MANAGER WEB INTERFACE

1. Open the MS Internet Explorer WEB browser on your DAP Controller/Manager PC. Enter an URL that points to the / **CDS/ directory/file** on the DAP Controller/Manager PC.(e.g. <http://127.0.0.1/CDS/>)

It is also possible to open the WEB interface from another PC in the network. However, you must know the right path. This could be e.g. <http://192.168.4.80/CDS/>, where "192.168.4.80" is the IP address of the DAP Controller/Manager PC.

2. Now, you should see the "**DECT Manager**" main screen. If not, then check if your IIS is running on the DAP Controller/Manager PC. Also check if the default.aspx file is present in the **C:\inetpub\wwwroot\CDS** directory.
3. If you have a licensed configuration, assign licenses to your IP DECT system via the DECT Manager interface.

 *The DECT Manager interface is described in the IP DECT Manager Administrator Guide.*

4. Enter the extension number range via the DECT Manager interface.
5. Check that the DAPs are operational.
6. Subscribe the handsets. Check that you can make phone calls.

THIS PAGE INTENTIONALLY LEFT BLANK

Portable Sharing

SECTION 1 WHAT IT IS

Portable Sharing allows the user to give the portable (handset) an extension number via a "login" procedure.

When a portable is enabled for Portable Sharing, you will get a **"Login"** message when you go off hook after one of the following conditions:

- ☐ after the handset was subscribed
- ☐ after the handset was switched on
- ☐ after the handset was taken from the charger with silent charging switched on

In this **"login" mode**, you must enter the extension number that you want to activate for the handset. This extension number must already be present in the SIP Proxy. After you entered the extension number, you must terminate the login with a closing digit. By default, **"#"** is the closing digit. However, this can be changed. After entering the closing digit, the handset is active for the extension number that you have entered. Only after a "logout" the handset displays the "login" again.

How and when does a handset do a Logout? A Logout is executed automatically, when the handset sends a **"Detach"** signal to the DECT System. Sending a **"Detach"** signal is done automatically at the following manual action:

- ☐ **Switching off the handset** - The handset types C922, C933, C944, I600, G355, G955, I755 and later types, will send a **"Detach"** signal when they are within reach of the IP DECT system **AND** when the user switches off the handset!
- ☐ **Putting the handset in charger with silent charging enabled** - The handset type C933, C944, I600, G355, G955, I755 and later types, will send a **"Detach"** signal when they are within reach of the IP DECT system **AND** when the user puts the handset in the charger in silent charging mode.

- ✍ *When any type of handset goes out of range, no Detach signal is sent! Therefore **"login"** is not activated when the handset comes within range again.*
- ✍ *This Portable Sharing mechanism is supported for C922, C933, C944, I600, G355, G955, i755 and later types. On other types of handsets, support of Portable Sharing is not available at all, or you can login only once because there is no **"Detach"** possible*

Portable Sharing is disabled by default for the IP DECT system, but can be switched on using the DAP Configurator.

When enabled, you must designate a certain number range in the subscription numbers that is used for Portable Sharing. The numbers in this range may NOT exist as extension numbers in the SIP Proxy. These numbers must start with the same "prefix". This prefix must be specified in the DAP Configurator and could be e.g. "00".

1.1 Portable Sharing and the DAP Manager

The DAP Manager PC is always needed for handling the Login information and for providing the login information to the DAPs (e.g. when a DAP restarts). This means that the DAP Manager should always be connected and should be up-and-running. However, it is not "Single point of failure", which means that if the DAP Manager is down, you can still make and receive calls.

The login information is stored in a file **dds-login.txt** on the hard disk of the DAP Manager PC.

Upgrade To Latest Release

To upgrade to the latest release of the DAP Controller software consult the IP DECT Advanced Data Manual.

Chapter

A


THIS PAGE INTENTIONALLY LEFT BLANK

AP300 Versus AP200

SECTION 1 OVERVIEW OF DIFFERENCES

From November 2009 onwards a new DAP will be introduced, the AP300 as a successor of the AP200.

In this Appendix you will find an overview of the differences between the AP200 and the AP300.

 For more information on the characteristics of the AP300, please consult the AP300 Installation Manual.

1.1 Main Differences

[Table B-1 Main Differences between AP200 and AP300](#) highlights the major differences between the AP200 and the AP300 handsets.

Table B-1 Main Differences between AP200 and AP300

Item	AP200	AP300
Compact Size	A5	2/3 of A5
Mounting	Vertical	Vertical or Horizontal
Localization Support	Various Types	One type of AP300 suitable for all regions. Country and region selection in the DAP Configurator.

Item	AP200	AP300
G.729	AP200 only, not in AP200S	Available via daughter board on the AP300. See Section 1 Overview of Differences on page C-1 . From June 2012 onwards the AP400 will be introduced, as a successor of the AP300. In this Appendix you will find an overview of the differences between the AP300 and the AP400. Please note that the AP300 and the AP400 are similar in many aspects.
Power Supply	Local via AC Adaptor and PoE support IEEE802.3af	PoE IEEE802.3af. No local power supply.
DC voltage on DAP via PoE	36 - 60 Volt	36 - 57 Volt
PoE Class	Class 0	Class 2
Service/Maintenance	One LED for AP200 Status.	Two LEDs, one for AP300 status, another for AP300 network status indication.

1.2 Mechanical Differences

[Table B- 2 Mechanical Differences AP200 - AP300](#) provides a comparison of mechanical differences between the AP200 and AP300 handsets.

Table B- 2 Mechanical Differences AP200 - AP300

Item	AP200	AP300
Dimensions	235 x 45 x 172 mm (w x d x h)	145 x 43 x 174 (w x d x h)
Weight	540 gram (including packaging)	307 gram (excluding packaging)
Protection	IP20	IP40
Color	Light grey (color code 70109)	Light Grey, RAL 9010
Antenna	Fixed Position	Adjustable: horizontal or vertical position

1.3 Outdoor Cabinet Differences

Table B-3 Outdoor Cabinet Differences AP200 - AP300 provides a description of the outdoor cabinet differences between the AP200 and AP300 handsets.

Table B-3 Outdoor Cabinet Differences AP200 - AP300

Item	AP200	AP300
Dimensions	430 x 330 x 200 mm (w x d x h)	275 x 225 x 80 mm (w x d x h)
Weight	6 kg (AP200 inclusive)	
Material	Glass enforced polyester	IP40
Relative Humidity	5 to 95 %	5 to 95 %
Color	Grey (RAL 7032)f	
Protection	IP66	IP66
Operating Temperature	-15° to +60° C	-20° to +45° C

THIS PAGE INTENTIONALLY LEFT BLANK

AP400 Versus AP200

SECTION 1 OVERVIEW OF DIFFERENCES

From June 2012 onwards the AP400 will be introduced, as a successor of the AP300.

In this Appendix you will find an overview of the differences between the AP300 and the AP400. Please note that the AP300 and the AP400 are similar in many aspects.

1.1 Main Differences

Table C-1 Differences between AP300 and AP400 highlights the differences between the AP300 and the AP400 handsets.

Table C-1 Differences between AP300 and AP400

Item	AP300	AP400
Outside Temperature	0 C . . . 45 C	-5 C . . . 45 C
HD Voice	—	Yes, G.722, but depends on used handsets types and on the SIP PBX.
CAT-iq Data facilities	—	Not applicable yet.
DAP Type: Generic type, NEC branded	AP300	AP400
DAP Type: Generic Type, un-branded	—	AP400G

Item	AP300	AP400
DAP Type: Type to be used on NEC SMB systems.	AP300C	AP400C
DAP Type: Generic type with connectors for external antennas	AP300E	AP400E
DAP Type: Type to be used on NEC SMB PBXs, but with a max. of 4 DAPs per system.	—	AP400S
Boot Package	In Read Only Memory	In Flash Memory Name: 49920xxx.dwl
Firmware Package	Name 4910bxxx.dwl	Name 4920bxxx
IGMP Version	IGMPv2	IGMPv3

SIP Configuration Characteristics

SECTION 1 **GENERAL**

Setting up the SIP configuration requires basic SIP knowledge. Make sure that you have basic SIP knowledge before continuing this Chapter and the Chapters that follow. The SIP implementation differs between the various types of SIP Proxy/Registrar servers. It is important to know the basic characteristics of the SIP Proxy/Registrar server to which you want to connect the SIP IP DECT system.

In the following Sections, the Business Mobility IP DECT SIP characteristics are described. This can be useful before you continue with the installation. However, if you are familiar with the SIP characteristics of the Business Mobility IP DECT system, continue with the installation of the Business Mobility IP DECT system, see [Installing The DAP Controller/Manager on page 9-1](#) and onwards.

SECTION 2 **MAIN CHARACTERISTICS**

The following overview shows the main SIP characteristics of the Business Mobility IP DECT system:

- ❑ **Connectivity** - The Business Mobility IP DECT system can be connected to many SIP types of commercial, open-source or freeware SIP Proxy server, SIP Registrar server, SIP Gateways, SIP IP-phones, SIP soft phones, SIP IP enabled PBX's etc.

The Business Mobility IP DECT system can also be connected directly to a DSL line for small branch and home offices.

❑ SIP Extension Registration

- Usage of SIP Registrar server is supported (optional).
- Detached portables are unregistered from the SIP registrar server. (Portables can be detached automatically, when they support sending a "Detach" signal and "switches off". Also when they support "Detach" signal and put in the charger in "Silent Charge" mode a Detach signal is send.
- Digest authentication security.
- SIP URL configurable: sip:phone-number@ip-address e.g. sip:2500@192.168.1.1 or sip:"phone-number"@host-domainname e.g. sip:2500@sipproxy.test.com.
- Username and/or password configurable.

❑ Transmission

- High quality voice over IP, G.711 when the call remains within the LAN segment, or G.711/G.729 when the peer-to-peer connection crosses a router in a Branch office configuration. However, you can select whether you want to use G.729 only, or never use G.729.
- Congestion control and packet filtering.
- Reliable UDP transport using retransmissions.

SECTION 3 CALL HANDLING

[Table D-1 Supported SIP Features](#) provides a list of supported SIP call handling features.

Table D-1 Supported SIP Features


Feature	Reference
Basic Call	RFC3261 (except for TCP, IP, Multicaster. MIME and authentication)
Negotiation of most efficient CODEC based upon network information. <ul style="list-style-type: none"> ○ Supported CODECs: ○ G.711 a-Law ○ G.711 u-Law ○ G.729 	RFC 2327 RFC 3264
Payload negotiation. Supported payload values: 20 ,30, 40, 50, 60 msec.	RFC 2327 RFC 3264

Feature	Reference
En-block (pre-dial) and overlap dialling	RFC 3578
Remote name, or if not available, phone number is displayed on the handset.	
Discrimination between internal and external calls based upon extension number length (configurable)	
Established session modification (re-INVITE)	
Call hold using re-INVITE	
Shuttle between two parties	
Call transfer: <ul style="list-style-type: none"> ○ Attended call transfer using REFER, Refer-To and Replaces ○ Unattended call transfer using REFER and Refer-To 	RFC 3515 RFC 3891
DTMF digit sending: <ul style="list-style-type: none"> ○ Via SIP INFO messages ○ In RTP stream 	- RFC 2976 RFC 2833
SIP Music-On-Hold	
When connected to a FXO gateway, it switches to transparent mode to save trunk lines	
Instant Messaging to and from SIP-DECT portables	RFC 3428 (protocol supported, no application implemented)
MWI (Message Waiting Indication)	RFC 3842

SECTION 4 CONFIGURABLE ITEMS IN IP DECT SIP

[Table D-2 Configurable Items in SIP IP DECT](#) gives an overview of the items that can be configured in the SIP IP DECT configuration, in order to adapt to the SIP Proxy Server and, if present, SIP Registrar. Note that this gives an overview only, the actual settings must be entered during the installation of the Business Mobility IP DECT software when asked for. It is always possible to change the settings after the installation.

Table D-2 Configurable Items in SIP IP DECT

Parameter	Default Value	Description
proxy_address	no default	The IP address of the Proxy server
proxy_port	5060	The port number on the Proxy server
registrar_addr	[proxy_address]	The IP address of the Registrar server. IP4, dotted format. If nothing is specified, Proxy server address.
registrar_port	[proxy_port]	The port number on the Registrar server. If nothing is specified, this address is equal to the specified Proxy server address.
sip_domain	[proxy_address]	SIP domain. If nothing is specified, this address is equal to the specified Proxy server address.
max_intern_dnr_len	6	Extension numbers longer than this value are considered as “external”. Only applicable for numeric extension numbers.
local_port	5060	Local SIP port on the DAPs.
realm1...realm5	[empty]	Up to five authentication realms (for both www and proxy) can be specified.
user1...user5	[empty]	Up to five authentication users (for both www and proxy) can be specified.  In case “%s” the DNR (extension number) will be used instead.
passw1...passw5	[empty]	Up to five authentication passwords (for both www and proxy) can be specified.

Parameter	Default Value	Description
sdp_late_send recv	no	Enables/disables the ability of SIP DECT to issue an initial invite without SDP offer.
sdp_rfc3264	yes	Enables/disables "Hold" according to RFC3264
sdp_MoH	no	When enabled, no local tone is generated when DECT portable is put in "recv only" (hold) mode.
sdp_payload_ size	20	Offered payload size in SDP offer (in msec). However, the proposed payload size of the other party is used.
sdp_DTMF_rfc 2833	no	When enabled, DTMF digits are sent according to RFC2833 (in RTP). Otherwise, the DTMF digits are sent as SIP INFO messages.
mwi_support	no	Enables/disables Message Waiting indication.

SECTION 5 TLS AND SRTP SUPPORT


5.1 General

IP DECT Release 4.2 or higher supports TLS and SRTP. The following items are important to understand how the IP DECT TLS support is implemented.

5.2 TLS

TLS (Transport Layer Security), defined in RFC 2246, is a protocol for Authenticating the server. It also supports encryption of the data that is exchanged between the client and the server. The TLS protocol is extensible, meaning that new algorithms can be added for any of these purposes, as long as both the server and the client are aware of the new algorithms.

Using TLS means that certificates must be generated, using a Root Authority. IP DECT does not support generating Certificates. This means that the **SIP Server** must have a build in Root Authority and must be capable to generate a certificate for every new connection from the DAP. The DAP can verify the server certificate with the SIP Server Root certificate to authenticate.

 *TLS is tested against the NEC iS3000 equipment. If you want to connect to another type of SIP Server using TLS, please contact your IP DECT supplier to check if this is possible or not.*

5.3 SRTP

SRTP (Secure Real-Time Transport Protocol - or Secure RTP) is an extension to RTP (Real-Time Transport Protocol) that incorporates enhanced security features. Like RTP, it is intended particularly for VoIP communications. SRTP is defined in RFC 3711. SRTP uses encryption and authentication to minimize the risk tapping the data stream.

Note that SRTP is between the SIP User agents, the actual voice data stream. For encryption, it uses a key that is randomly generated by one of the User Agents. This key (crypto key) is offered to the opposite User Agent in the SDP. This means that the crypto key can easily be read if the "Invite" with SDP data is un-encrypted. Therefore, if you use SRTP, also use TLS, otherwise one could see the key in the "Invite" and therefore decrypt the SRTP data. (Note that this crypto key is not the TLS Certificate.) Note that when a call is relayed to another DAP, the encryption key is security moved to the other DAP as well.

 *IP DECT Release 5 only supports AES_CM_128_HMAC_SHA1_80 encryption.*

5.4 Configurable Items in IP DECT

The following items are configurable in IP DECT:


○ **Transport protocol selection: TLS, TCP or UDP**

In the IP DECT Configurator, you can select TLS or TCP. If you do not select TLS or TCP automatically UDP is chosen.

You can check the results in the dapcfg.txt file. If you do not select TLS or TCP, there is no information in the dapcfg.txt file. If you select TLS or TCP, you will see the following line in the dapcfg.txt file:


[XDS]

transport_protocol=tls or transport_protocol=tcp

 *If you have selected either TCP or TLS, IP DECT will not fall back to UDP anymore! If IP DECT would fall back from TLS to UDP, encryption would be gone without knowing.*

- **TLS Port Number**


You must specify the TLS port number in the IP DECT Configurator. This is 5061 by default.

 *There is no separate configuration item to select SRTP. SRTP will only be offered when TLS is selected.*

THIS PAGE INTENTIONALLY LEFT BLANK

LRMS Messaging

SECTION 1 GENERAL

 *Messaging can only be used with handsets that support LRMS (E2) messaging.*

IP DECT supports LRMS (Low Rate Message Services). There are two options:

- ☐ **Handset - handset Messaging** - This means that handsets can send messages between each other.

Depending on the connection to the Messaging Server, and depending on the SIP Messaging setting, handset to handset messaging is possible or not.
- ☐ **Messaging Server - Handset Messaging** - You can connect a Messaging Server to IP DECT to send and receive messages to/from handsets. The DAP Controller offers an interface for Messaging to and from handsets. However, the DAP Controller supports a proprietary protocol, which requires a converter program called: DMLS (DECT Messaging and Location Services). The DMLS offers a rich, yet simple, interface for Third Party Messaging servers.

For more information about Messaging Server applications, please contact your IP DECT supplier.

[Figure E-1 Message Path in IP DECT - Messaging Server Configuration](#) shows the message path between a Messaging Server and IP DECT.

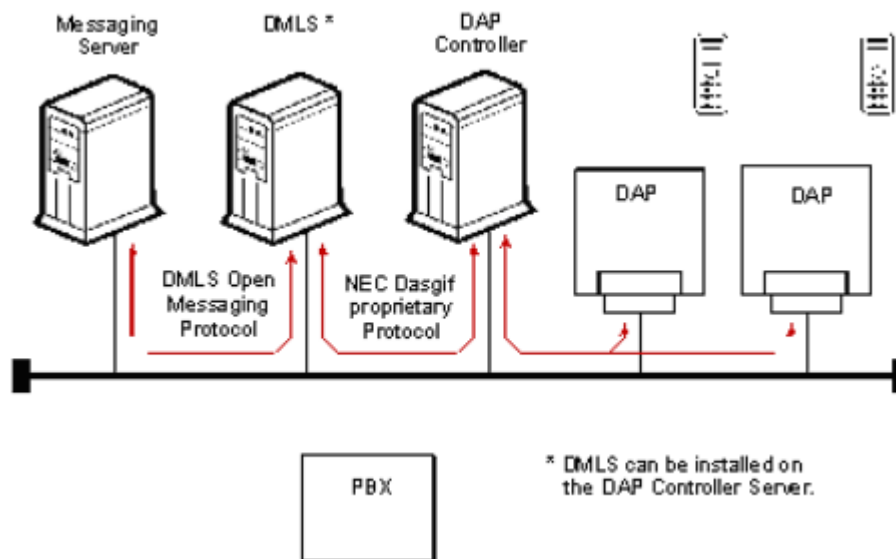


Figure E-1 Message Path in IP DECT - Messaging Server Configuration

Note that the messaging between the Messaging Server and IP DECT, always goes via the DAP Controller/Manager. It is an TCP/IP connection. The TCP port for messaging on the DAP Controller/Manager is always the lowest port number + 1 (default 28001). The moment that there is a connection to this port, all messages will be handled by the Messaging Server and handset to handset messaging is only possible via the Messaging Server.

✎ When the option **"Local Message Relay Override"** is selected in the DAP Configurator, the Messaging Server can send messages to handset and handset to handset messaging is still possible.

✎ When the SIP option **"SIP Messaging"** is enabled in the IP DECT Configurator, all messages will go via the SIP interface (SIP instant messaging) and not via the DAP Controller. SIP messaging does not support Normal, Urgent and Emergency messages (see [Section 2 Types of Messages on page E-3](#)) and it does not support broadcast messaging. (see [section E.3 "Broadcast Messaging"](#))

☐ **Messaging Server - Handset Messaging with Local Message Relay Override** - In the DAP Configurator, there is an option **"Local Message Relay Override"**. When you activate this option, you can send messages between handsets and the Messaging Server can send messages to handsets. Note that you cannot send messages from handsets to the Messaging Server when **"Local Relay Override"** is active.

SECTION 2 TYPES OF MESSAGES

When sending a message to a handset, there are three types of messages distinguished. The message types indicate the emergency level.

- ☐ **Normal Message** - When this type of message is send to a handset, the handset displays the message and will alert with a short ringing. The user of the handset cannot confirm the message. The handset sends back a technical "ACK" to the originator of the message (e.g. DECT Server) to indicate that the message arrived on the handset.
- ☐ **Urgent Message** - When this type of message is sent to a handset, the handset displays the message and alerts with a ringing type that gets louder and louder until the handset user confirms the message (or a timer expires). The user can confirm the message by pressing the "OK" button or the "Delete" button. When the message is send to the handset, a timer is started. The user must confirm the message within the time period of the timer (default 30 sec.). If not confirmed within this time, ringing stops and a "NACK" is send to the originator of the message, to indicate that the user didn't confirm the message.
- ☐ **Emergency Message** - When this type of message is send to a handset, the handset displays the message and alerts with a very compelling ringing type. This forces the user to confirm the message by pressing the "OK" button or the "Delete" button. Confirmation must be done within a certain time period, which is the same as for an Urgent message. (Also 30 seconds by default.) If not confirmed within this time, ringing stops and a "NACK" is send to the originator of the message, to indicate that the user didn't confirm the message.

The originator of the message determines the urgency type of the message. Note that if the handset is the originator, there are only two message types possible: Normal and Urgent. When the Messaging Server is the originator, three message types are possible: Normal, Urgent, Emergency.

SECTION 3 BROADCAST MESSAGING

3.1 General

Broadcast Messaging is implemented from IP DECT Release 4.2 onwards. Broadcast messaging will normally be used in case of an emergency situation where a large group of people needs to be reached in a very short time.

Broadcast Messaging has the following characteristics:

- It uses a kind of "connection-less" data transfer.
- To improve message delivery, the Messaging Server can repeat the message a few times. The handset will ignore duplicate messages.

- Neither the portable nor the end-user can confirm reception of the message.
- No traffic bearers are occupied. This avoids congestion.
- ✎ *The maximum message length is 54 characters.*
- ✎ *Broadcast Messaging is optional in IP DECT. It must be enabled using the DAP Configurator tool.*

Broadcast messaging works with groups. If a handset is member of a group, it is capable of receiving messages for that group. Note that all handsets are always part of the default group ("000").

3.2 Additional Broadcast Type Messages

There are three (additional) message types defined for broadcast messaging. The Message Server must be capable of sending these messages, because the handset is not able to send broadcast messages, it is only able to receive broadcast messages.

- **Broadcast Messages** - A Broadcast message is a real message which is addressed to a group of portables. A three digit number identifies the group. (A handset must have been made member of a group before it can receive messages for the group.)

All portables that support broadcast messages are automatically member of the group '000'. Next to this group a portable can be member of 5 other groups.


Note that these messages are not acknowledged. Therefore it is possible that a portable did not receive this message, because it was for instance out of reach, powered down, in silence charging mode or because of bit-errors in the air. It is the responsibility of the Messaging Server to repeat the same message, to get a higher chance of correct reception by all portables.

Although these messages are not acknowledged, it is still useful to distinguish between normal, urgent and very urgent broadcast messages, because it determines also how the message is presented to the user.

- **Group Membership** - This is not a user message send to the display of the handset. It is a membership message send to the handset. A message Server can instruct a portable to become member of a group or give-up membership of a group by means of this message type. It is also possible to instruct a portable to give-up membership of all groups except '000'.

It is the responsibility of the messaging server to keep track of the group membership of each individual portable, since a portable has to acknowledge this type of message.

- **Broadcast Group Membership** - (This is not a user message send to the display of the handset.) By means of this type of message a Messaging Server can instruct a group of portables to give-up membership of one group or all groups (except of course of group "000".) Note that these messages are not acknowledged.

 *Group Membership arrangement is the task of the Messaging Server. IP DECT only forwards the group membership messages to the handsets.*

3.3 How about Normal, Urgent, Emergency Messages

Sending a broadcast message to a handset still supports urgency levels: Normal, Urgent and Emergency. However, there is no B-channel used and there is no acknowledge send back.

Using broadcast messaging the behavior of Normal, Urgent and Emergency messages is as follows:

- **Normal Broadcast Message** - A normal broadcast message appears on the handset as if it is a normal message.

The difference is a technical difference. In case of a normal unicast message the handset will respond and an ACK is sent to the Messaging Server.
- **Urgent Broadcast Message** - When the handset receives a broadcast Urgent message, it appears on the handset as if it is unicast Urgent message. The ringing rhythm is the same. To stop the ringing, the handset user has to acknowledge the message by means of pressing the "OK" or "Delete" button. Note that pressing this button does NOT send a confirmation to the system, it only stops ringing. If the user does not press the "OK" or "Delete" button, the handset will terminate the ringing when a timer in the handset expires. This timer is always longer than 30 seconds and normally shorter than one minute. The time value may be different per handset type.
- **Urgent and Emergency Broadcast Message** - When the handset receives a broadcast Emergency message, it appears on the handset as if it is unicast Emergency message. The ringing rhythm is the same. To stop the ringing, the handset user has to acknowledge the message by means of pressing the "OK" or "Delete" button. Note that pressing this button does NOT send a confirmation to the system, it only stops ringing. If the user does not press the "OK" or "Delete" button, the handset will terminate the ringing when a timer in the handset expires. This timer is always longer than 30 seconds and normally shorter than one minute. The time value may be different per handset type.

SECTION 4 **SIP MESSAGING AND DASGIF MESSAGING (IP DECT REL. 5.00_401 OR HIGHER)**


SIP Messaging and messaging via the DASGIF interface are available in IP DECT. It is important to know how this works together.

When IP DECT is connected to a SIP Proxy that supports SIP Messaging, you can select whether you want to use LRMS or SIP Messaging. It is an option in the DAP Configurator.

When you select "SIP Messaging", the messages from the handset are sent from the DAP where the subscription record resides to the SIP Proxy instead of to the DAP Controller/Manager. It uses SIP instant Messaging. The opposite way around, the SIP Proxy can send messages straight to the DAP where the subscription record resides. This means that the DAP Controller/Manager is not involved in the SIP Messaging.

In a mixed configuration, the following OUTBOUND messaging is supported:

- ☐ **From SIP Proxy to DAP** - Using the SIP instant Messaging - SIP Method "MESSAGE".
- ☐ **From External Messaging Application to the DAP Controller** - From External Messaging Application to the DAP Controller. In the External Messaging Application, there is the Application Interface component called CTI or DMLS as interface between the Messenger Application and the DASGIF interface to the DAP Controller.

 *Both incoming messages as mentioned above, will always work, independently of settings in IP DECT.*

In a mixed configuration, the following INBOUND messaging is supported:

When a handset sends a message, the destination of the message is determined by a number of conditions. This is shown in [Figure E-2 Outbound Messaging from Handset](#).

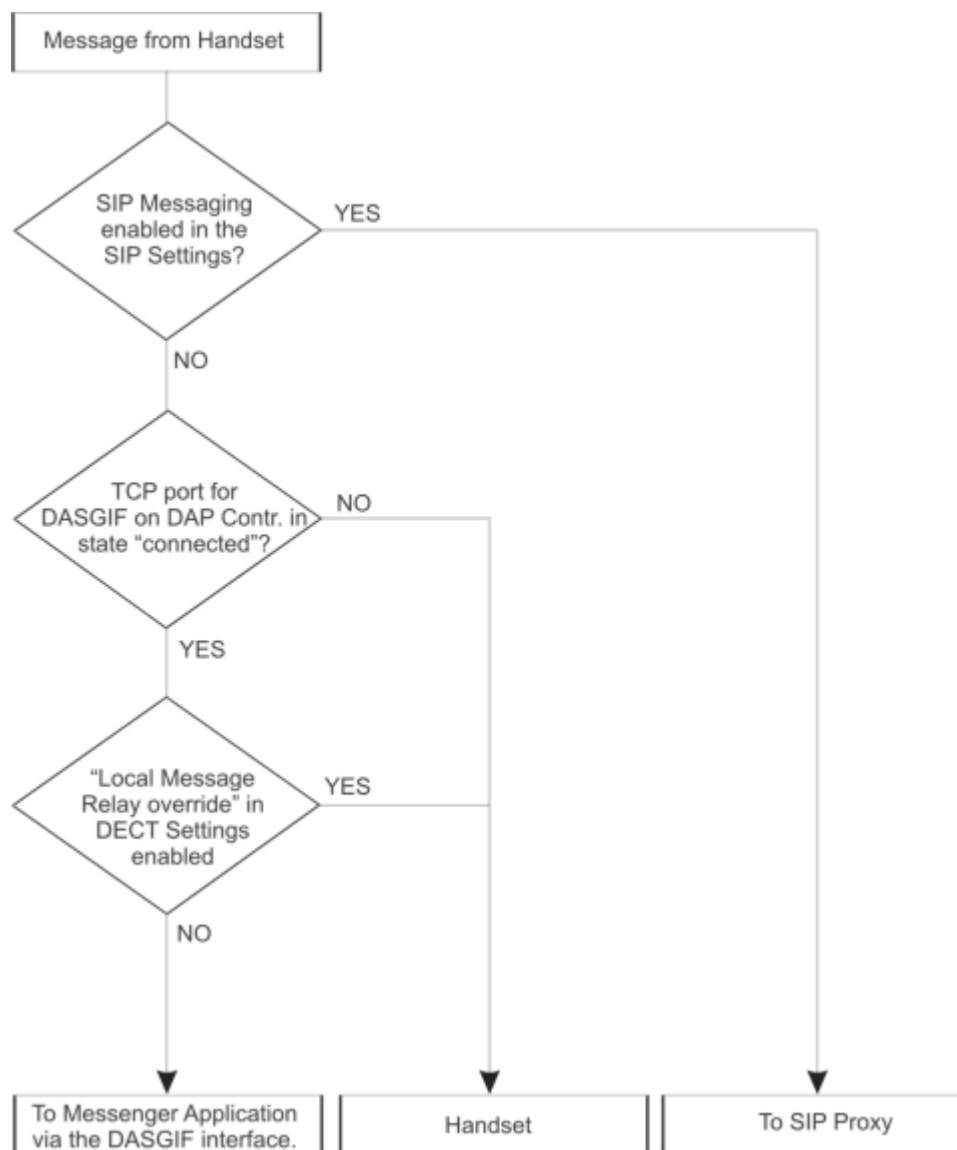


Figure E-2 Outbound Messaging from Handset

THIS PAGE INTENTIONALLY LEFT BLANK

Handset Mobility on iS3000

SECTION 1 **GENERIC INFORMATION**

When using IP DECT SIP on an iS3000, it is possible to use handset mobility. There are two types of mobility:

- ☐ MAN - Metropolitan Area Network. This allows roaming between iS3000 Units.
- ☐ WAN - Wide Area Network. This allows roaming between iS300 nodes having a QSIG connection or a DPNSS connection.


As a matter of fact, this type of roaming already existed for traditional DECT as well as IP DECT using iTMP.

The following system type and combinations are possible:

- ☐ IP DECT SIP with Branch Offices - Please note that when you have IP DECT SIP roaming, the DAPs of all location must be in the same IP DECT System. This means that you have one IP DECT system with Branch Offices in the other locations/sites.
- ☐ IP DECT SIP with Branch Offices and Traditional DECT - This is the same as mentioned in the bullet above, but now Traditional DECT is also involved. Please note that you can have only one IP DECT SIP system with or without Branch Offices on other locations.

The Traditional DECT system must be adapted (Signalling Group adaptation) because you must setup communication between the traditional DECT system and the DAP Controller.

Also please note that the DAP Controller must be up and running permanently.

-  *Except for the above mentioned configurations, other mobility configurations are not possible. So, combinations of IP DECT SIP with IP DECT iTMP are not possible.*

SECTION 2 SOFTWARE REQUIREMENTS

Your system must have the following minimum software versions:

- ☐ iS3000 software SIP@NET 4.3.E.
- ☐ DAP Controller Software Release 5.0, build 411 or higher
- ☐ DAP Software Release 4910b510.dwl

SECTION 3 HOW TO SET IT UP

3.1 IP DECT SIP With Branch Offices

Using Mobility, you can have only one IP DECT SIP configuration over all the Units (MAN) or over all the Nodes. This means that you will have an IP DECT Head quarter (main site) and Branch Offices. It is not possible to have more than one IP DECT system!

3.1.1 Setting up IP DECT SIP Mobility with Branch Offices

1. Determine your IP Network topology. Where do you want to have the Head quarter and where the Branch offices. Think about your IP Network structure. Remember that you must have Routers between the head quarter and the Branch Offices and between the individual Branch Offices.
2. Consult the IP DECT Customer Engineer Manual for iS3000 for the description of the IP DECT Mobility. Setup the Mobility as described in that manual. However, be aware of the fact that you must assign the extension numbers to the virtual SIP circuits in the iS3000. Assigning the extension numbers is described in the following steps.
3. For MAN/WAN mobility, it is required that for every DECT DNR subjected to Mobility there is a virtual SIP extension circuit in each Unit/Node where Mobility is required. So, make sure that you have setup the SIP configuration in your iS3000.
4. For MAN: assign the DNR to the virtual circuit that you want to use for Mobility in one of the Units.
5. For WAN: assign the DNR to the virtual circuits that you want to use for Mobility in all Nodes.

Example for DNR 1000

CHDNRC:1000,15,2,0;

6. Assign the alternative user name to the virtual circuits that are used for IP DECT SIP in all Units/systems involved. The alternative user name for IP DECT SIP Mobility must comply with the following combination DECT<DNR>.:
For example:

CHSUSR:15,2,0;

PASSWORD::

ALTERNATIVE-USERNAME:DECT1000;

3.2 IP DECT SIP With Branch Offices and Traditional DECT

Using Mobility, you can have only one IP DECT SIP configuration over all the Units (MAN) or over all the Nodes. This means that you will have an IP DECT Head quarter (main site) and Branch Offices. It is not possible to have more than one IP DECT system!

This IP DECT configuration should work together with the traditional DECT installation. This means that you must setup IP DECT SIP as described in the previous sub-section and you must add the Traditional DECT configuration to it.

3.2.1 Setting up Traditional DECT to Work with IP DECT SIP

Make sure that you have followed the procedure [3.1.1 Setting up IP DECT SIP Mobility with Branch Offices on page F-2](#) in the previous sub-section. If you have only one Unit or Node having IP DECT SIP, then execute the procedure for that unit only.

1. Make sure that there is IP connectivity between one DCC-8(R) and the DAP Controller.
2. Add the IP Address of the DAP Controller to the DECT Signalling Group in the iS3000. Use OM command CHPMPD. The IP address must be entered into byte 22 . . . 25 of signalling group 960x.

Example for IP address 192.168.1.1:

CHPMPD:0,9600,,,<unit>;

ITEM-NR>,BIT/BYTE>,<DATA>:22,1,192;

ITEM-NR>,BIT/BYTE>,<DATA>:23,1,168;

ITEM-NR>,BIT/BYTE>,<DATA>:24,1,1;

ITEM-NR>,BIT/BYTE>,<DATA>:25,1,1;

ITEM-NR>,BIT/BYTE>,<DATA>;

3. Also you must enter the port number for the port on the DAP Controller.

CHPMPD:0,9600,,,<unit>;

ITEM-NR>,BIT/BYTE>,<DATA>:26,1,109;

ITEM-NR>,BIT/BYTE>,<DATA>:27,1,105;

ITEM-NR>,BIT/BYTE>,<DATA>;

4. To make the settings active execute a warm start.

STWARM;;

5. Make sure that the DAP Controller stays up-and-running permanently.

Overview Of Default Used IP Ports

Table D-1 Default ports used in Business Mobility IP DECT gives an overview of the default ports used in a Business Mobility IP DECT configuration.

Table D-1 Default ports used in Business Mobility IP DECT

Protocol	Interface/Device	Default Destination Port
DHCP	DHCP Server	67
	DAP	68
Proprietary IP DECT protocol and messaging (port 28001).	DAP Controller	28000-28017
IP DECT Proprietary signalling (IP Unicast and IP Multicast), SIP Protocol and RTP (Real Time Protocol)	DAP	3000-22635
TFTP	TFTP Server	69 (only for initial communication) then:1024-65535

THIS PAGE INTENTIONALLY LEFT BLANK

UNIVERGE SV8100

IP DECT Installation Guide