



NORTEL

Nortel Communication Server 1000

SIP DECT Fundamentals

Release: 5.5

Document Revision: 01.07

www.nortel.com

NN43120-123

Nortel Communication Server 1000
Release: 5.5
Publication: NN43120-123
Document release date: 6 January 2009

Copyright © 2008-2009 Nortel Networks
All Rights Reserved.

Sourced in Canada

LEGAL NOTICE

While the information in this document is believed to be accurate and reliable, except as otherwise expressly agreed to in writing NORTEL PROVIDES THIS DOCUMENT "AS IS" WITHOUT WARRANTY OR CONDITION OF ANY KIND, EITHER EXPRESS OR IMPLIED. The information and/or products described in this document are subject to change without notice.

Nortel, the Nortel Logo, the Globemark, SL-1, Meridian 1, and Succession are trademarks of Nortel Networks.

All other trademarks are the property of their respective owners.

Contents

New in this release	7
Other changes	7
Product overview	9
Navigation	9
Overview of SIP DECT	9
Types of SIP DECT configuration	12
Universal extension support	14
DECT handset features	16
CallPilot and Message Waiting Indication support	16
SIP DECT capacity limitations	17
Site planning	19
Navigation	19
Site planning overview	19
Position and use of available cabling	20
Radio coverage	20
Number of handset users	21
Site survey example	21
A normal site survey	21
Site planning example: Able-Studio	22
The facts for Able-Studio	22
The site survey process for Able-Studio	22
DAP deployment rules and requirements	27
Radio synchronization	27
IP network configuration	31
DAP power configuration	34
Initial critical points on the floor plan to identify	34
Rules and guidelines to locate cell centers	35
Coverage and signal strength calculation	37
Determine cell boundaries	38
Identify critical points and cell boundaries	39
Mark the points, centers, and boundaries on the floor plan	40
Deployment illustrations	42
Deployment terms	50

Coverage terms	51
Deployment tool	52
Prepare the tool for deployment	54
How the deployment tool works	61
Using the deployment tool	62
Handset tones interpretation	63
Rules for outdoor deployment	63
DECT Deployment Kit 2	64
DAP deployment	67
Correct audio quality problems	71
Single and multiple floor deployment	72
Single floor deployment	72
Multiple floor deployment	78
Reengineer cells for high traffic areas	83
Traffic volume	83
The cell reengineering process	83
Cell division requirements in special cases	92
No office information	92
A mix of users with and without wired telephones in a cell	93
High handset density deployment	95
Limit the anticipated number of handsets	95
Subdivide a cell	95
Deployment review	97
Floor plan completion	97
Hardware installation	99
Navigation	99
Call server	99
Signaling server	99
PC (DAP controller)	100
DECT Access Points	100
Software requirements	103
Navigation	103
Call server software	103
Signaling server software	103
DAP controller software	103
Firewall protection	104
Internet information services	105
DHCP and TFTP servers	111
DAP Controller	130
System configuration	135
Navigation	135
Simple SIP DECT configuration	135

- Configuration of settings using IP DECT Configurator 136
- DAP manager configuration 150
- Configuration on Element manager 154
- NRS configuration 163
- Call server configuration 170
- Routed Head Quarter configuration 173
 - Choice of system configuration 174
- Multi site mobility network configuration 175
 - Subscribe a multi site DECT handset 176
 - Import and export subscriptions 177
 - Configure NRS for multi site mobility network 178
 - Call server configuration to MSMN 179
 - Configuration of Personal Call Assistant 182
 - Configuration of Universal Extension (UEXT) on the remote system 182

System administration

185

- Navigation 185
- DAP manager overview 185
- Subscription management 187
 - Subscribe a handset 187
 - Edit a subscription RPN 188
 - Disable a subscription 189
 - Remove a subscription 190
 - Delete a number 190
 - Use the DNR filter 191
 - Handset status 192
- DAP management 194
 - Change a DAP Radio Part Number (RPN) 194
 - Reboot a DAP 195
 - Reboot all DAPs 195
- Add a DN range 196
- Back up and restore subscriptions 197
- Subscription export and import 198
 - Export subscriptions 199
 - Import subscriptions 201
- DAP reboot history 202
- System archive 202
- Handset firmware update 204
- Central directory access tool 208
 - Supported database types 209
 - Installation 210
 - Configure SIP DECT for Central directory access 213

System maintenance

215

- Navigation 215

DAP LED indications	215
DAP firmware update	216
Remove and replace a DAP (if a new DAP is available)	217
Remove and replace a DAP (if a new DAP is not available at the moment)	218
System synchronization analysis	219
Synchronization Analyzer interface	220
Export and import SIP DECT system	228
Export a system	228
Import a system	229
DAP Controller deactivation	230
DAP Controller software deinstallation	230
DAP Controller software update	231
Troubleshooting	232
If DAP is not working	232
If you cannot make calls from a DECT handset to an IP/TDM telephone on the call server	233
If you cannot make calls between DECT handsets	234
If you have problems	236
System survey	236
System archive	238
Network packet capture traces	238

Location builder tool

239

Use the Location builder tool	239
Create a location file	241
Maintenance	246

New in this release

Nortel Communication Server 1000 (CS 1000) Release 5.5 introduces Nortel Session Initiation Protocol (SIP) Digital Enhanced Cordless Telecommunications (DECT). SIP DECT includes new SIP DECT Access Points (DAP).

Other changes

This section describes the detailed history of past releases of this document.

Revision History

Date	Description
January 2009	Standard 01.07. This document is up-issued for Release 5.5 with editorial changes.
December 2008	Standard 01.06. This document is up-issued for Release 5.5, in response to change requests for content related to SIP DECT 4.1.
July 2008	Standard 01.05. This document is up-issued in response to change requests.
July 2008	Standard 01.04. This document is up-issued in response to change requests.
May 2008	Standard 01.03. This document is up-issued in response to change requests.
March 2008	Standard 01.02. This document is up-issued in response to change requests.
February 2008	Standard 01.01. This is a new document issued to support Communication Server 1000 (CS 1000) Release 5.5. Some of the information in this new document was previously contained in the following document: <i>DECT Fundamentals</i> (NN43120-114).

Product overview

Navigation

This chapter contains information about the following topics.

- [“Overview of SIP DECT” \(page 9\)](#)

Overview of SIP DECT

You can use Nortel Session Initiation Protocol (SIP) Digital Enhanced Cordless Telecommunications (DECT) to move without restriction about your work site while conducting telephone conversations, using wireless handsets. The Nortel SIP DECT system includes one or more DECT access points (DAPs or basestations) connected to the TLAN.

A minimal SIP DECT system has the following five main components.

- Call Server
- Signaling Server
- PC with DAP controller software installed
- DAP
- handset

Use the following four tools to configure an IP DECT system.

- Element manager or overlay program for Call Server
- Element manager and, if required, Network Routing Service (NRS) manager for Signaling Server
- IP DECT Configurator
- DAP manager IP DECT

Note: The IP DECT Configurator and the DAP manager IP DECT are available as a part of the DAP controller software package.

The following software releases are required on the main system components.

- Call Server, Release 5.5
- Signaling Server, Release 5.5
- DAP software 4910b414.dwl or later
- DAP controller 4.1 or later (PC software)

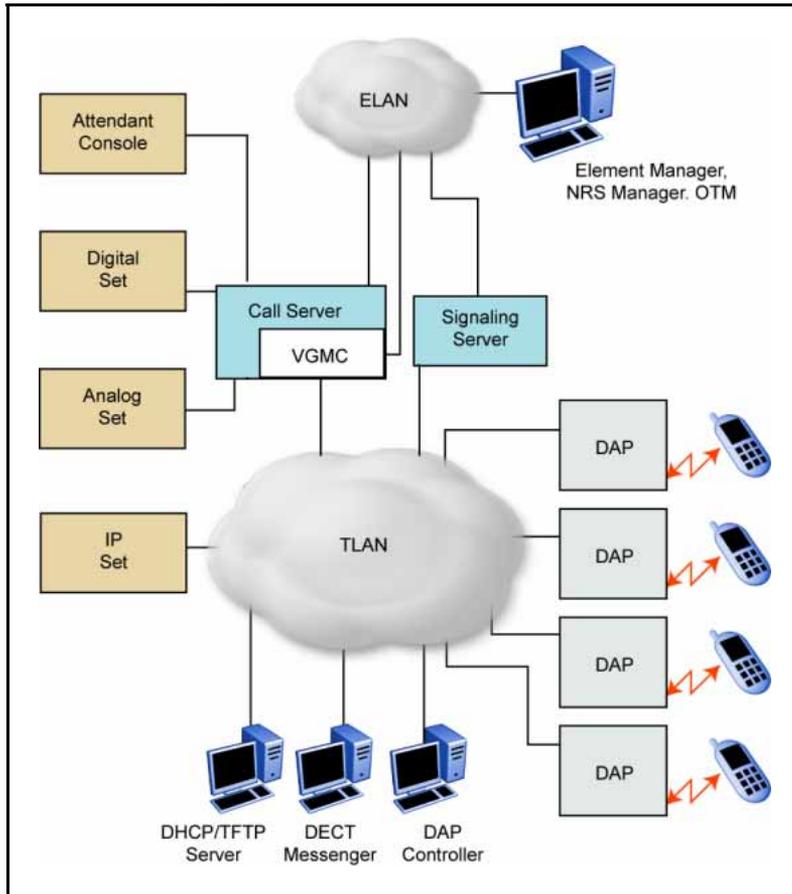
You can connect IP phones to the TLAN, connect TDM phones to the Call Server, Voice Gateway Media Cards and other required cards in Call Server. Use Voice Gateway Media Cards for IP-to-TDM calls and for conference calls involving IP phones or DECT handsets on basestations. The configuration can also include a PC with DECT Messenger to provide the DECT messaging service on SIP DECT.

Note: For SIP DECT to function properly, you must install a dedicated Signalling Server running the SIP Gateway application. Other applications, such as H323 Gateway, NRS, and IP Phones, can be used on the same Signaling Server without limitations.

Use the Dynamic Host Control Protocol (DHCP) server or the Trivial File Transfer Protocol (TFTP) server unless you use a DAP configuration without DHCP or TFTP. You can configure the system to use two separate servers; one for DHCP and the other for TFTP. If the system requires DAP configuration without DHCP or TFTP, the DHCP or TFTP server is required during installation or configuration changes.

Figure 1 "SIP DECT configuration" (page 11) shows a general SIP DECT system configuration.

Figure 1
SIP DECT configuration



You can install the DHCP or TFTP services, DECT Messenger, and DAP controller on a single server or PC. However, you can also choose to install them on separate servers to enhance performance or facilitate administration. You can also install Element manager, NRS manager, and OTM on the same server, provided that the server has both a TLAN network interface and an ELAN network interface. If the server you use is incapable of supporting all of these applications, you can use more than one server.

You connect the DAP to the Communication Server 1000 using the SIP trunks that you configure between the DAP and the Signaling Server. Each DAP communicates with the subscribed DECT handsets in its coverage area, and it interacts with the Communication Server 1000 and with other configured DAPs in the company network.

You can run SIP DECT on the following configurations.

- Communication Server 1000M or Communication 1000E
- Signaling Server running SIP Gateway

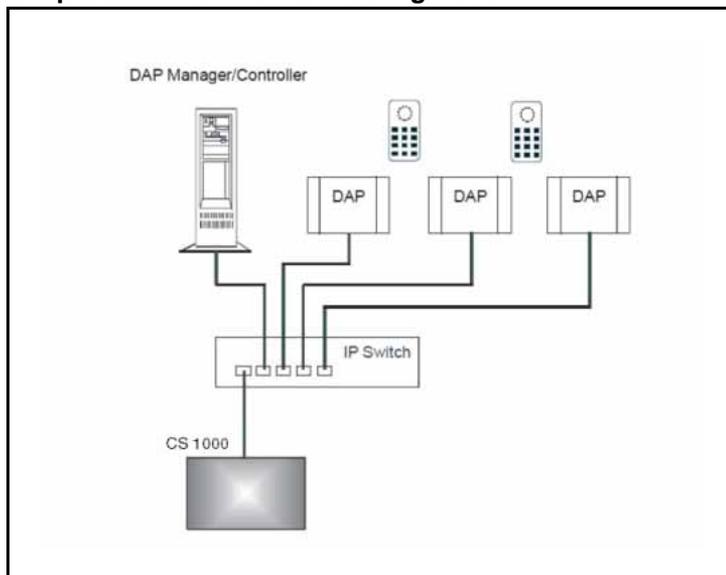
Use the SIP Redirect Server or SIP Proxy Server to perform the appropriate NRS configuration for SIP DECT. You can run SIP Redirect Server on Internet Server Platform (ISP) 1100, Call Processor Pentium Mobile (CP PM) signaling server, or on IBM or HP Commercial-off-the-shelf (COTS) servers under VxWorks. You can run SIP Proxy Server on IBM or HP COTS servers under Linux. You can run SIP Redirect Server on the same Signaling Server as SIP Gateway dedicated to SIP DECT, or you can run SIP Redirect Server on a stand-alone Signaling Server. If you install SIP Proxy Server you must use a stand-alone COTS server. You cannot run SIP Gateway on the same server as the SIP Proxy Server.

Types of SIP DECT configuration

Nortel SIP DECT can be implemented in various system configurations to accommodate your needs. The most common Nortel SIP DECT system configurations are as follows:

- Simple SIP DECT configuration provides seamless hand over between DAPs. A simple SIP DECT configuration is shown in [Figure 2 "Simple SIP DECT network configuration"](#) (page 12).

Figure 2
Simple SIP DECT network configuration



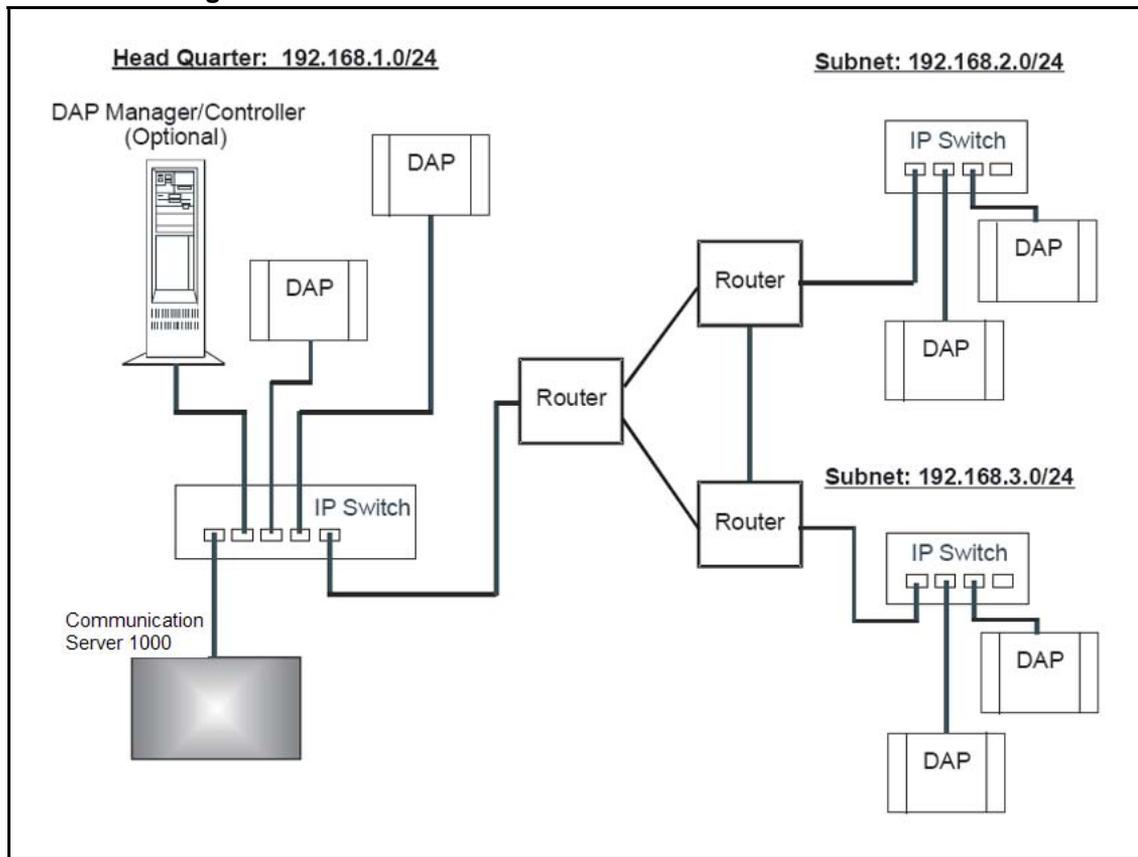
In simple DECT configuration, configure all SIP DECT devices in one subnet based on one or more IP switches, which must support IP multicast. Configure the switches as follows.

- Disable IGMP Snooping.
- Disable Spanning Tree Protocol (STP) on switch ports where SIP DECT equipment connects
- If the switches serve more than one Virtual Local Area Network (VLAN), configure all SIP DECT devices in one VLAN, so they behave as one subnet

- **Routed Head Quarter configuration**

A Routed Head Quarter configuration provides seamless hand over between DAPs. A Routed Head Quarter configuration is shown in Figure 3 "SIP DECT configuration Routed Head Quarter" (page 13).

Figure 3
SIP DECT configuration Routed Head Quarter



Routed Head Quarter configuration requires different subnets connected using one or more routers. The subnets in the network must be part of one company network, and if you configure the subnets in this fashion, SIP DECT behaves as one large SIP DECT system. Use SIP DECT Routed Head Quarter configuration for a large campus network that is split into different geographical subnets. The campus must meet the following requirements.

- The network must support Quality of Service (QoS) and IP connectivity throughout the Campus.
- Routers must support IP multicast routing.
- The IP multicast address for SIP DECT must be the same in all subnets.
- multicast Time to live (TTL) must be greater than 1.
- In the SIP DECT configuration, you must enter the subnet mask for all networks, for example, 255.255.248.0.

Universal extension support

DECT handsets subscribed on DAPs are external to Communication Server 1000. The Communication Server 1000 does not control the state of DECT handsets. Therefore, the Communication Server 1000

- cannot detect individual key-presses on DECT handsets
- cannot control cadences on DECT handsets
- cannot detect if a DECT handset is switched off and on
- cannot control the handset display content

A DECT handset subscribed on a DAP cannot use the same range of features available to analog, digital, or UNiStim IP phones on the Communication Server 1000.

Configuration and status information for subscribed DECT handsets is provided using the Universal Extension (UEXT) feature on the Call Server.

No Associated Telephone (AST) or Computer-Telephone Integration (CTI) capabilities are available for SIP DECT at the present time.

Each DECT handset has a local Directory Number (DN) in Communication Server 1000. Use this local DN to subscribe the corresponding DECT handsets on the SIP DECT system through SIP DECT manager. SIP DECT manager is available on the server where you installed the DAP controller.

Configure the UEXT associated with a DECT handset as follows.

- For the Primary DN of the UEXT (key 0 SCR), enter the local DN associated with the DECT handset.
- For the Target DN of the UEXT (key 1 HOT P), enter the digits required to access the SIP route (SIP Trunks) configured to access DAPs, plus the local DN of the handsets. This consists of one of the following.

- For access based on the configured Coordinated Dialing Plan (CDP), compose the Target DN as follows. <TSC>+<LOCAL DN>.
- For access based on the configured Uniform Dialing Plan (UDP), compose the Target DN as follows. <AC1 or AC2>+<LOC>+<LOCAL DN>.

A UEXT corresponding to a DECT handset on the SIP DECT system reflects the idle or busy status of the associated handset by a check for a call processed between the handset and a DAP.

The Nortel Integrated SIP DECT system provides the following UEXT features.

- Making and receiving simple calls
- Call Hold. There can be only one active call and one call on hold for a handset
- Consultative or Announced Call Transfer
- Blind Call Transfer
- Participation in a conference call if another party adds the DECT handset to the conference
- Calling Line ID (CLID) and Calling Party Name Display (CPND) for simple calls not involving call transfer
- CLID and CPND for an internal line (digital or IP phone with display) calling to, or receiving a call from a DECT handset
- Sending DTMF tones through the established connection to interact with the called line (party), for example, to work with CallPilot
- Support for a voice mailbox on CallPilot and MWI
- Call Forward No Answer
- Call Forward By Time of Day
- Call Forward Busy
- Hunting
- Call Restrictions applicable to a UEXT
- Twinned configuration (typically a desk phone plus a DECT handset)

DECT handset features

The user of a DECT handset subscribed on SIP DECT can do the following.

- Make calls to valid DNs except restricted or blocked DNs.
- Receive and answer calls from the Call Server. If CPND is available, the name of the caller and DN appear on the handset display. The position and appearance of the name DN on the display depend on the firmware installed on the handset.
- Put the active call on hold by pressing the **R** key on the handset. Return to the held call by pressing the **R** key. If a call is put on hold, another call can be made from the handset. After the second call is established, the user can switch between the two calls with the **R** key.
- Transfer a call to another DN
 - To perform a Blind Transfer
Put the current call on hold, call the required DN and immediately release from the call.
 - To perform a Consultative Transfer
Put the current call on hold, call the required DN, wait for the answer and release the call after the DN answers.
- Press digit keys on the handset during an established call. DTMF tones are sent to the other party on the call.

You cannot use a DECT handset to configure Call Forward or Hunting, or to configure Call Restrictions. You can configure these options from the Call Server using overlays, or if a twinned configuration is used, the twinned desk phone can be used to configure Call Forward for its Primary DN with the existing keys or with Flexible Feature Codes (FFC).

CallPilot and Message Waiting Indication support

CallPilot can be used with DECT handsets subscribed on SIP DECT.

Call Forward No Answer can be configured for the Primary DN of the UEXT so that the calls which are not answered on the corresponding DECT handset or IP phone (in the case of a twinned configuration) are forwarded to CallPilot. Calls can also be forwarded to CallPilot as busy treatment for the Primary DN.

The CallPilot system can be called from a DECT handset and the user of the handset can login to the voice mailbox with the corresponding DN and password. The user can then use the voice menus of the system as usual.

Message Waiting Indications can be sent to the DECT handset through the SIP Trunk. This is achieved by configuring additional DNs (to which CallPilot sends MWI) for the voice mailbox corresponding to the UEXT

Primary DN. The additional DN configured in CallPilot is the external DN of DECT handset, that is, the Target DN on the UEXT corresponding to the DECT handset.

Communication Server 1000 only supports the so-called Unsolicited MWI NOTIFY model

An external SIP UA cannot SUBSCRIBE to MWI NOTIFY messages and cannot request the current status of MWI for the DN from the system (by sending SUBSCRIBE messages). Instead of that a SIP UA has to be ready to get MWI NOTIFY messages from system even if it did not SUBSCRIBE to those and it has to update MWI according to those messages only.

Due to the Unsolicited MWI NOTIFY model in Release 5.5, the DECT handset can only rely on the MWI notifications sent by Communication Server 1000. Therefore, the MWI indication based on that existing mechanism may not be in the correct state on the DECT handset if the handset was turned off and then turned on. Also, the MWI indication may not be in the correct state if the user of the handset goes out of the coverage area of the SIP DECT system and then enters the coverage area again. In such a situation, the MWI indication on the DECT handset is guaranteed to be in the correct state only after the next MWI state change happens in the CallPilot system.

If a twinned configuration is used for a DECT handset, the corresponding IP or TDM phone always correctly reflects the current state of MWI, assuming that it receives MWI notifications for its Primary DN from CallPilot.

SIP DECT capacity limitations

The following capacity limitations apply to SIP DECT.

- a maximum of 12 simultaneous calls for each DAP
 - a maximum of 256 DAPs on each network (where hand over and synchronization between DAPs is possible)
 - a maximum of 6000 DECT handsets on each SIP DECT system (there can potentially be several isolated SIP DECT systems connected to Communication Server 1000)
 - a maximum of 1000 simultaneous calls on each network
 - a maximum of 25 subscription records for each DAP
- If the planned number of DECT handsets in a SIP DECT system is equal to M, and the number of DAPs in that system is equal to N, M must be less than or equal to $N \cdot 25$.

Consider the following additional capacity limitations based on the Communication Server 1000 configuration characteristics.

- The number of available UEXTs is limited by the number of available virtual Telephone Numbers (TN) in the system
- The number of DNs available for DECT handsets depends on the configured dialing plan and the availability of the Directory Number Expansion (DNXP) package (150).

Site planning

Navigation

This section contains information about the following topics.

- [“Site planning overview”](#) (page 19)
- [“DAP deployment rules and requirements”](#) (page 27)
- [“Deployment tool”](#) (page 52)
- [“Using the deployment tool”](#) (page 62)
- [“DECT Deployment Kit 2”](#) (page 64)
- [“DAP deployment”](#) (page 67)
- [“Correct audio quality problems”](#) (page 71)
- [“Single and multiple floor deployment”](#) (page 72)
- [“Reengineer cells for high traffic areas”](#) (page 83)
- [“Cell division requirements in special cases”](#) (page 92)
- [“High handset density deployment”](#) (page 95)
- [“Deployment review”](#) (page 97)

Site planning overview

The site planning process is an information gathering process that begins with a site survey and ends with deploying SIP DECT. The information received in the site survey determines customer requirements and the number of cells required to support traffic.

This section contains information about a key piece of deployment equipment, the DECT Radio Deployment Tool. Deployment is the process of locating basestations at the site. For general information about the deployment process, see [“DAP deployment rules and requirements”](#) (page 27). For more information about how to prepare equipment for deployment, see [“Prepare the tool for deployment”](#) (page 54).

ATTENTION

You can use a location builder tool to plan your site. For details, see [“Location builder tool”](#) (page 239).

Other modules describe in detail the procedures related to deployment. These procedures vary according to site details and user requirements.

Position and use of available cabling

Cables that connect the basestation to the DECT system must meet or exceed the UTP Cat 5 standard. New cabling is required if the existing cabling does not meet the standard.

Radio coverage

A basestation coverage list is required to indicate the following.

- a areas where radio coverage is required;
- b areas excluded from radio coverage due to the proximity of sensitive electronic equipment;
- c areas where radio coverage is not required;
- d areas where radio coverage is not feasible or requires specific basestations;
- e objects inside buildings; and,
- f details of furniture, cupboards, and machinery on every floor of the building

If customers request that the basestation be installed out of sight, do not mount basestations in unsuitable locations, such as behind stone columns, next to air ducts or horizontally on the ceiling. Radio coverage cannot be guaranteed if basestations are mounted in unsuitable locations.

Know in advance where coverage is required. Some examples of coverage areas follow.

- elevators
- stairwells
- washrooms
- outdoor areas

Number of handset users

The following information must be available.

- The number of handset users
- The potential growth of handset users
- The areas of above average and below average traffic density Number of cells required to support traffic

Traffic requirements are determined for each cell. The deployer calculates system requirements to support user traffic.

Customer review

After the site survey and before the deployment process, the person deploying the site must review coverage requirements with the customer representative. The person deploying the site must explain to the customer representative how the survey is conducted. The customer representative must tell fellow employees that a person deploying the site is taking measurements in their work place.

Site survey example

The site survey process is an information gathering process. The information received in the site survey determines customer requirements and the number of cells required to support traffic.

A normal site survey

The site survey process includes gathering the following.

- Survey materials
- Site contact information
- Site plans or maps
- Building information
- Existing cable information
- basestation radio coverage information
- Handset user information
- Reviewing the work

Methods and examples for surveying more detailed sites are shown in the Detailed Site Planning section of this guide. Use one or more of the following surveying methods in the following site survey.

- Single floor
- Subsequent system installation

- High handset density area
- Multiple systems installation

Site planning example: Able-Studio

This section describes a site survey for Able-Studio, a fictitious company. Follow this example to conduct the site survey.

The facts for Able-Studio

- The contact is Rolf Sundby at 555-0000. A guest lab coat is necessary to be on the site. Get this lab coat from Rolf.
- The sales representative has recommended DECT.
- The location of user offices with wired IP phones often changes within the coverage area.
- Not all users have offices and desk phones. Some users only have handsets.
- The customer does not need coverage in the washrooms.
- The telephone switch room is next to the washrooms.
- The customer has no installation restrictions.

The site survey process for Able-Studio

The technician must gather the following information to conduct a site survey.

- [“Gather survey items” \(page 22\)](#)
- [“Identify site contacts” \(page 23\)](#)
- [“Obtain site plans” \(page 23\)](#)
- [“Gather building information” \(page 24\)](#)
- [“Identify existing cabling” \(page 25\)](#)
- [“Profile handset use” \(page 26\)](#)

Gather survey items

Obtain the following items before beginning the site survey. The items are not customer supplied.

- Pick up the DECT tool kit (consisting of tripod and deployment tool kit).
- Get the appropriate DECT provisioning record.
- Gather a pencil, an eraser, a ruler, and colored pencils.

Identify site contacts

Gather the following information and enter it into the work order and the provisioning records. The installer requires the following information.

Procedure 1
Identifying site contacts

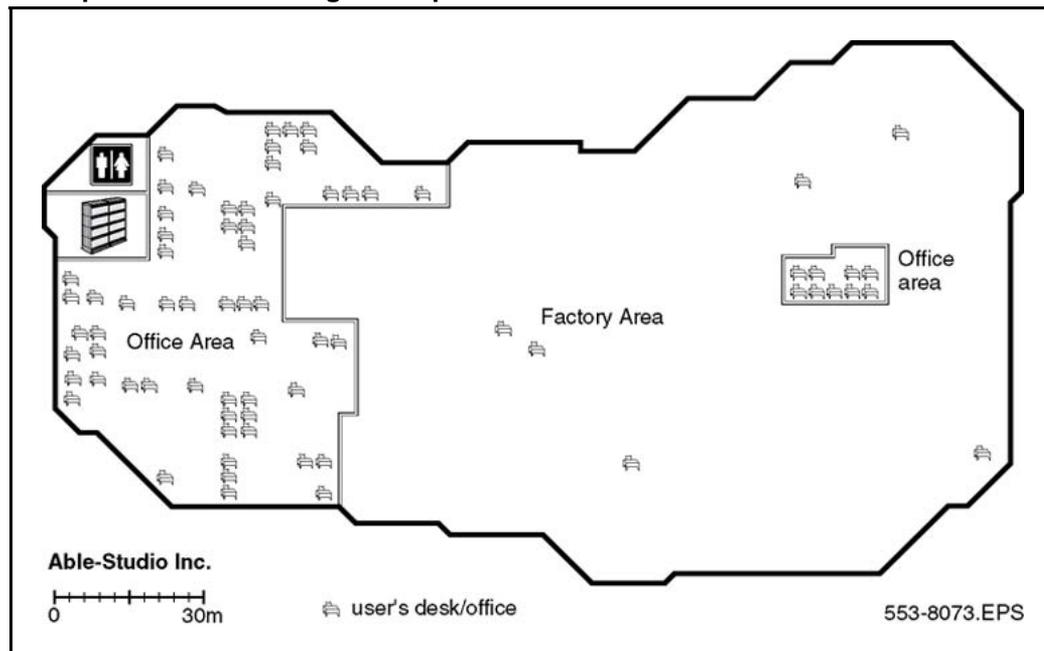
Step	Action
1	Record company name.
2	Record the company address.
3	Record the contact name.
4	Record the contact telephone number.
5	Obtain and record scheduling times and date.
6	Obtain access to controlled areas.
7	Obtain keys or codes you need for secured site areas where radio coverage is required.
8	Obtain and record additional contact information, if required.
9	Obtain the safety equipment you require, such as a hard hat or safety glasses.
10	Record information regarding existing DECT systems in the radio coverage area.

--End--

Obtain site plans

Obtain two scaled plans. You need scale to check wiring distances from the controller to the basestations. The scale is in the form of a measured line so it remains in proportion to the floor plan through reduction copiers.

Figure 4
Example of a site coverage floor plan



Procedure 2
Obtaining site plans

Step	Action
1	Obtain two site plans or maps, with dimensions marked. Use one working copy to identify critical points, cell centers, and cell boundaries. Use one clean copy to attach to the site provisioning record for the installer, customer, or maintenance.
--End--	

Gather building information
 Gather the following information and enter it into the work order.

Procedure 3
Gathering building information

Step	Action
1	Obtain and record building identification.
2	Obtain and record information about construction materials, such as walls, floors, and ceilings.
3	Record the type facilities, such as office, hotel, factory, store.
4	Record the number of floors in the building.

If the building contains atriums, multiple floors, or floors not all the same shape or unusual conditions, see “Multiple floor deployment” (page 78).

- 5 Record the height of floors.
- 6 Record as much information as you can obtain about the partitioning of floors.
- 7 Discuss and record the details of furniture, cupboards, and machinery in the interior of buildings on every floor.
- 8 Ask about other building details as necessary and record this information.

--End--

Identify existing cabling

Gather the following information and enter it into the work order.

Procedure 4 Identifying existing cabling

Step	Action
1	Obtain the location of the telephone switching room.
2	Determine the total length of the existing cable.
3	Ask about the existing cabling from the DAPs to the IP Switch. The wiring from the DAPs to the IP Switch must be at least UTP Cat 5.

--End--

Assess radio coverage

Note: If the customer requires the basestations be installed out of sight, this can reduce the coverage capability of each basestation. It can limit the performance of the system and substantially increase the cost.

Gather the following information and enter it into the work order.

Procedure 5 Assessing radio coverage

Step	Action
1	Record areas where radio coverage is required.
2	Record areas where radio coverage is not required.

- 3 Record external or outdoor radio coverage.
- 4 Record where radio coverage is not feasible or requires specific basestations.
- 5 Record areas excluded from radio coverage due to the proximity of sensitive electronic equipment.
- 6 Record objects inside buildings that can affect radio coverage.
- 7 Record unsuitable basestation locations, such as stone columns, air ducts or horizontally on the ceiling.
- 8 Discuss what basestations are to be installed out of sight.
See the preceding note.
- 9 Inquire about areas of special coverage, such as, elevators, stairwells, and washrooms.

--End--

Profile handset use

Areas of above average traffic density can have a low number of incumbent users but many incoming users. These can include areas such as cafeterias, restaurants, canteens, and meeting room areas where handset users tend to gather.

Another example of above average traffic density is an environment where all occupants of an area are provided with handsets. This area requires special planning.

Areas of below average traffic density are areas users access infrequently, such as store rooms and maintenance areas.

Obtain the following information and enter it into the work order.

Procedure 6 Profiling handset users

Step	Action
1	Record the number of handset users.
2	Record an estimate of the potential growth of handset users.
3	Locate and record areas of above average and below average traffic density.
4	Determine and record which users have a wired IP phone in their office.
5	Determine and record the locations of user offices.

- 6 Ask about and record the mobility of the users. For example, do the users move from cell to cell, or is the area of movement restricted, such that the users remain within one cell?

--End--

DAP deployment rules and requirements

Use the information in this section to plan the deployment of a SIP DECT system, including the locations of basestations and cells. The deployment process consists of the following.

- ["Radio synchronization" \(page 27\)](#)
- ["IP network configuration" \(page 31\)](#)
- ["DAP power configuration" \(page 34\)](#)
- ["Initial critical points on the floor plan to identify" \(page 34\).](#)
- ["Rules and guidelines to locate cell centers" \(page 35\).](#)
- ["Determine cell boundaries" \(page 38\).](#)
- ["Identify critical points and cell boundaries" \(page 39\).](#)
- ["Mark the points, centers, and boundaries on the floor plan" \(page 40\).](#)

Radio synchronization

The radio network structure supports seamless hand over of existing calls. This means that, during a call, if a handset moves from the coverage area of one DAP into the coverage area of another DAP, the new DAP can take over the call. The call is not interrupted, and you are not aware of the hand over. Supporting hand over requires an accurate synchronization of the radio signals in the air. You use radio signals, rather than over the wired network, to perform the synchronization.

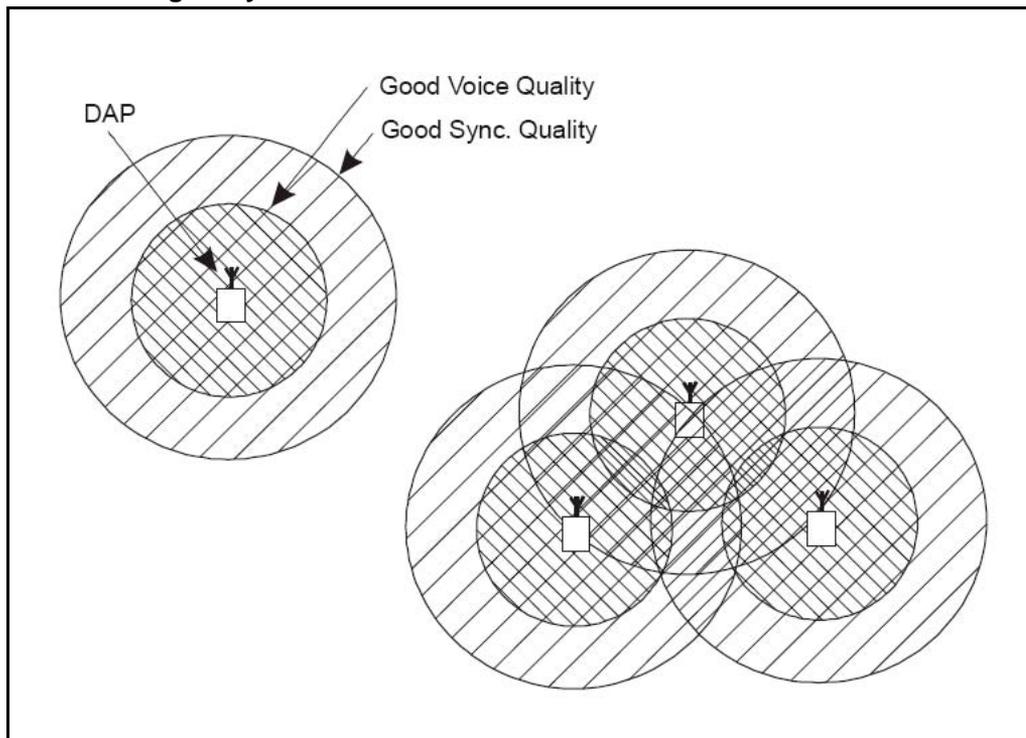
ATTENTION

DAPs must be able to receive synchronization signals from at least one other DAP. If not, the DAP operates in single cell mode and hand over to other DAPs is not possible.

[Figure 5 "DAP radio signal synchronization" \(page 28\)](#) shows two circles around the DAP.

- an inner circle in which there is sufficient radio signal strength for acceptable voice quality
- an outer circle in which there is sufficient signal strength for synchronization, but not enough for acceptable voice quality

Figure 5
DAP radio signal 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 therefore has some overlap with the other cell and reaches to the radio of the other cell. Therefore, the DAPs of the overlapping cells exchange radio signals with each other. These radio signals are weak relative the signal needed by the handsets, but are still strong enough for synchronization purposes.

ATTENTION

For signal strength calculation see [“Coverage and signal strength calculation” \(page 37\)](#).

If one DAP receives a signal from another, the receiving DAP checks the radio signals on Primary Access Right Identity (PARI), to ensure that the signals belong to the same DECT system. If the signals belong to the same DECT system, the DAPs synchronize with each other according to predefined rules.

ATTENTION

If there are two or more independent Nortel SIP DECT systems with overlapping areas of coverage, it is always preferable that you configure these systems so that each system has a unique subset of carriers. When each system has a unique subset of carriers, any unnecessary interference between the systems is avoided.

Note that reducing the number of available carriers reduces the maximum number of simultaneous calls in the DECT system. To achieve your desired call capacity, you can be required to install extra DAPs. See step 4 of [Procedure 52 "Configuring DECT Settings" \(page 143\)](#).

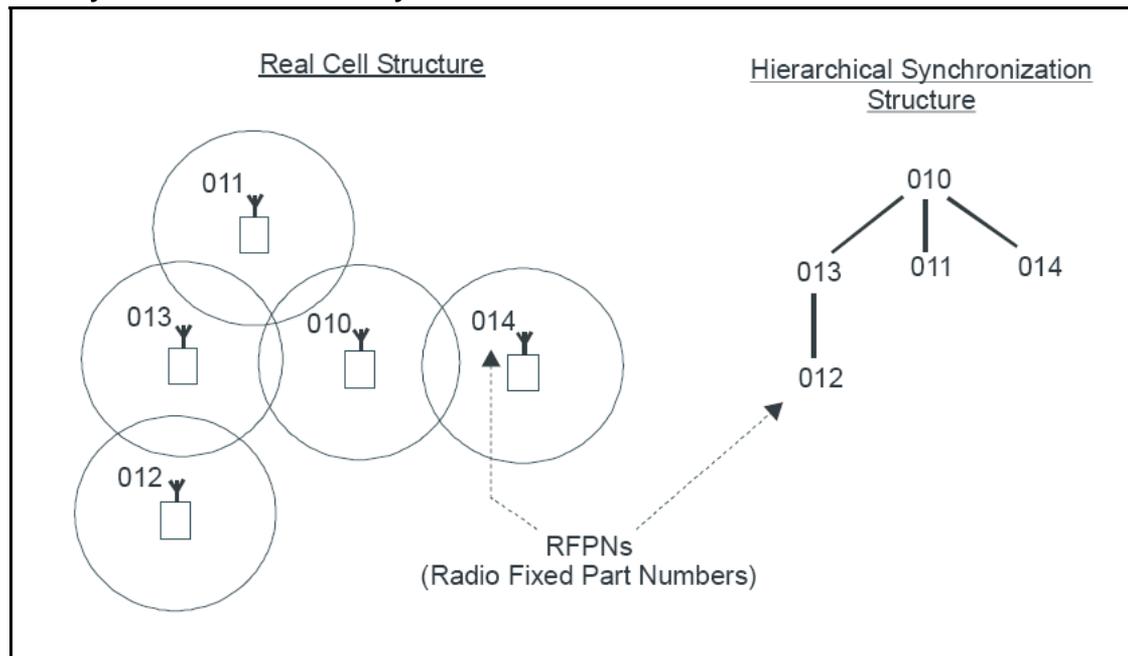
The DAPs transmit with a minimum of two bearers. If there are no voice calls over a DAP, the DAP transmits two dummy bearers. If there is one or more voice calls on the DAP, there is one dummy bearer, plus the voice calls.

Synchronization hierarchy

If two or more DAPs belong to the same system, the DAPS automatically synchronize using a hierarchical structure. In most cases, synchronization is automatic, but if your system has a complex DAP cell structure, configure synchronization manually.

The DAP controller keeps track of the synchronization structure and assigns each DAP a unique Radio Part Number (RPN) after the DAP starts up for the first time. One or more of the DAPs act as a synchronization source, forming the root of the hierarchical structure, as illustrated in [Figure 6 "DAP synchronization hierarchy" \(page 30\)](#).

Figure 6
DAP synchronization hierarchy



If more than one synchronization source is present, each one forms a separate hierarchy of DAPs called a synchronization island.

Automatic synchronization is performed within each synchronization island using the following rules.

- After a DAP starts, it searches for existing DAPs. If it finds one with a lower RPN, it synchronizes with it. If no other DAP exists with a lower RPN, the new DAP becomes the synchronization source.

ATTENTION

It is possible that extra DAPs are required to establish a synchronization path.

- If a DAP detects more than one other DAP, it synchronizes with the DAP that has the shortest path to the synchronization master. If two or more DAPs have the same path length separating them from the master, the new DAP synchronizes to the DAP with the lowest RPN.

ATTENTION

After you install the SIP DECT system, wait at least fifteen minutes until you see the results of the automatic synchronization.

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 using

the DECT manager WEB interface. Automatically assigned RPNs start at 010. If you manually assign a new RPN, ensure that it is in the range 000 . . . 00F.

ATTENTION

It is very important that you determine the position of the Synchronization Master before you start site planning. Place the synchronization master, which is the DAP with the lowest RPN, in the middle of your site, building, or buildings.

IP network configuration

The IP network must be capable of supporting SIP DECT; this section provides more information about planning an IP network that is suitable for supporting SIP DECT.

SIP DECT system typically uses existing IP network infrastructure and facilities for the network connection. For IP connectivity, the network must be configured in such a way that all SIP DECT components have the following characteristics.

- are equipped with unique IP addresses (some static, some dynamic)
- can reach all the required services
- can be reached by all their clients and counterparts

Ethernet requirements

The following items describe the Ethernet requirements.

- The Quality-of-Service that is offered by the IP network must be sufficient for the Voice-over-IP application SIP DECT.
- The IP network must support transparent IP multicast between all DAPs and the DAP controller.
- Connect only one DAP to one IP Switch port.
- DAP supports full duplex and supports autonegotiation if DAP is connected to a port on an Ethernet Switch.

ATTENTION

Autonegotiation must be used on the Ethernet switch ports connected to DAPs. Full duplex can be tried only if the switch does not support autonegotiation. In that case, the correct operation of SIP DECT is not guaranteed and the results can vary for different Ethernet switches.

- Enough unique IP addresses must be available to support both data networking traffic and SIP DECT components. Private IP addresses can be used for local traffic, and private IP addresses on the local network can also be used to connect to public IP addresses if Network Address Translation (NAT) is used. However, NAT is not supported by SIP DECT.

- IP addresses and routing must be consistent with each other to deliver the required transparency. IP addresses must be consistent with routing for normal unicast traffic as well as for the required multicast traffic.
- The maximum cable length between the DAP and IP network equipment, such as a switch, is 100 meters if a Category 5, unshielded twisted pair half-duplex cable is used. If the required cable length between the IP network equipment and the DAP exceeds 100 meters, use Long Range Ethernet equipment in the connection. Several manufacturers offer such a solution, which allows cable lengths of more than one km.

Fixed IP network addresses

You must provision fixed IP addresses for the following servers.

- **TFTP server**
The TFTP server stores the configuration file and the firmware that must be available to the DAPs. After a DAP starts up, the DHCP server sends the DAP the IP address of the TFTP server. The DAP then downloads the configuration files from the TFTP server. The TFTP server often runs on the DAP controller or manager PC.
- **DNS server (optional)**
The DHCP server sends the address of the DNS server to the DAP. The DAP does not support Domain Name Resolution.
- **DAP controller or manager**
The DAP controller or manager requires a fixed IP address. The DAPs retrieve this fixed IP address from the configuration file that the DAP loads from the TFTP server.
- **Gatekeeper and PABX address.**
The IP address of the PABX must be reachable either through a router or directly.
The PABX is sometimes referred to as Gatekeeper or SIP proxy, depending on the type of PABX that is used.

To make network management easier, it is recommended that fixed IP addresses are also assigned by the DHCP server. The DHCP server must know the hardware MAC addresses of all servers, to be able to assign the proper (fixed) IP addresses to each individual server.

It is possible to store the IP address of the DAP in its Flash memory. If the IP address is stored, the DHCP server is needed only for the first startup. After that the DAP has its own IP address.

Dynamic IP network addresses

Network stations, which do not act as servers (PC workstations as well as DAPs), can use dynamic IP addresses assigned by DHCP. For dynamic IP addresses, there is no need to specify the MAC addresses of all the network stations in the DHCP server.

The DHCP server must be configured to assign IP addresses from a certain range to unknown MAC addresses. The drawback is that unknown LAN stations get valid IP addresses, which can be a small network security issue. To overcome this drawback, use the Vendor Class Identification in the DHCP server. The DHCP server only issues IP addresses to devices that have the Vendor Class Identification of the DAPs. However, the DHCP server must be capable of making a distinction in Vendor Class Identifications. The Vendor Class Identification of the DAPs is D(ECT)AP 49.

ATTENTION

The DAP chosen as the DAP Redirect Server must have a static IP address. For more information, see [“Adding Gateway Endpoint for DAP redirect server” \(page 166\)](#).

Each DAP in a SIP DECT system is assigned a dynamic IP addresses. You can configure the DAPs to store the IP address in Flash memory, so the DHCP server is required only during the initial configuration of the system.

Multicast addresses

Multicast is used in SIP DECT systems for the following functions:

- Communication between the SIP DECT network components to locate or address a handset.
If a handset must be reached, the request must go to all DAPs simultaneously. For example, if you use the page function during an incoming call, a single multicast message is sent to all DAPs to find the DAP for your handset in a fast and efficient way.
- Seamless hand over from one DAP to the other
If inter-cell hand over is necessary, the media path must be redirected from the existing DAP, to another DAP. A hand over is always initiated by the handset. The handset does request on another DAP (not the DAP where the connection is at the moment). This DAP issues a multicast on the network to find out on which DAP the voice connection exists. The DAP, with the existing voice connection, responds and then the connection can be redirected from the DAP with the existing voice connection to the new DAP.

All network components must support forwarding of IP multicast packages. The DAP Configurator proposes a default multicast IP address (239.192.49.49). This is a multicast address in the private multicast IP address range that can be used in private IP networks. If you are not sure you can access this address, contact the local IT manager.

ATTENTION

You must disable IGMP Snooping and Spanning Tree Protocol on switch ports where SIP DECT equipment is connected.

DAP power configuration

DAPs are powered using one of the following methods.

- Locally using an RJ11 connector. The AC voltage must be 40V (+ or - 10%). Use an AC adaptor that provides at least 10 Watts. See [Table 1 "Part numbers" \(page 34\)](#) for part numbers of available AC adaptors.

Table 1
Part numbers

NTCW28AAE5	N0162030	DAP AC/AC adaptor Eur
NTCW28BAE5	N0162032	DAP AC/AC adaptor UK
NTCW28CAE5	N0162033	DAP AC/AC adaptor ANZ

- Through Power over Ethernet (PoE) as defined by IEEE802.3af specifications. The DAPs support both phantom power and power over spare wires. The following specifications are applicable to PoE power.
 - Minimum 36 Volts and maximum 60 Volts of voltage at the DAP
 - Standard RJ45 connector, using the spare wires pins (wires)
 - Maximum cable length of 100 meters

Both phantom power and power over spare wires are provisioned on the same DAP to provide system redundancy. The power provision providing the highest voltage is active. If one of the power inputs fail, the other takes over without service interruption.

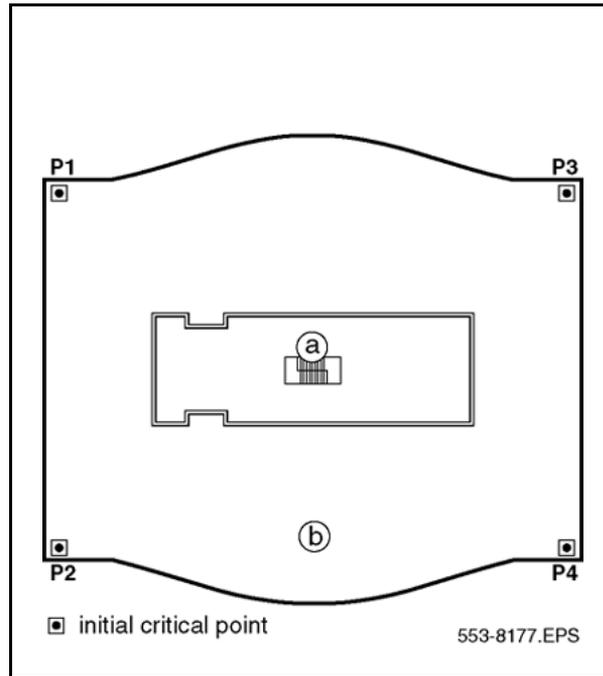
Initial critical points on the floor plan to identify

A critical point is a place that can be difficult for the radio signal to reach, such as a corner of a room, lifts, and stairwells. Initial critical points are shown in [Figure 7 "Critical points" \(page 35\)](#) as P1, P2, P3, and P4.

[Figure 7 "Critical points" \(page 35\)](#) shows the following.

- stairwell
- second floor plan

Figure 7
Critical points



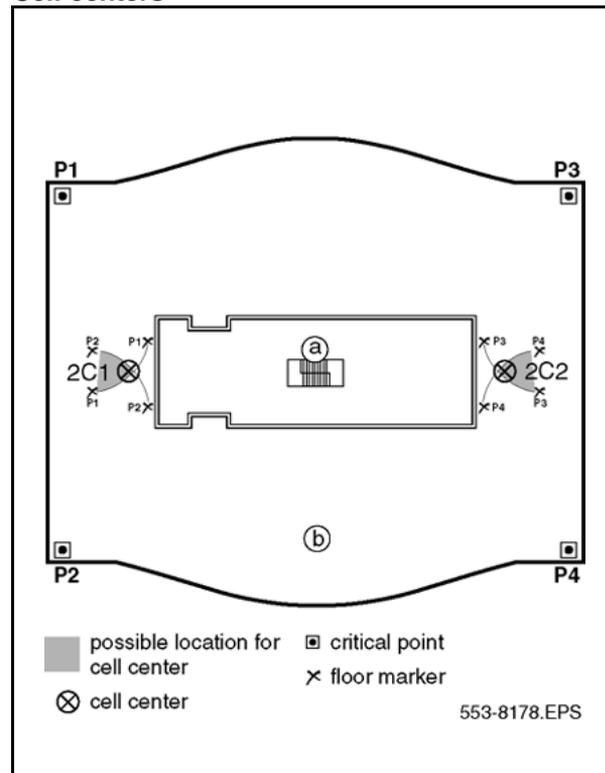
Rules and guidelines to locate cell centers

Figure 8 "Cell centers" (page 36) shows the following.

- stairwell
- second floor plan

To locate a cell center, place the deployment tool at one critical point, for example P1, and then use the deployment handset to obtain a change in audio quality. The audio quality change determines the cell boundary contour. This process is repeated at an adjacent critical point, for example P2. Where the cell boundaries of both critical points meet is the cell center. The cell center position is marked on a floor plan. The cell center determines the location of a basestation, shown in Figure 8 "Cell centers" (page 36), as arc 2C1.

Figure 8
Cell centers



Comply with the following as you select cell centers.

- Ensure that the installation complies with local electrical codes.
- Install basestations indoors where there is no condensation and the temperature remains between 0°C and 40°C.
- Install DAPs in a vertical position. Note that the radiation pattern differs between the horizontal and vertical positions.
- Do not mount a DAP to a metal surface.
- Do not roll up the extra cabling behind a DAP.
- Position basestations upright on walls. Basestations must be at least 30 centimeters from the ceiling.
- Position basestations at least 1 m from large concrete or stone columns and from major building structural members such as support beams or columns.
- Position the basestations high enough to clear obstructions between the basestations and the cell edge close to the ceiling.
- Mount the basestations clear of obstacles such as pipes or ducts.

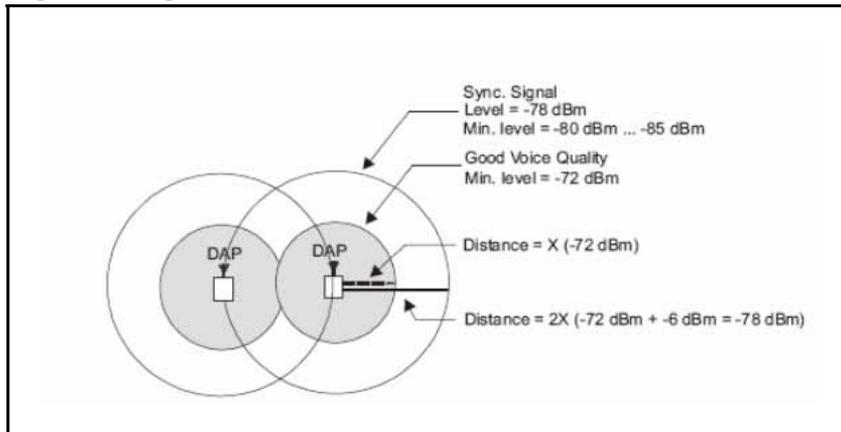
- Do not install basestations in spaces that transport air, such as ducts or plenums.
- Do not mount basestations on the ceiling.

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 an 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 9 "Signal strength considerations"](#) (page 37).

Figure 9
Signal strength considerations



- In an 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.
- Objects between the DAPs can introduce loss. Also, many objects cause reflections that let the signal reach the DAPs through other path with sufficient signal strength.
- In rare cases, factors in the surrounding environment can cause the error rate in the received frames to be temporarily much higher

than is normal for speech. An occasionally elevated error rate does not indicate a problem with your SIP DECT system. However, if you consistently see a high error rate, then there is a problem with the deployment of your SIP DECT system.

Determine cell boundaries

A specific RSSI value on the handset defines the cell boundary range. Links can be made outside the cell boundary but the audio quality of the link is poor. The link drops if the handset and the basestation are too far apart.

ATTENTION

DAPs must be able to receive synchronization signals from at least one other DAP. This means the DAP must receive a signal strength of -80 dBm or better from at least one other DAP.

As shown in [Figure 10 "Cell boundary terminology" \(page 38\)](#), the cell boundary is the furthest point from the cell center where a clear radio signal can be heard.

The range from the cell center to the cell boundary, or the distance to a potential cell center from a critical point, is determined by using the cell boundary value and the deployment tool.

Figure 10
Cell boundary terminology

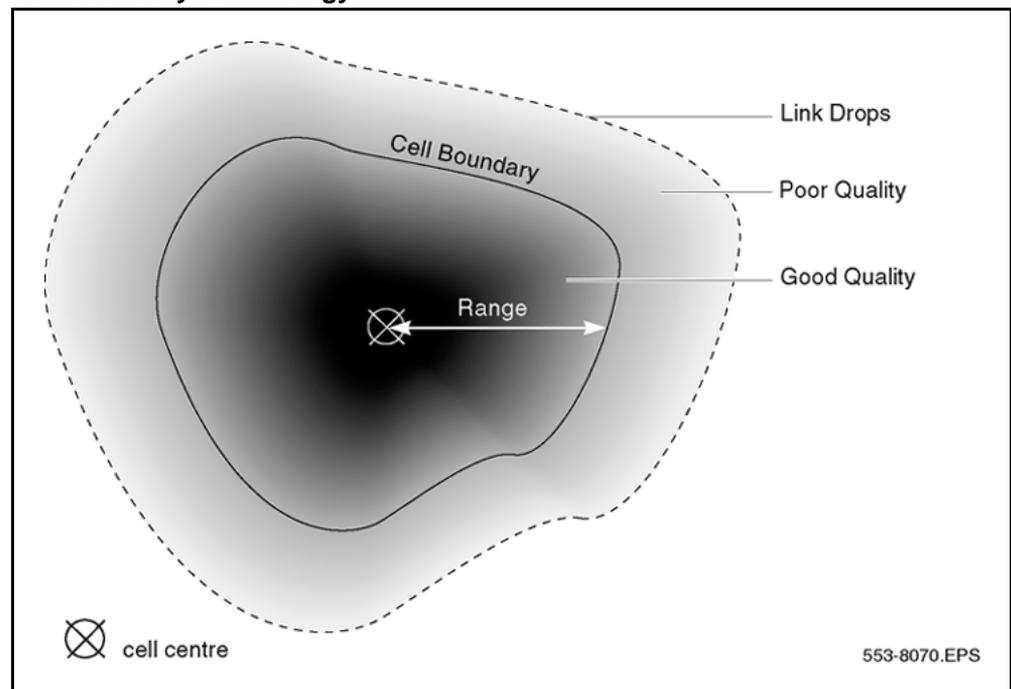
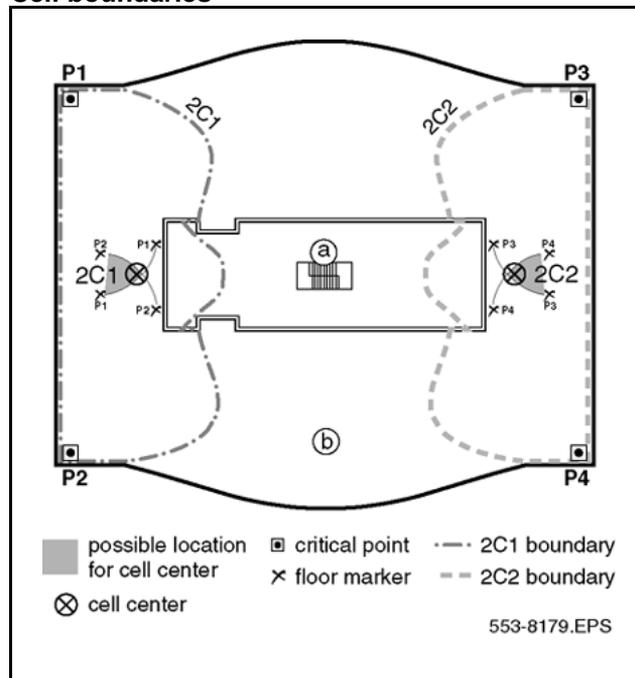


Figure 11 "Cell boundaries" (page 39) shows the following.

A cell boundary for the cell center is determined by placing the deployment tool at the cell center, for example 2C1, and using the deployment handset to establish the cell boundary. The cell boundary contour is marked on the floor plan, and shown in Figure 11 "Cell boundaries" (page 39) by a dash-dot line.

Figure 11
Cell boundaries



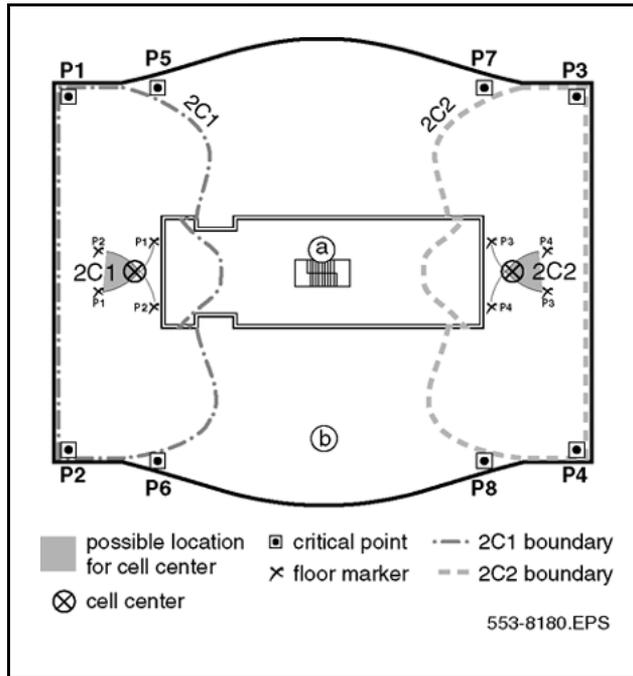
Identify critical points and cell boundaries

Figure 12 "Additional critical points and cell boundaries" (page 40) shows the following.

- stairwell
- second floor plan

Additional critical points, shown in Figure 12 "Additional critical points and cell boundaries" (page 40) as P5, P6, P7, and P8, are identified to ensure basestation radio coverage for the entire area.

Figure 12
Additional critical points and cell boundaries



Mark the points, centers, and boundaries on the floor plan

This section describes how to label critical points, cell centers, and cell boundaries on the floor plan.

Mark the information clearly on the floor plans during the survey. The customer, the sales group, the installer, and maintenance personnel must read these floor plans.

Use a different color for each cell. Use the same color for each cell center and its corresponding cell boundaries. Label the floor plan using the conventions described in [Table 2 "Floor plan markings" \(page 40\)](#).

Table 2
Floor plan markings

Marking	Description
⊗	Mark each cell center on the floor plan using this symbol.
◻	Mark each critical point on the floor plan using this symbol.

Table 2
Floor plan markings (cont'd.)

Marking	Description
xCn	Label each cell center using this format. Where x is the floor, and n is the next sequential cell center.
Wide, colored lines.	Mark cell boundaries on the floor plan using wide, colored lines.

For example, label a cell center on the second floor as 2C3. The 2 before the C indicates that the cell center is on the second floor. The 3 after the C indicates that this cell is the third cell in sequence in the site planning process.

Table 3
Example cell labels

Floor	Cell label
First floor	2C1, 2C2, 2C3
Ground floor	1C1, 1C2, 1C3
Basement level one	-1C1, -1C2, -1C3
Basement level two	-2C1, -2C2, -2C3

Figure 13
Example cell boundaries

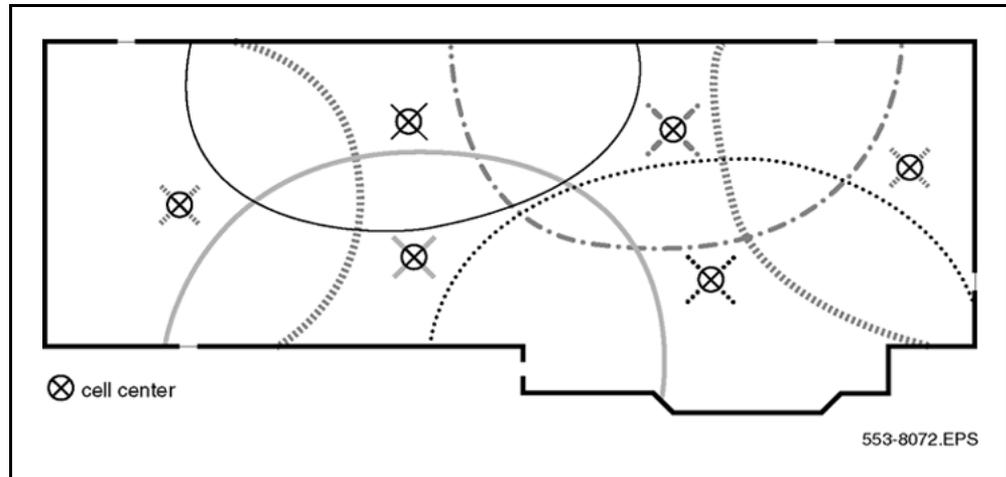


Figure 14
Points, centers, and boundaries on the floor plan

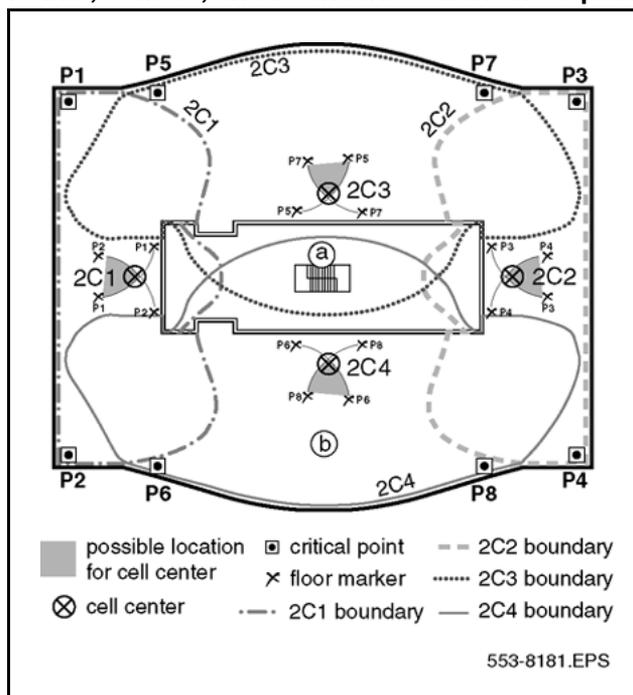


Figure 14 "Points, centers, and boundaries on the floor plan" (page 42) shows a typical floor plan marked-up after determining subsequent cell boundaries. The completed floor plan is as follows.

- Initial critical points are shown at P1, P2, P3, and P4.
- Cell centers are located where arcs from P1/P2, P3/P4 intersect.
- 2C1 and 2C2 show cell centers or basestation locations.
- Dashed and dotted lines show cell boundaries.
- Additional critical points are shown at P5, P6, P7, and P8.
- 2C3 and 2C4 cell centers provide full coverage of the floor.

Two copies of the floor plan are required. One copy is used during the site planning. The second copy is marked with the information from the site planning copy and attached to the provisioning records for the installer.

Deployment illustrations

The illustrations in this section represent the deployment process from start to finish.

Figure 15
Example of initial critical points

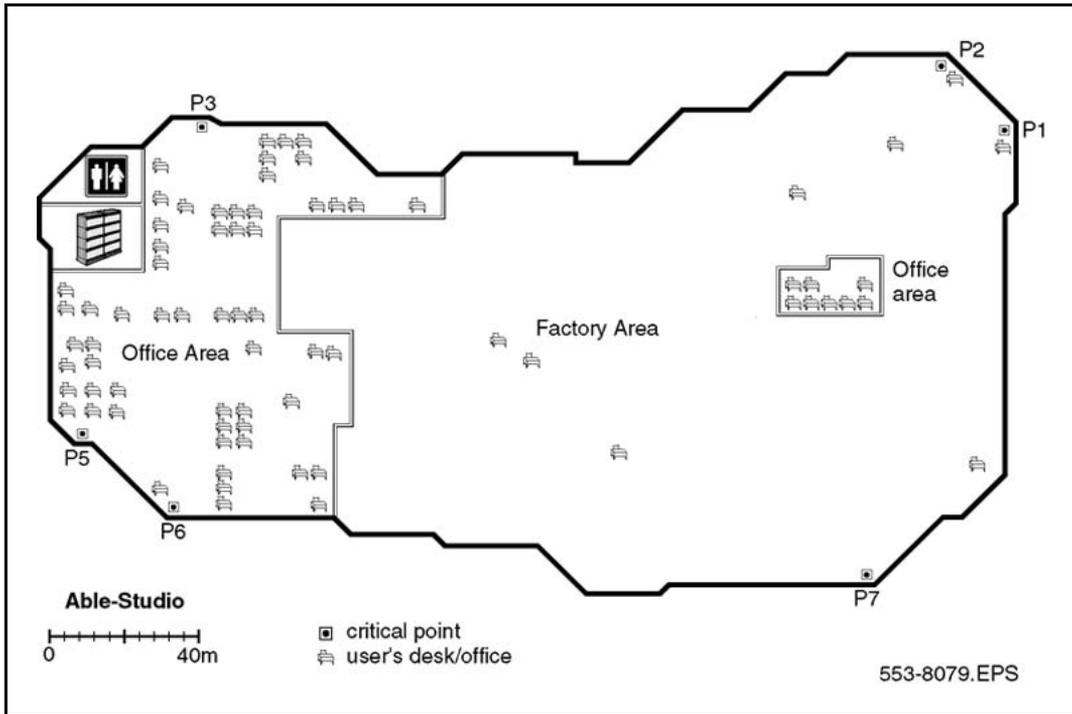


Figure 16
Cell contour of the initial critical point

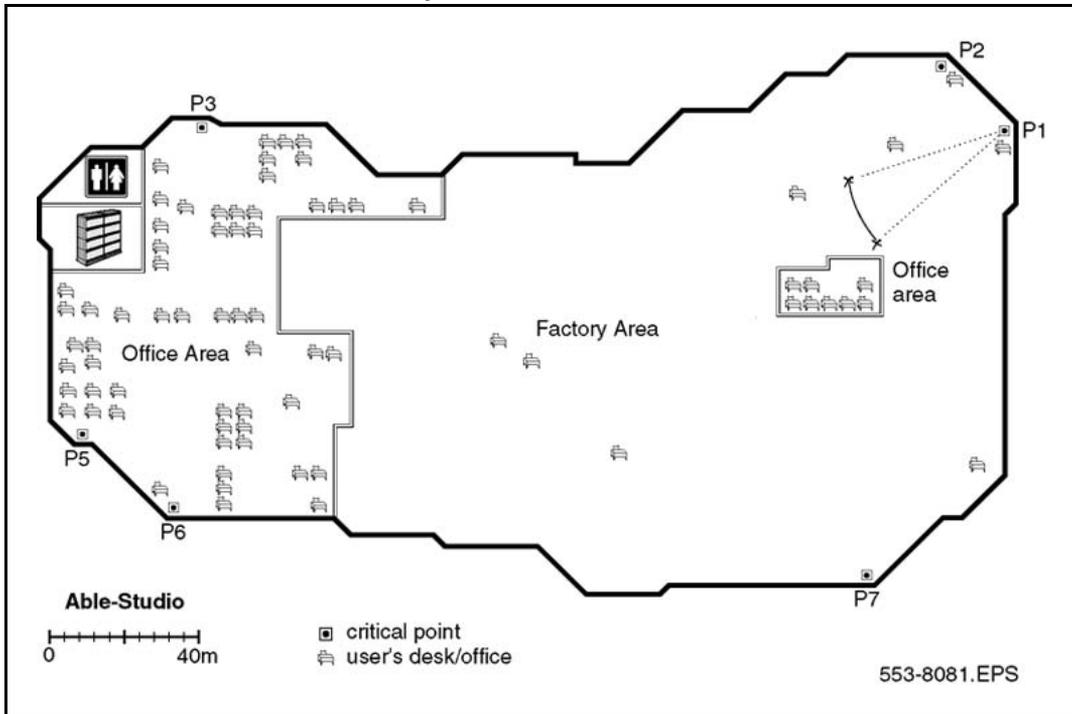


Figure 17
Cell contour of the closest adjacent critical point to the initial critical point

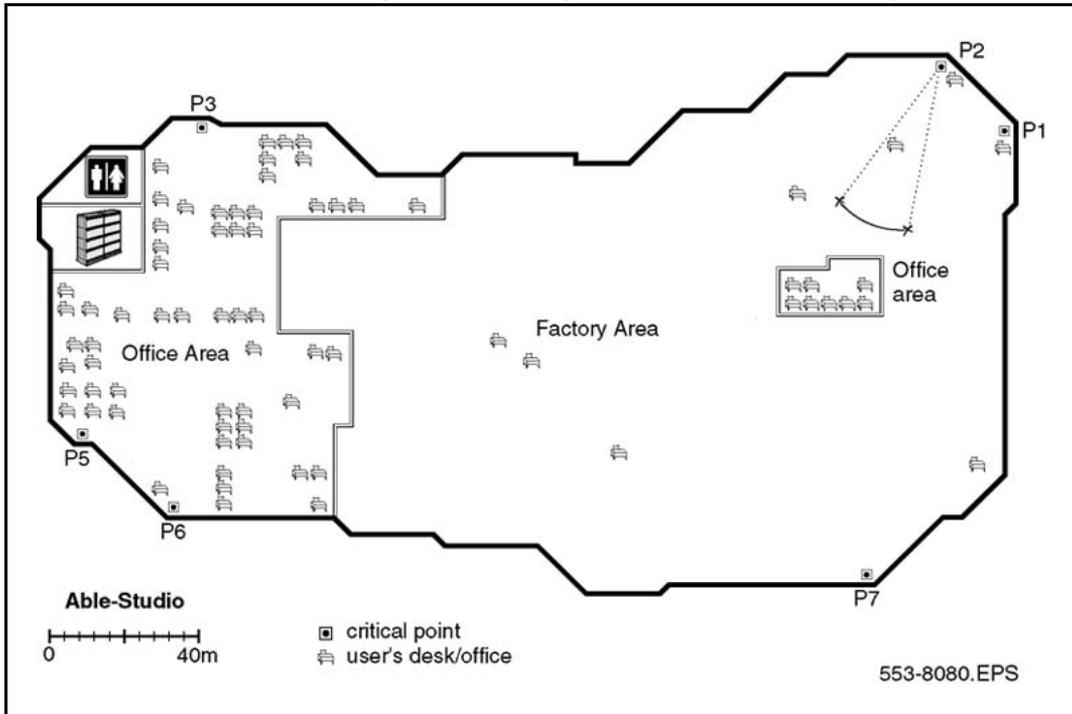


Figure 18
Example of a cell center

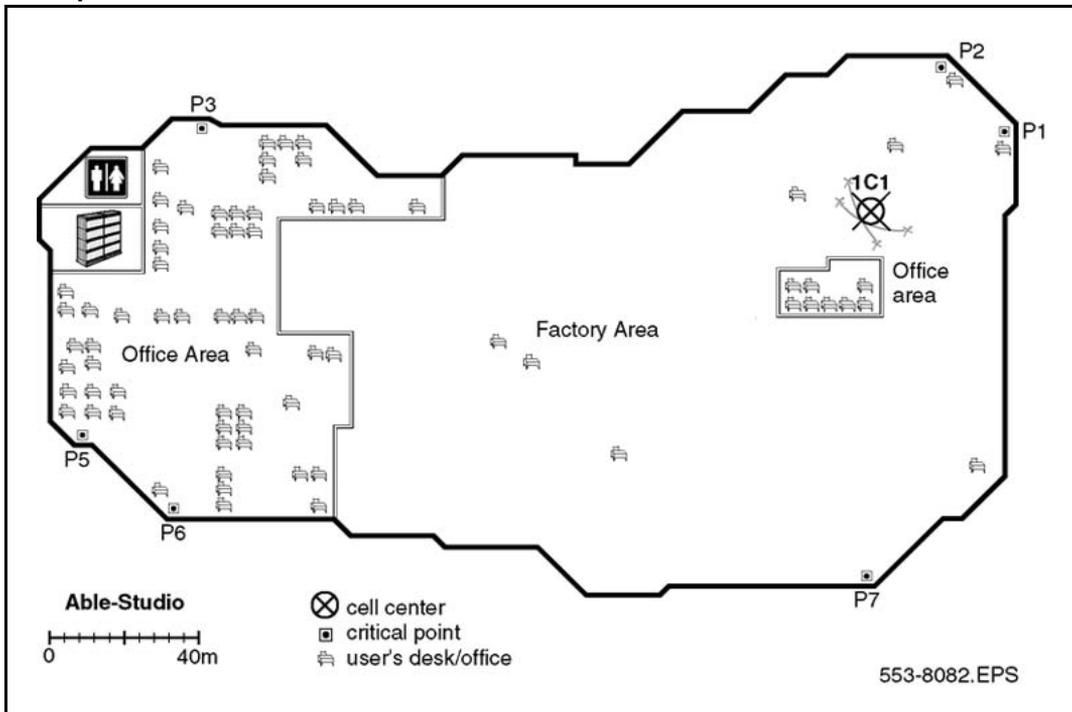


Figure 19
Example of a cell center boundary

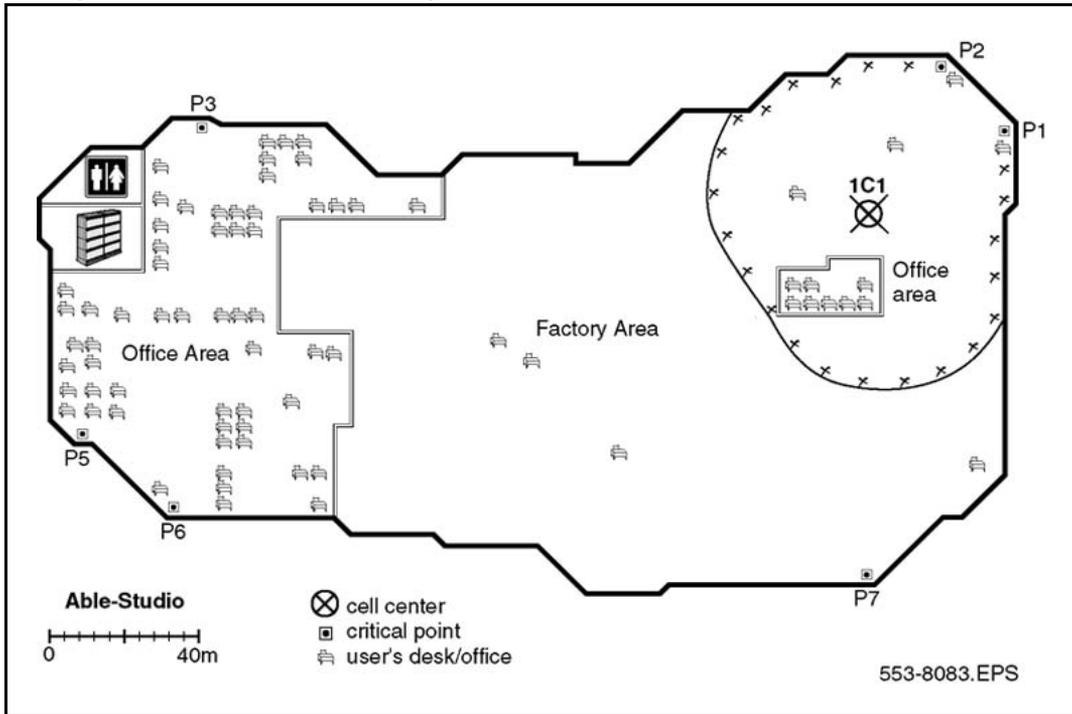


Figure 20
Example of new critical points (P8 and P9)

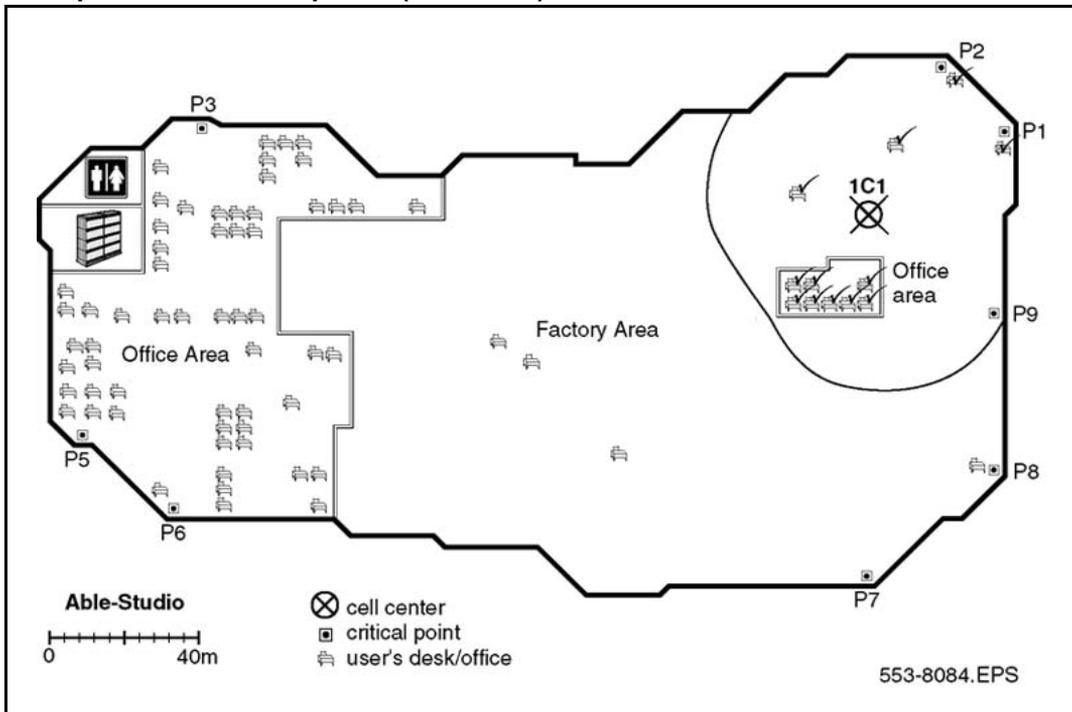


Figure 21
Example of deployment for cell center 1C2

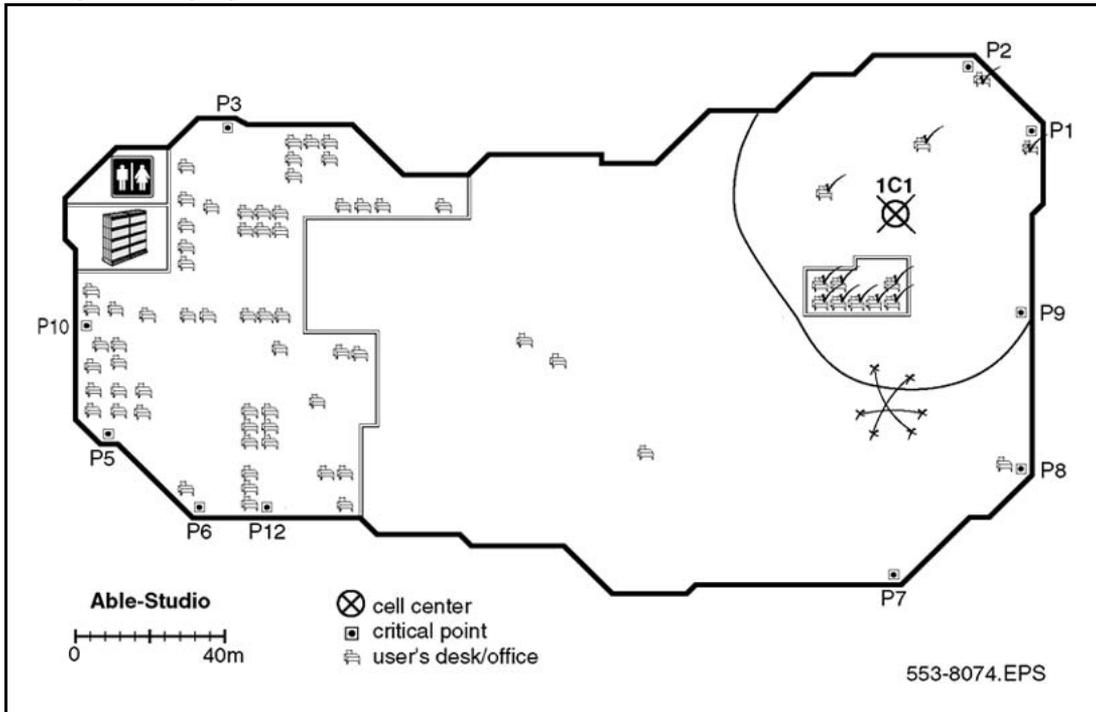


Figure 22
Example of deployment for cells 1C3 and 1C4

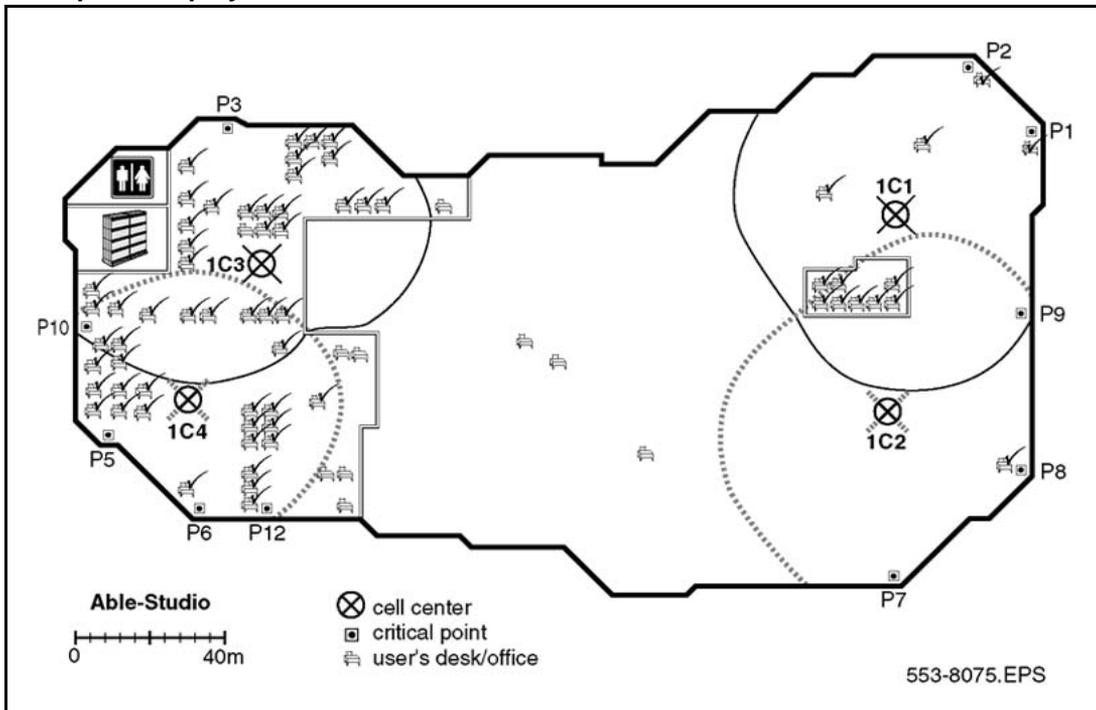


Figure 23
Identify new critical points (P11, P12, P13, P14, P15, P16, P17)

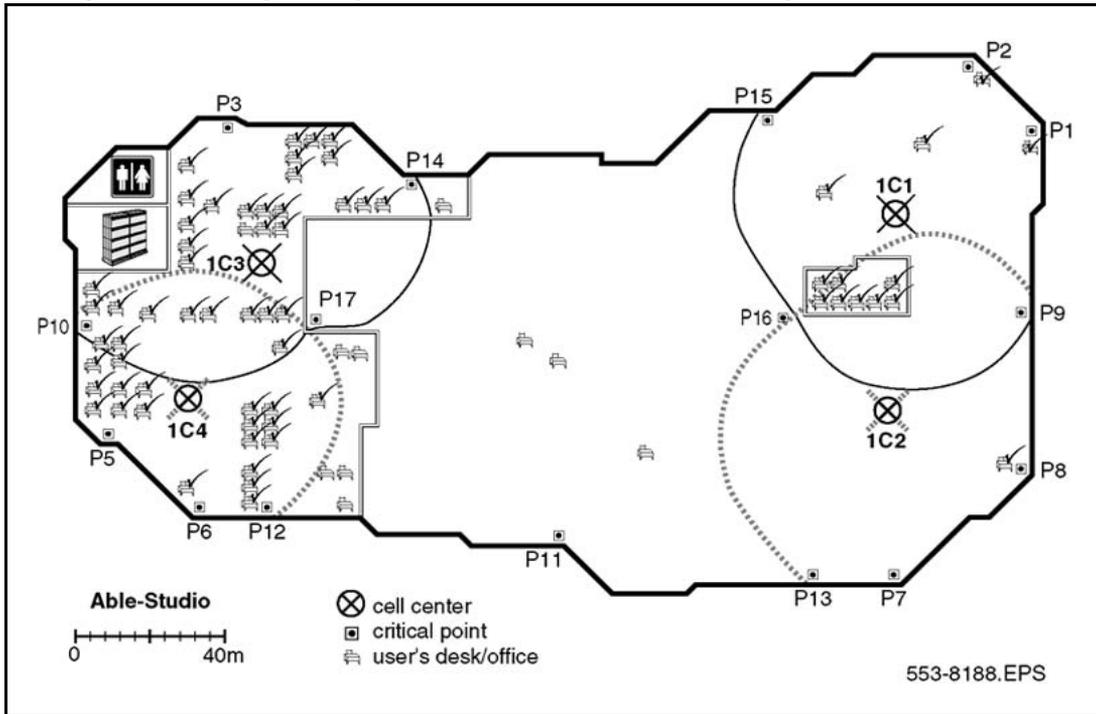


Figure 24
Contours formed by critical points P11, P13, and P16

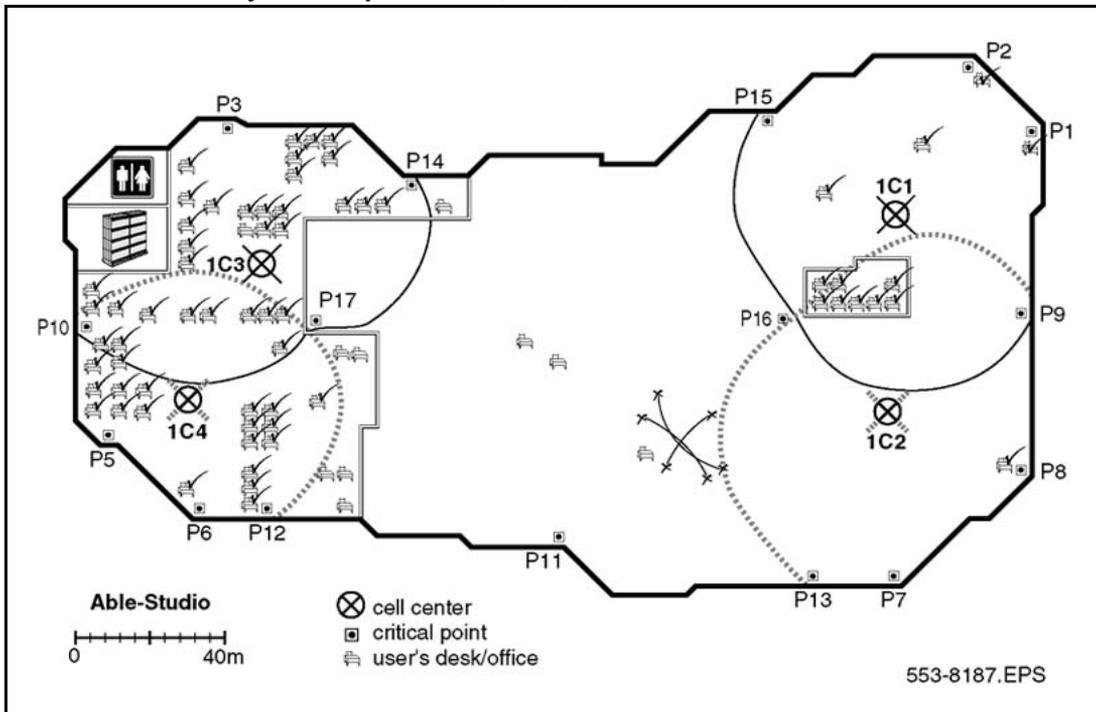


Figure 25
Cell center 1C5 formed by critical points P11, P13, and P16

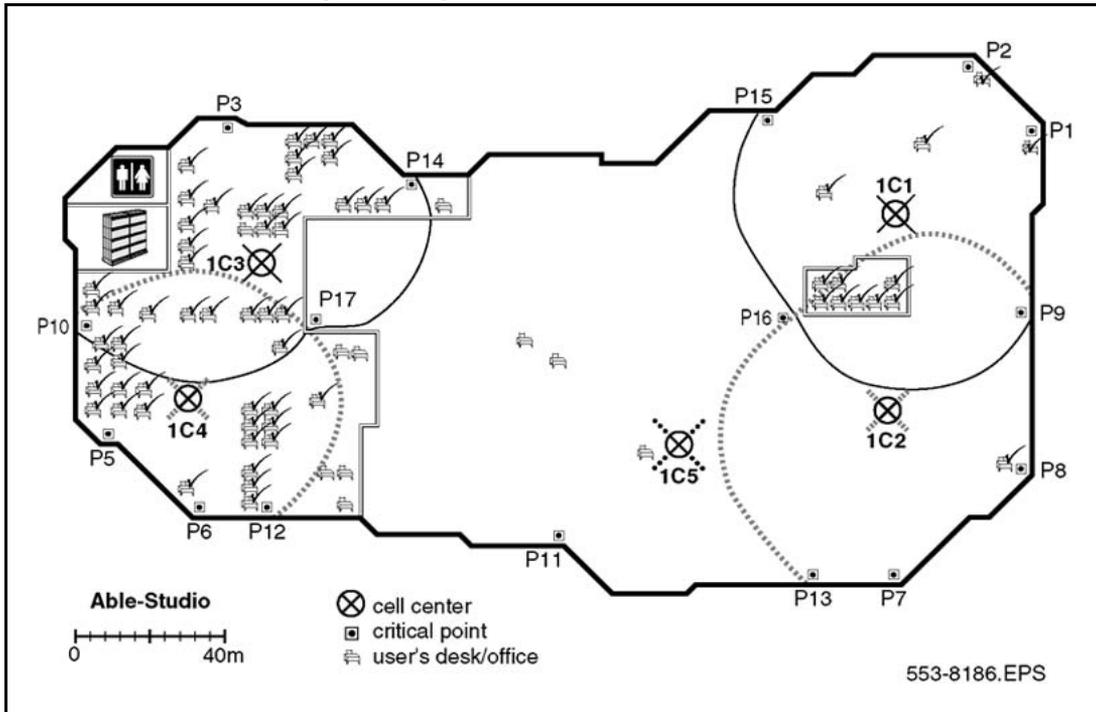


Figure 26
Cell boundary 1C5 formed by critical points P11, P13, and P16

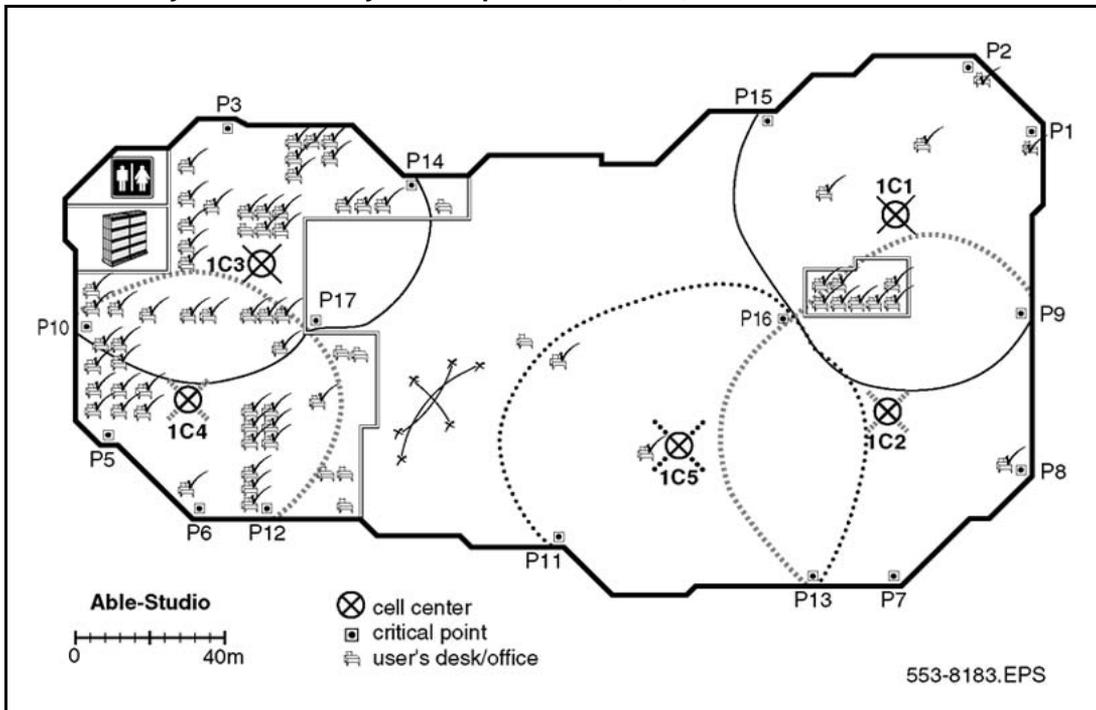


Figure 27
Example of critical point cell boundaries

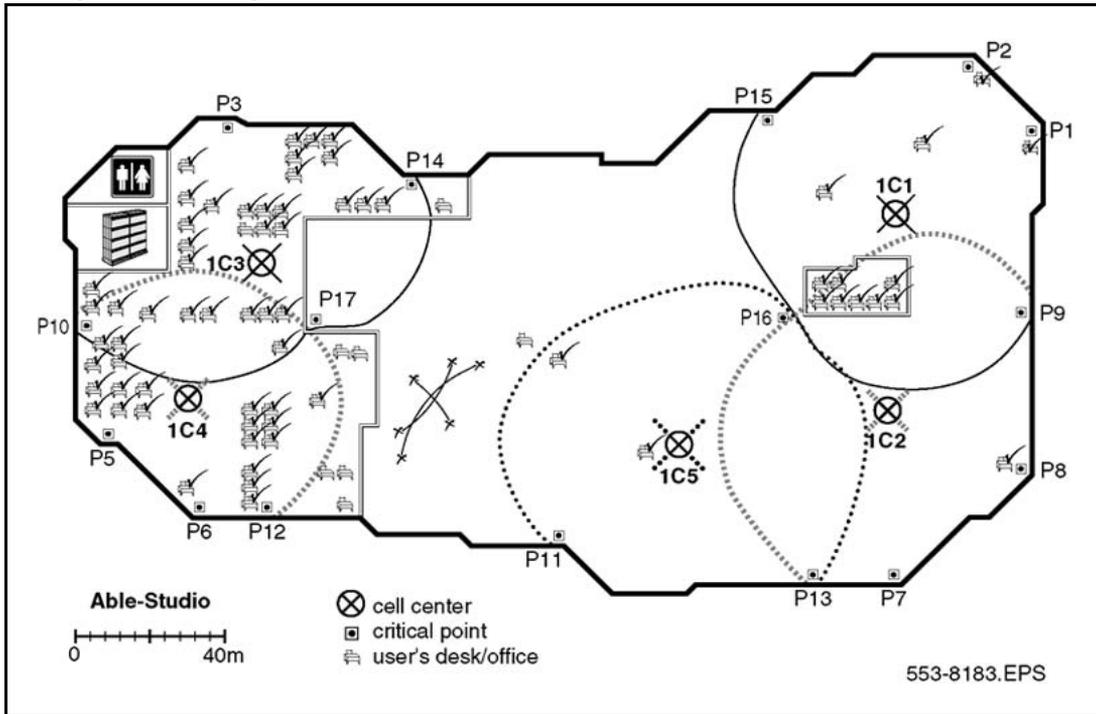


Figure 28
Example of cell center boundary 1C6

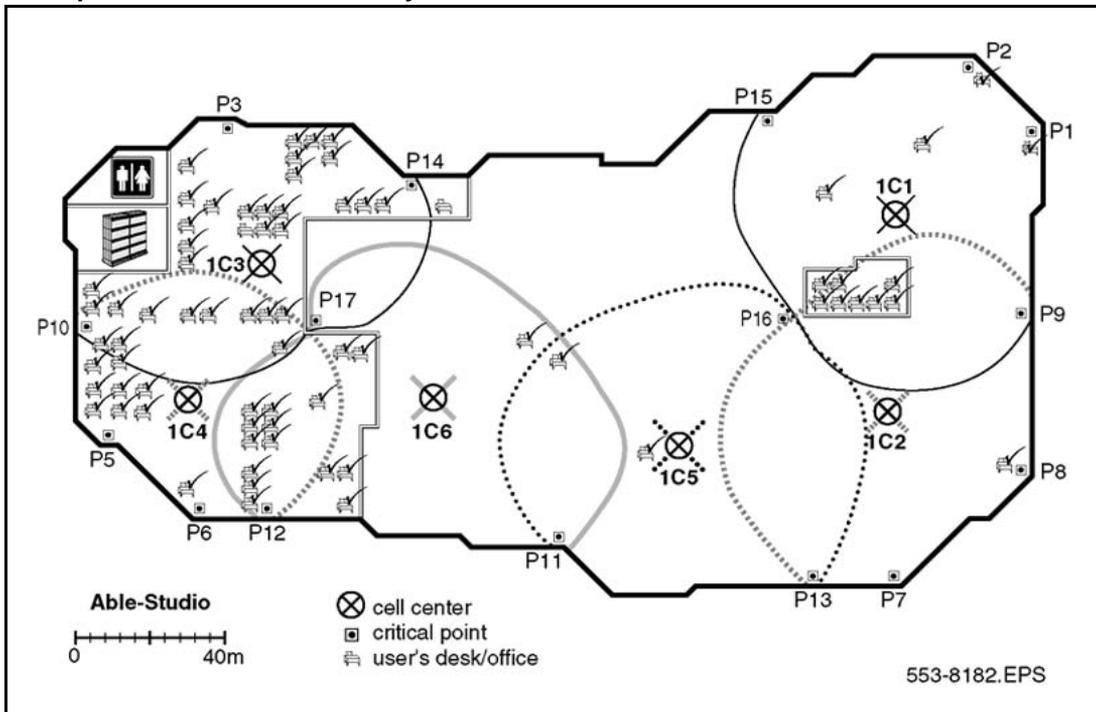
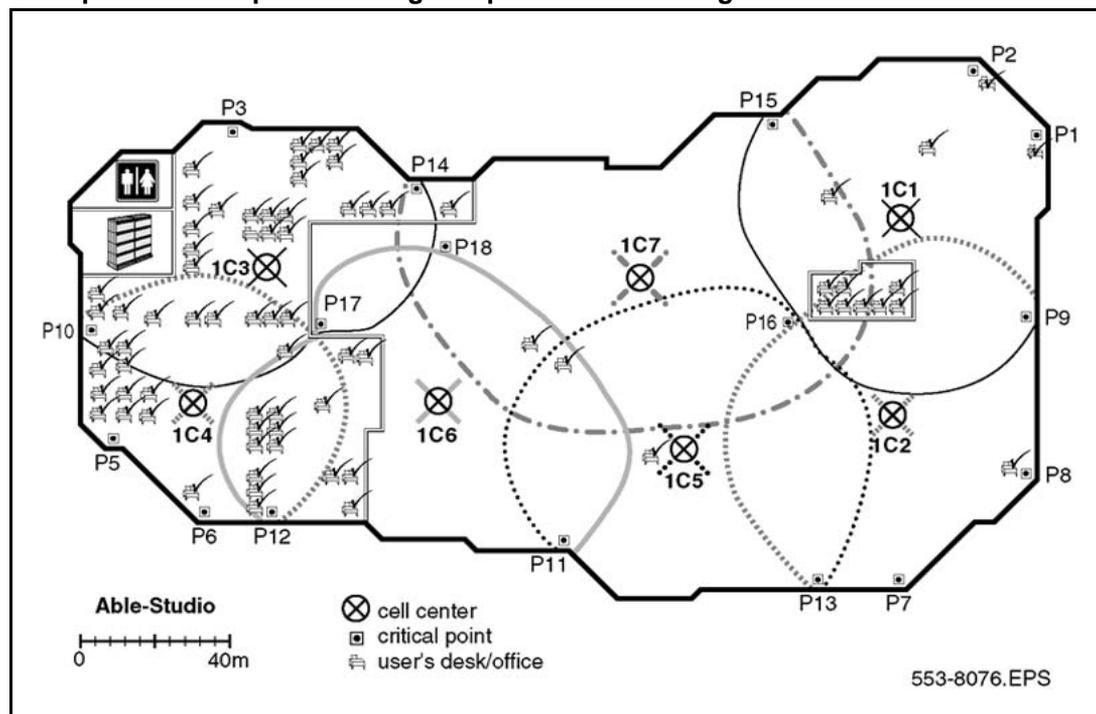


Figure 29
Example of a floor plan showing complete radio coverage



Deployment terms

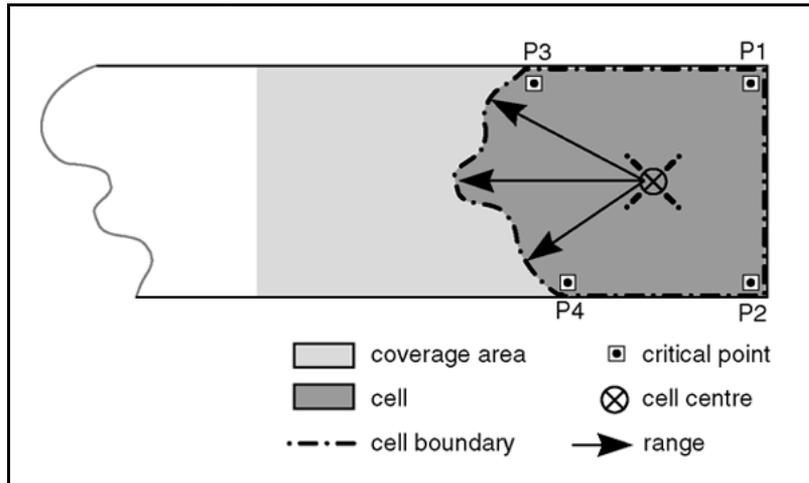
Terms associated with deployment are listed in the following table.

Table 4
Deployment terms

Term	Definition
Coverage area	An area where a handset can be used to make and receive calls.
Cell	The coverage area provided by the basestation antennas.
Cell boundary	The parameter of a cell coverage area.
Critical point	A point or location defined as the extreme corner of a coverage area that can be difficult for the radio signal to reach.
Cell center	The installation point of the basestation serving the cell.
Range	The distance from a cell center to its cell boundary.
Traffic table	Traffic tables record site traffic information from the floor plan and the customer. The traffic table helps to determine the required number of basestations for each cell.

The following figure illustrates these terms.

Figure 30
Example showing deployment terms



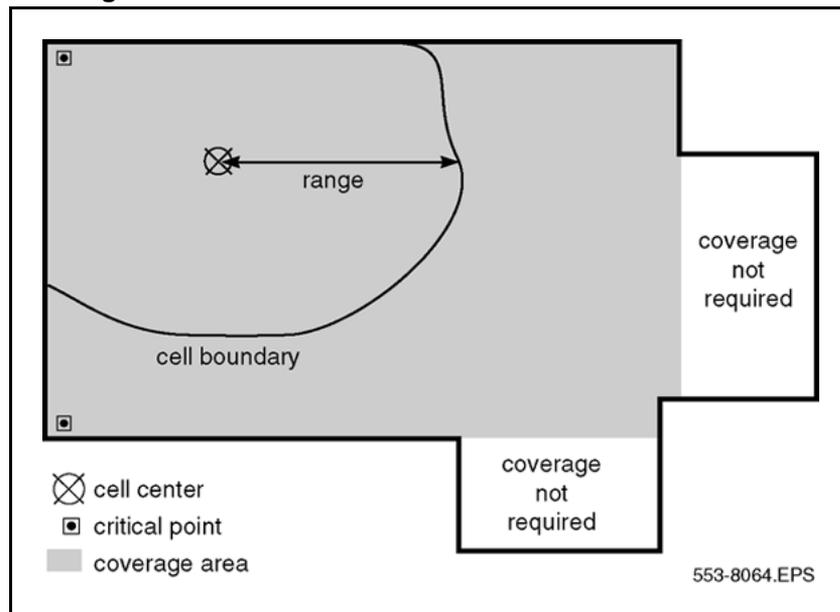
Coverage terms

The terms used in this guide are described in [Table 5 "Coverage terms" \(page 51\)](#) and illustrated in [Figure 31 "Coverage terms" \(page 52\)](#).

Table 5
Coverage terms

Term	Definition
Estimated number of handsets	The average number of handsets expected in a particular cell.
Cell	The coverage area provided by a basestation.
Cell boundary	The edge of a cell showing the cell coverage area.
Cell center	The place where all the basestations are installed.
DECT Radio Deployment Tool	The tool used to determine the radio range of a basestation.
Critical point	A point or location defined as an outer corner of a coverage area, or points that can be difficult for the radio signal to reach.
Coverage area	The area defined by the customer in which a handset user can expect to be able to make and receive calls.
Link	If a handset and a basestation are in radio communication with each other.
Range	The distance from a cell center to the cell boundary.
Office	The location where a handset user spends the majority of their day.
Traffic table	Traffic tables record site traffic information from the floor plan and the customer. The traffic table helps to determine the required number of basestations for each cell.

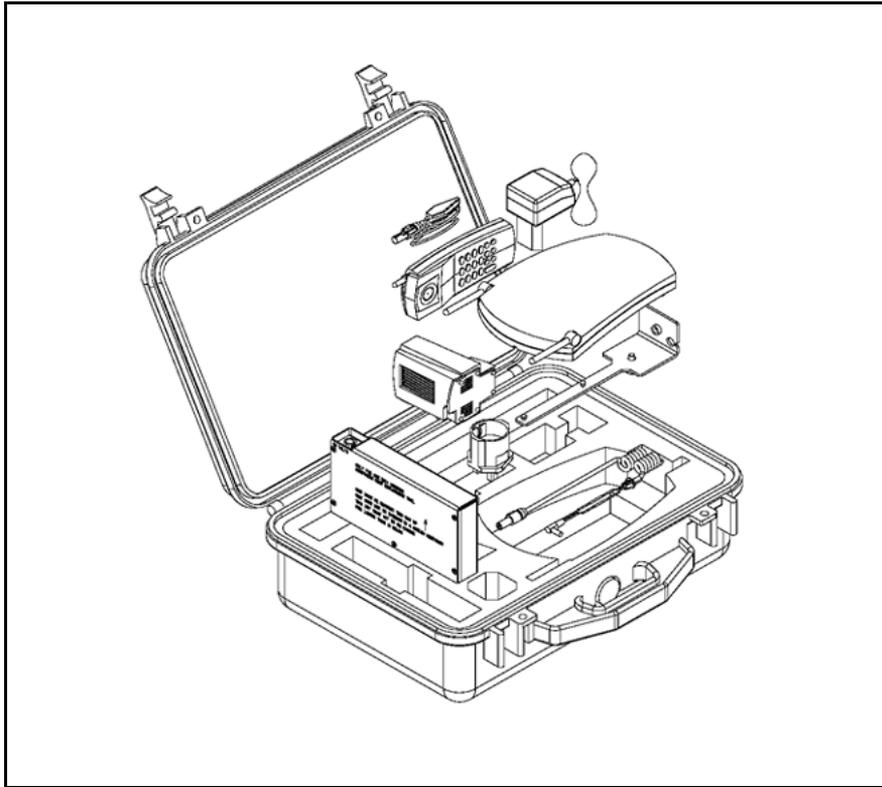
Figure 31
Coverage terms



Deployment tool

The DECT Deployment Tool (deployment tool) determines cell centers and cell boundaries. See [Figure 40 "Deployment Kit 2 and carrying case" \(page 64\)](#) and [Figure 41 "Assembled Deployment Kit 2 and DeTeWe handsets" \(page 66\)](#).

Figure 32
Deployment tool carrying case and packing details



Charging the deployment tool battery

Charge the deployment tool battery for at least six hours before using.



CAUTION Equipment Damage

Use the Nortel battery charger. This charger is a separately ordered item. Failure to use an automatic shutoff battery charger can damage the battery.

Do not use the battery supplied with the CT2 deployment tool. The CT2 and DECT batteries are not interchangeable.

Figure 34
Deployment tool battery charger

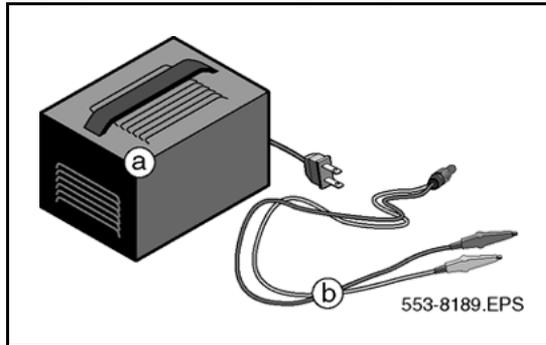


Table 6
Deployment tool battery charger key

a	battery charger (must be ordered separately)
b	battery charger cable

Procedure 7

Charging the deployment tool battery

Step	Action
1	Set up the deployment tool battery charging equipment. Remove the deployment tool battery, charger, and charger cord from the yellow case.
2	Charge the deployment tool battery. Connect the charger cord plug into the battery. Connect the red alligator clip to the positive lead of the charger, and the black clip to the negative lead of the charger. Connect the battery charger to the AC mains.
3	Remove the deployment tool battery from the charger after it is charged.

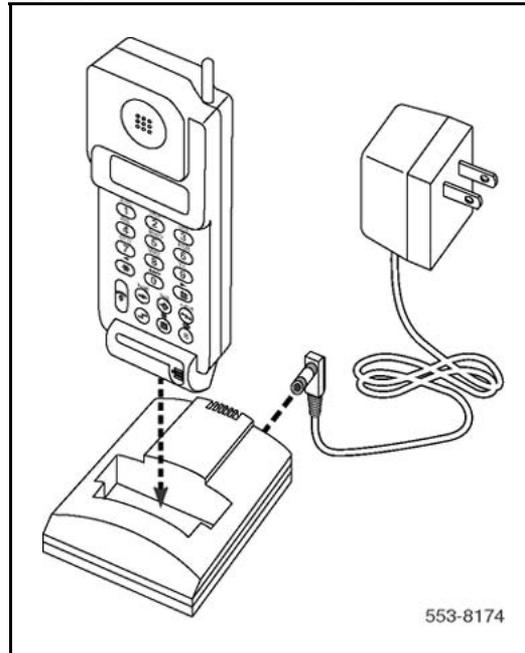
The battery must charge for at least six hours.

--End--

Charging the deployment handset battery

Figure 35

Deployment handset battery charger



Charging time Charge the deployment handset battery for at least 12 hours before using the first time. Charge the handset at least six hours before subsequent use.

Procedure 8

Charging the deployment handset battery

Step	Action
1	Set up the deployment handset battery charging equipment. Remove the deployment handset battery, charger and charger cord from the yellow case.
2	Charge the deployment tool battery. Connect the charger cord to the charging stand. Connect the charger cord to the AC mains. Place the handset into the charging stand. The red LED flashes while the handset is charging.

- 3 Remove the handset from the charger after it is ready for use.

--End--

Assembling the deployment tool

Figure 36

Deployment tool extension details

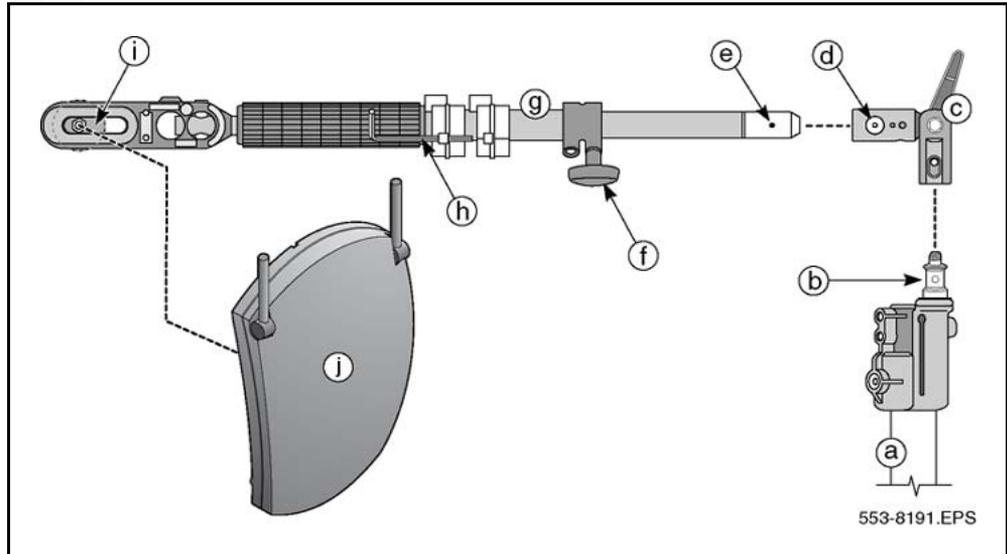


Table 7

Key for Assembling the deployment tool

a	adjustable tripod
b	extender arm connector
c	extender arm swivel
d	detente stop
e	detente
f	extension thumb screw
g	telescopic extension
h	Allen key
i	basestation attaching thumb screw
j	basestation

Note: The deployment tool battery and the deployment handset battery must be charged for at least six hours before use.

Figure 37
Deployment tool battery details

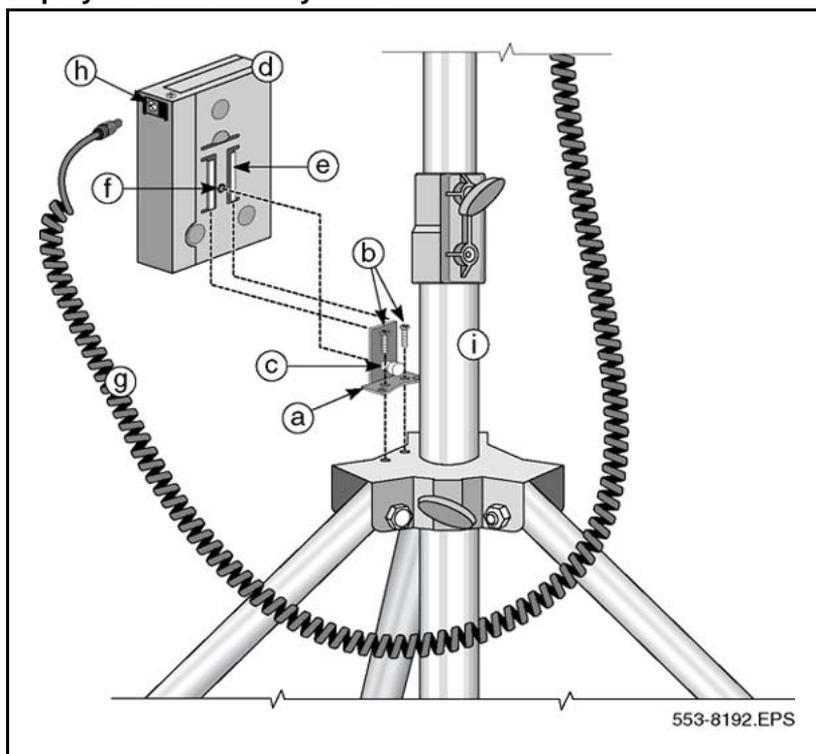


Table 8
Deployment tool battery details key

a	battery mount
b	Allen screws
c	thumb screw
d	battery pack
e	guides
f	thumb screw nut
g	power cord
h	power cord receptacle
i	tripod

Procedure 9
Assembling the deployment tool

Step	Action
1	Set up the tripod. Remove the tripod from its carrying case and set upright. Lock the casters.

- 2** If required, install the extension arm fitting on the tripod. If not required, go to step 4.

Place the extension arm fitting, shown in [Figure 40 "Deployment Kit 2 and carrying case" \(page 64\)](#), onto the brass fitting on the top of the tripod.
- 3** If required, secure the extension arm fitting.

Use the Allen key attached to the extender arm to secure the extension arm fitting Allen screw.
- 4** Mount the extension arm on the tripod.

Place the brass end of the extension arm into the fitting, so that the keying hole of the extension arm mates with the retaining thumb screw locking device of the tripod fitting. The thumb screw locking device clicks into the keying hole of the extension arm.
- 5** Position the extension arm.

Orient the arm into the proper position. Secure the tripod fitting and the extension arm thumb screw.
- 6** Affix the basestation to the extension arm.

Remove the basestation from the yellow case. Mount the basestation onto the end of the arm. Screw the brass thumb screw on the arm into the bottom of the basestation and secure it in place with the grey lock thumb screw.
- 7** Position the antenna.

Rotate the antenna from its stowed position, against the body of the basestation, to its upright operating position.
- 8** Position the basestation. The normal position is with the antenna pointing upwards.

Secure the basestation with the arm thumb screw.
- 9** Mount the battery fixture on the tripod.

Remove the battery bracket, shown in [Figure 37 "Deployment tool battery details" \(page 58\)](#), from the yellow case. Screw the battery bracket onto the tripod caster brace, with the two machine screws.
- 10** Mount the battery.

Pull the release pin on the bracket back and slide the battery grooves on to the bracket. Ensure the bracket pin locks into the battery.
- 11** Connect the basestation to the battery.

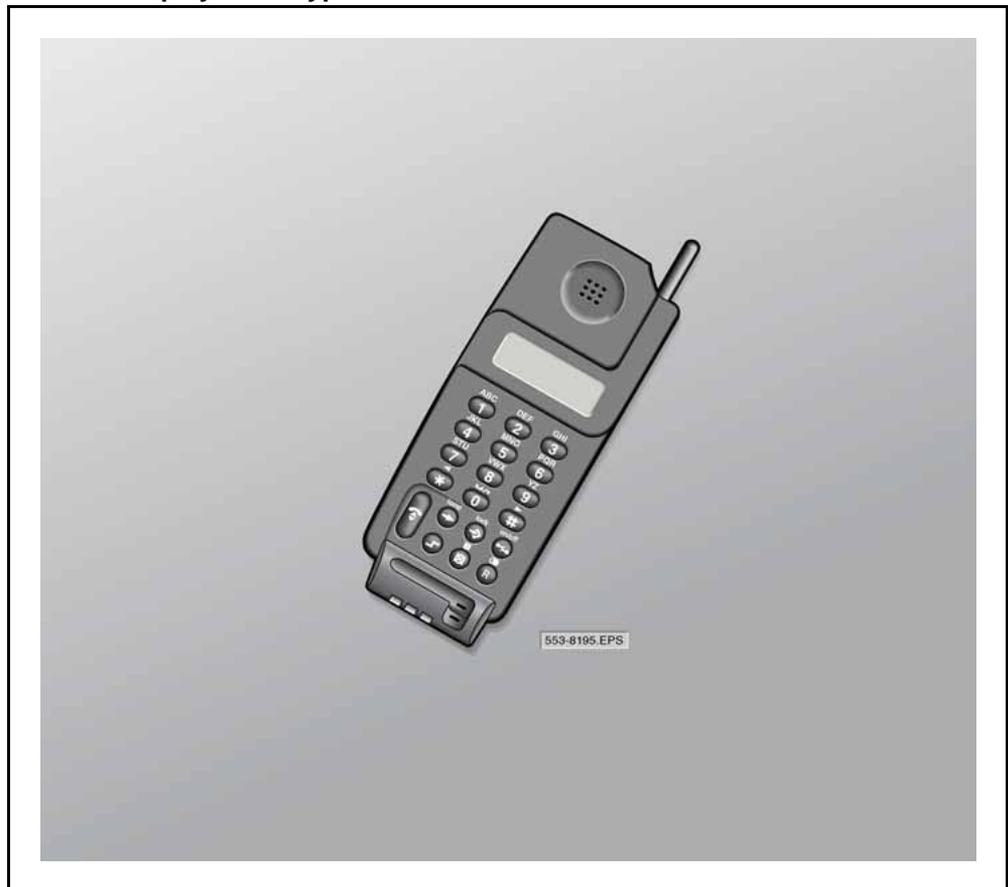
Plug the basestation power cord connector into the upper right edge of the battery.

--End--

Testing the deployment handset

Figure 38

Handset display and keypad details



Procedure 10

Testing the deployment tool handset

Step	Action
1	Start the test and establish a link with the basestation. Remove the handset from its charger.
2	Turn on the handset. Press the shift key and press the ON/OFF button. DECT HANDSET appears on the handset display.



- 3 Select system mode.
Press the **shift** key and press the **local** key. The handset displays **SYSTEM**.
- 4 Select the monitor mode.
Press the **star (*)** key. The handset displays **MONITOR MODE**.
- 5 Select the monitor mode code.
Press the **lock** button. The handset displays **CODE**.
- 6 Enter the monitor mode code.
On the dial pad, enter **2530**. Press the **lock** button.
- 7 Interpret the handset RSSI display and test tone.
Follow the explanation in [“How the deployment tool works”](#) (page 61) and [“Using the deployment tool”](#) (page 62).

--End--

How the deployment tool works

The deployment tool basestation and the deployment handset establishes a radio link under the following circumstances.

- the handset is in the deployment mode
- the handset and basestation are within range of one another

The closer the handset is to the basestation the stronger the link. As the handset moves away from the basestation, a point is reached where the signal is no longer reliable for telephone conversations.

After a link is established, the handset emits a continuous 1.4kHz tone and displays a Radio Signal Strength Indication (RSSI).

Figure 39
Deployment handset link display



The display, shown in [Figure 39 "Deployment handset link display"](#) (page 61), means as follows.

- A circle and dot indicates a locked signal.
- The antenna symbol indicates a link establishment.
- The number 10 indicates an RSSI value.
- The dash, equal sign and shaded box icons indicate signal strength.

The maximum RSSI is 10. As signal strength diminishes, the number 10 decreases and the icons disappear. For example, at signal strength 7, the three shaded boxes that are on the right side of the display disappear. At signal strength 5, all the shaded boxes and one of the equal sign icons disappear.

The signal strength diminishes as the distance between the handset and the basestation increases. The tone remains unchanged until the handset is out of range of the basestation.

Using the deployment tool

The deployment tool is assembled as shown in [Figure 33 "Assembled deployment tool"](#) (page 54), with the extension arm parallel to the floor. Position the basestation antenna upwards. Place the basestation as close to the wall as possible and at the height recommended for basestations.

To test the deployment tool, stand in an open area approximately three to five metres away from the deployment tool on its tripod. Establish a link between the basestation and the handset. Keep the deployment tool basestation in plain view. Ensure there are no obstructions (including people).

Walk away from the basestation and observe the deployment handset link display. As the deployment handset moves away from the basestation, the RSSI value changes. After the RSSI value changes from 7 to 6 and the last shaded block disappears, the cell boundary is reached.

After the cell boundary is reached, stop and listen to the tone. Ensure the tone is clear with no tone changes, tone breakup, modulation, mutes or clicks.

Do not select a cell edge that has an RSSI reading of less than 6. However, keep the following in mind.

- There can be environments that cause poor tone at a RSSI meter reading of between 7 and 10. In this case, contact Nortel support team for assistance.
- The tone stops after the radio link is lost.

Handset tones interpretation

The handset tones indicate how close the handset is to the deployment tool basestation.

- Steady tone – the handset is within the cell boundary, or at the cell boundary edge.
- Tone change, tone breakup, modulation, mute or click – the handset is beyond cell boundary edge.

Rules for outdoor deployment

Procedure 11

Complying with the rules for outdoor deployment

Step	Action
1	Cover outdoor areas before covering indoor areas. Use the deployment tool to determine outdoor cell centers.
2	Use the deployment handset to determine the outdoor coverage provided by a basestation located indoors.
3	External housings for outdoor basestations must be mounted directly on walls or similar vertical surfaces.
4	If you are using the deployment tool outdoors, ensure the deployment tool does not fall over or come in contact with electrical wires and cables.
5	If an outdoor critical point cannot be reached, inform the customer.
6	Do not use the deployment tool on windy days.
7	Do not use the deployment tool in bad weather.
8	Keep all personnel away from the apparatus.
9	Follow all safety requirements.
10	Use batteries to power the deployment tool.

- 11 Charge the batteries indoors.

--End--

DECT Deployment Kit 2

The DECT Deployment Kit 2 is shown in [Figure 40 "Deployment Kit 2 and carrying case"](#) (page 64). For more information, see the DeTeWe User Manual that accompanies each kit.

Figure 40
Deployment Kit 2 and carrying case



The following information can be used in conjunction with the DeTeWe User Manual that accompanies the deployment tool.

- The two DeTeWe handsets with the kit are subscribed to the basestation and are numbered 13 and 15. To view the assembled basestation and the DeTeWe handsets, see [Figure 41 "Assembled Deployment Kit 2 and DeTeWe handsets"](#) (page 66).
- The key on the handset is the Off-Hook key.



- To enter Site Survey Mode on the handset, perform the following.

- Press Menu
- Scroll to System
- Dial ***76#
- Scroll to Site Survey
- Press OK
- The FE value for the PP is the number of detected Sync/ACRC errors within the last 100 receiving frames, for example, 1 sec. For proper deployment, the FE value must not exceed 4.
- The FE value for the FP is the number of received Q1/Q2 bit information within the last 100 receiving frames, for example 1 sec. For proper deployment, the FE value must not exceed 4.
- An RSSI value of -80dBm ... -85dBm is used to indicate the cell boundary.
- Use the following procedure to subscribe a handset that has de-subscribed in error.
 - a. Long-press the button on the basestation to open the DECT system.
 - b. On the handset, navigate to **Menu > System > Subscription > New**.
 - c. Enter the **PARK** number provided at the bottom of the basestation.
 - d. Enter the authorization code (the last 4 digits of the serial number located at the bottom of the basestation).The handset subscribes with the basestation.

Figure 41
Assembled Deployment Kit 2 and DeTeWe handsets



Figure 42
Deployment Kit 2 basestation



DAP deployment

To deploy a DECT system follow [Procedure 12 “Deploying a DECT system”](#) (page 67).

Procedure 12
Deploying a DECT system

Step	Action
1	Identify and mark initial critical points. Mark critical initial points on the floor plan with the following symbol.  Figure 15 "Example of initial critical points" (page 43) shows the initial critical points: P1, P2, P3, P5, P6 and P7.
2	Demarcate the cell contour for the critical point farthest from the center of the full coverage area. To demarcate a cell contour, perform the following.

- a Set up the deployment tool basestation. Raise the deployment tool basestation as high as possible, or until it is at the height recommended for basestations.
- b Establish a link. See [“Deployment tool” \(page 52\)](#) for details.
- c Measure the range into the coverage area in a few directions to determine where a cell center can be located and still be within range of the critical point. Listen to the deployment tool handset while moving away from the basestation. After the RSSI value changes from 7 to 6, the cell boundary is detected.
- d Mark the cell boundary on the floor plan with a small x.
- e Repeat step c and step d until there are enough Xs to draw a thin contour arc through the Xs.

In [Figure 16 "Cell contour of the initial critical point" \(page 43\)](#), P1 is the initial critical point.

- 3 Demarcate the cell contour of the closest adjacent critical point to the first critical point.

See [step 2](#) for details. In [Figure 17 "Cell contour of the closest adjacent critical point to the initial critical point" \(page 44\)](#), P2 is the closest adjacent critical point to the first critical point.

- 4 Use the cell contours to locate a cell center.

Locate the cell center where the cell contours meet. Choose a position on the floor plan that meets the following requirements.

- is furthest from the critical points,
- still provides good audio quality at the critical point,
- complies with the [“Rules and guidelines to locate cell centers” \(page 35\)](#), and
- is in the coverage area.

With a pencil, label the cell center on the floor plan with the following symbol. **xCn**, where **x** = the floor and **n** = is the cell number in sequence of the entire plan.



In [Figure 18 "Example of a cell center" \(page 44\)](#), IC1 is a cell center.

- 5 Demarcate a cell boundary.

To demarcate a cell boundary, perform the following steps.

- a Set up the deployment tool basestation at the cell center.
- b Establish a link.

- c See the floor plan and check audio quality in user offices within the cell. If a user office is in a zone where audio quality deteriorates, relocate the cell center closer to the critical point or the office.
- d Walk into all of the areas (rooms) necessary to demarcate the complete cell boundary. Radio signals travel further in uncluttered areas than in cluttered areas. Record the cell boundary.
- e Find the cell boundary by measuring the range and marking it on the floor plan with a small x. Repeat steps [step c](#) and [step d](#) until there are enough Xs so that a contour arc can be drawn around the cell center.

See [Figure 19 "Example of a cell center boundary"](#) (page 45) for an example of a cell boundary.

6 Mark and label the cell boundary on the floor plan

Follow these steps.

- a Mark each office within the cell that is isolated from the office area.
- b Label subsequent critical points on the floor plan with the following symbol.



- c Mark the cell contour on the floor plan. Trace a contour line through the Xs with a marker.
- d Trace the cell boundaries and cell centers with colored markers.

7 Identify new critical points.

Follow these steps.

- a Identify one new critical point slightly inside of where the cell boundary meets the outside wall. In [Figure 20 "Example of new critical points \(P8 and P9\)"](#) (page 45), this new critical point is P9.
- b Identify another new critical point which is adjacent to the first new critical point. Locate this critical point on the opposite side of the cell boundary area. In [Figure 20 "Example of new critical points \(P8 and P9\)"](#) (page 45), the cell boundary area is IC1 and the new critical point is P8.

8 Mark and label these new critical points on the floor plan with the following symbol.



See [step 6](#) for details.

- 9 Using the critical points from [step 7](#), demarcate new cell contours, a new cell center and a new cell boundary.

See [step 2](#) to [step 5](#) starting on [step 2](#) for details.

Note: Cell contour arcs must pass near the cell boundary of adjacent cells. For an example of this, see [Figure 21 "Example of deployment for cell center 1C2"](#) (page 46).

- 10 Demarcate additional cell contours, centers and boundaries at the other end of the building.

Repeat [step 1](#) to [step 8](#) as necessary to demarcate new cell boundaries at the other end of the building. In [Figure 22 "Example of deployment for cells 1C3 and 1C4"](#) (page 46), new cells are formed around cell centers IC3 and IC4.

- 11 Identify new critical points.

These critical points must be as follows.

- adjacent to a critical point and on the opposite side of the cell boundary area. (critical point = P11 in [Figure 23 "Identify new critical points \(P11, P12, P13, P14, P15, P16, P17\)"](#) (page 47), where cell boundary area = IC2),
- just inside of where the cell boundary meets the outside wall (P12, P13, P14, and P15 in [Figure 23 "Identify new critical points \(P11, P12, P13, P14, P15, P16, P17\)"](#) (page 47), and
- where cell boundaries meet (P16 and P17 in [Figure 23 "Identify new critical points \(P11, P12, P13, P14, P15, P16, P17\)"](#) (page 47).

- 12 Demarcate additional cell boundaries to cover all areas of the building.

Repeat [step 1](#) to [step 8](#) as necessary to demarcate new cell boundaries in the middle of the building.

For more information, see [Figure 24 "Contours formed by critical points P11, P13, and P16"](#) (page 47), [Figure 25 "Cell center 1C5 formed by critical points P11, P13, and P16"](#) (page 48), and [Figure 26 "Cell boundary 1C5 formed by critical points P11, P13,](#)

and P16" (page 48). Critical points P11, P13 and P16 form the following.

- contours in Figure 24 "Contours formed by critical points P11, P13, and P16" (page 47)
- the cell center 1C5 in Figure 25 "Cell center 1C5 formed by critical points P11, P13, and P16" (page 48)
- a new cell boundary in Figure 26 "Cell boundary 1C5 formed by critical points P11, P13, and P16" (page 48)

For more information, see Figure 27 "Example of critical point cell boundaries" (page 49) and Figure 28 "Example of cell center boundary 1C6" (page 49).

Critical points P11, P12, and P17 form the following.

- contours in Figure 27 "Example of critical point cell boundaries" (page 49)
- a new boundary based on cell center 1C6 in Figure 28 "Example of cell center boundary 1C6" (page 49)

Figure 24 "Contours formed by critical points P11, P13, and P16" (page 47) shows a floor plan with complete radio coverage. The floor plan is made complete by cell boundary 1C7.

--End--

Correct audio quality problems

If a user office is near the critical point and the audio quality deteriorates within the user office, the deployment tool and the cell center are not properly located.

Procedure 13 Correcting problems with audio quality

Step	Action
1	Move the cell center closer to the office or work area in question.
2	Repeat the coverage test in that area and ensure that coverage is sufficient. This can impact the coverage at other points, and you must ensure that all critical points are still properly covered by the new location.
3	Go into every location where users make and receive calls.

This includes washrooms, coffee areas, and meeting rooms. Do not speculate where users can make calls.

--End--

Single and multiple floor deployment

Whether the deployment situation involves a single floor or multiple floors, the deployment process uses basic rules.

- Deploy the external or outdoor areas first.
- Deploy from one side of the coverage area and then deploy the opposite side of the coverage area.
- Finish by deploying the middle of the coverage area.

Follow the preceding rules to prevent cell centers from clustering at one end of the site.

Consult the floor plan to be sure that there are no areas where a handset in the required coverage area can be outside the range of a cell center.

Defining a cell typically takes 25 to 40 minutes.

Single floor deployment

Deploying a single floor coverage area involves methods that apply to all other applications of coverage. For more information about multi-floor deployment, see [“Multiple floor deployment” \(page 78\)](#).

Use one or all of the following methods of deploying cells.

- [“Single-cell deployment” \(page 73\)](#) – covers the distance between two outside corners at the end of a coverage area with one cell.
- [“Double cell deployment” \(page 75\)](#) – covers the distance between two outside corners at the end of a coverage area with two cells.
- [“Multi cell deployment” \(page 76\)](#) – covers the distance between two outside corners at the end of a coverage area with more than two cells.

Always begin with the single cell method, because the range is not always known; therefore, it is not known how many cells are needed to cover the area between the critical points.

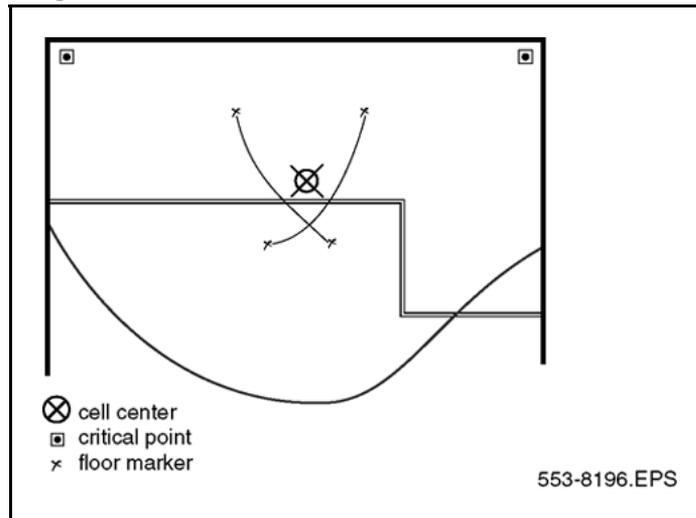
Start at the short side of the coverage area. First cover the corners, then the side between those corners, and finally inward to the center of the coverage area. Repeat the process for the other end of the coverage area.

By deploying the site using this method, cell centers are distributed throughout the site. If the site is deployed from one end to the other, cell centers can be clustered at one end of the site.

Single-cell deployment

Always start with the single-cell technique regardless of the width between the two critical points. Using this technique, you can find one cell center that serves two critical points, as shown in [Figure 43 "Single cell distance"](#) (page 73).

Figure 43
Single cell distance



Procedure 14

Single cell deployment

Step	Action
1	Identify the initial critical points. Mark them on the floor plan with a . Use different color pencils for each critical point. ■
2	Choose the first critical point at the edge of the coverage area furthest away from the center of the coverage area. Place the deployment tool at this critical point.
3	Establish a link. For more information, see "Deployment tool" (page 52).
4	Measure the range into the coverage area in a few directions to determine where a cell center can be located, and still remain within range of the critical point. Observe the deployment tool handset RSSI value while moving away from the basestation.

- After the display value changes from 7 to 6, the cell boundary is detected.
- 5 Record the cell boundary by marking a small X on the floor plan where the cell boundary value was reached. Use a pencil that is the same color as the critical point where the deployment tool is located.
 - 6 Repeat step 4 and 5 several times, walking in different directions to determine where the cell center can be located and still remain within range of the critical point.
 - 7 Draw a thin contour line through the Xs to mark an arc on the floor plan.
 - 8 Choose the other critical point adjacent to the first critical point and repeat steps 3 to 7.
 - 9 If the contour lines do not cross, or cross close to the edge of the coverage area between the two critical points, see [“Double cell deployment” \(page 75\)](#). Choose a position on the floor plan for the cell center that meets the following requirements.
 - a is furthest from the critical points and still provides good audio quality at the critical point
 - b complies with the [“Rules and guidelines to locate cell centers” \(page 35\)](#)
 - c is in the coverage area
 - 10 With a pencil, label the cell center on the floor plan with xCn. The x is the floor, and n is the cell number in sequence of the entire plan.


 - 11 Place the deployment tool at each cell center to locate the cell boundary.
 - 12 Mark the cell boundary on the floor plan.
 - 13 Repeat this task for the remaining coverage area from the extremes of the coverage area toward the center until the entire floor is been covered.
 - 14 If the cell boundary covers any other critical points, ignore these critical points as you proceed with coverage deployment.

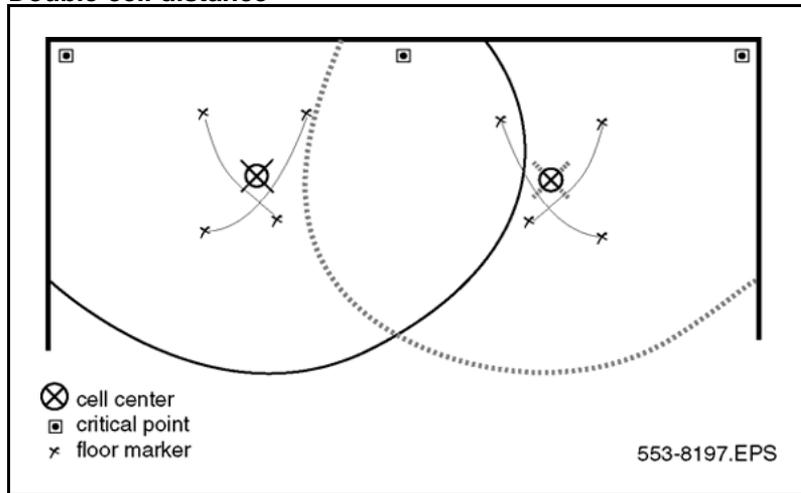
Note: If it is not possible to place the basestation at the exact crossover points of the arcs, place the basestation as close as possible to the crossover.

--End--

Double cell deployment

Use the double cell technique only if referred here from the single cell technique. Before beginning this technique, there must be two critical points that one cell center cannot serve. Using the double cell technique, find two locations for cell centers that cover three critical points, as shown in Figure 44 "Double cell distance" (page 75).

Figure 44
Double cell distance



Procedure 15

Double cell deployment

Step	Action
1	Mark a third critical point midway between the two critical points already identified.
2	Place the deployment tool at this midway critical point.
3	Establish a link.
4	Walk briskly into the coverage area within range of either of the first two critical points until the cell boundary is reached.
5	Record the cell boundary by marking a small X on the floor plan where the cell boundary is located.
6	Repeat step 4 and 5 several times, walking in different directions to determine where the cell center can be located and still be within range of the critical point.
7	Draw a thin contour line through the Xs to mark an arc on the floor plan.
8	Repeat steps 2 through 5 walking into the coverage area of the other of the first two critical points.
9	If the contour lines do not cross, or if the amount of overlap between the cells is less than half the distance between the cell

- center and the cell boundary, see [“Multi cell deployment” \(page 76\)](#).
- 10** Choose a position on the floor plan for the cell center that meets the following requirements.
- a** is furthest from the critical points and still provides good audio quality at the critical point,
 - b** complies with the [“Rules and guidelines to locate cell centers” \(page 35\)](#), and
 - c** is in the coverage area.
- 11** Mark each cell c on the floor plan and label them **1C1** and **1C2**.



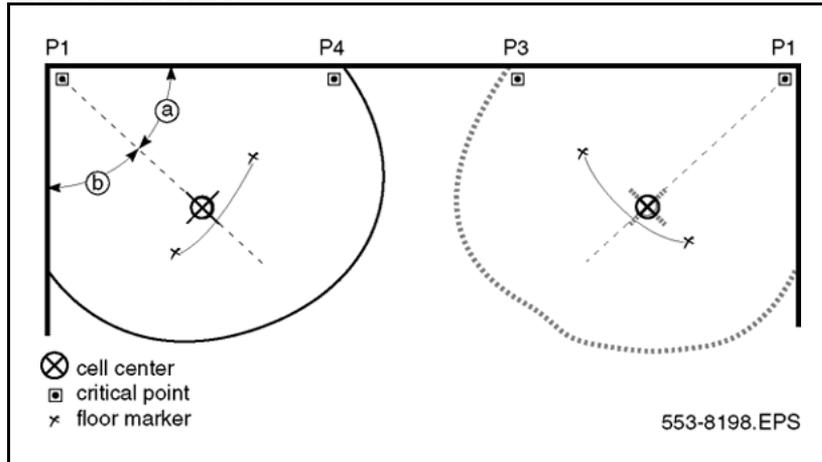
- 12** Place the deployment tool at each cell center to find the cell boundary and mark it on the floor plan.
- 13** Repeat this technique for the remaining coverage area from the outer extremes of the coverage area toward the center until the entire floor has been covered. If the cell boundary covers other critical points, ignore these critical points as you deploy coverage.

--End--

Multi cell deployment

Use the multi cell technique only if referred here from the double cell technique. Before beginning this technique, there must be two critical points that one cell center cannot serve. Using the multi cell technique, two cell centers, each one serving one of the two critical points, are found, as shown in [Figure 45 "Multi-cell distance" \(page 77\)](#).

Figure 45
Multi-cell distance



Procedure 16
Multi-cell deployment

Step	Action
1	Choose a position on the floor plan for the cell center that meets the following requirements. <ul style="list-style-type: none"> a is furthest from the critical points and still provides good audio quality at the critical point, b complies with the “Rules and guidelines to locate cell centers” (page 35), and c is in the coverage area.
2	Place the deployment tool at critical point P1 .
3	Establish a link.
4	Walk briskly into the coverage area away from the critical point until the cell boundary is reached.
5	Mark a small X on the floor plan where the cell boundary is found.
6	Repeat step 4 and 5 several times, walking in different directions from the critical point to establish an arc. The arc is at the cell boundary and is within range of the critical point.
7	Draw a thin contour line to mark an arc through the Xs on the floor plan.
8	Repeat steps 4 through 7 walking into the coverage area of critical point P2 .
9	Locate the cell center on the arc along a line from the critical point that is equal distant from the adjacent walls.

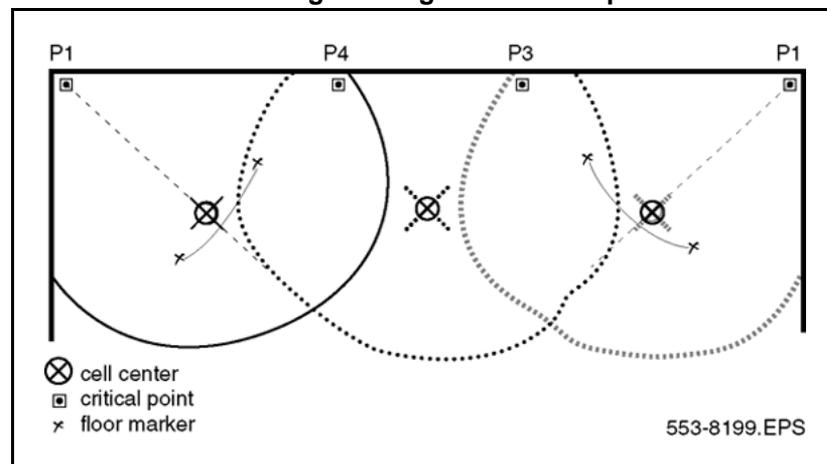
- 10 Mark each cell center on the floor plan and label them **1C1** and **1C2**.



- 11 Place the deployment tool at each cell center.
- 12 Locate the cell boundary and mark it on the floor plan. (Mark the contours in different colors for easy differentiation of cell centers.)
- 13 Define and mark on the plan subsequent critical points, where each cell boundary crosses the edge of the coverage area.
- 14 If the cell boundary covers other critical points, ignore these critical points as you proceed with coverage deploying.
- 15 Repeat the multi cell technique for the remaining area to be covered, from the extremes of the coverage area toward the center, until all of the floor is covered.

Figure 46

Multi cell distance using the single cell technique



- 16 Use the subsequent critical points to fill in the coverage area between the first two cells using the “Single-cell deployment” (page 73). An example of this is shown in Figure 46 “Multi cell distance using the single cell technique” (page 78).

--End--

Multiple floor deployment

This applies to deployment scenarios in the following situations.

- The coverage area is on more than one floor.
- The floors are not adjacent to each other.

Checking for through-the-floor coverage

The first step in covering a multi-floor building is assessing the availability of through-the-floor coverage. In buildings mainly constructed of wood, through-the-floor coverage can be used. However, due to the construction of most modern buildings with raised floors, high metal content, and reinforced concrete, through-the-floor coverage with DECT is limited.

Procedure 17

Checking for through-the-floor coverage

Step	Action
1	Place the deployment tool in a middle floor of the site.
2	Go to the floor above the deployment tool and establish a link with the deployment handset. Follow the steps in Procedure 10 "Testing the deployment tool handset" (page 60).
3	Measure the deployment contour as if the basestation was on this floor, instead of the floor below. If only a small area is covered (less than 10 metres radius), there is effectively no through-the-floor coverage on the floor above an installed basestation.
4	Go to the floor below the deployment tool and repeat the preceding process. If the area that can be covered is small, there is no through-the-floor coverage below a basestation location.
5	If there is no through-the-floor coverage or coverage is restricted to a small area. Deploy each floor using critical points, or if the floors are exactly similar, deploy as multi floors with the same layout.
--End--	

Assess floor layout

The deployment procedure changes according to the similarities and differences of the floors.

All floors have the same layout To begin a multi-floor deployment if all of the floors have the same layout, deploy one floor and enter the data on the floor plan. Use the data from the deployed floor for other identical floors.

For example, if floor 2 of an office tower is laid out with cubicle style offices with a perimeter of enclosed offices, and floor 3 is designed and laid out in the **exact** same manner, both floors can have the exact same installation profile for basestations.

All floors do not have the same layout If there are **deviations** in the floor plan from floor to floor, use the critical point method to deploy each distinct floor. For more information, see [“Prepare the tool for deployment” \(page 54\)](#).

Note: Do not underestimate the importance of changes in floor layout. Simple changes in a room from a meeting room to a storage room can have significant impact on the coverage from a basestation.

Multi floor coverage situations

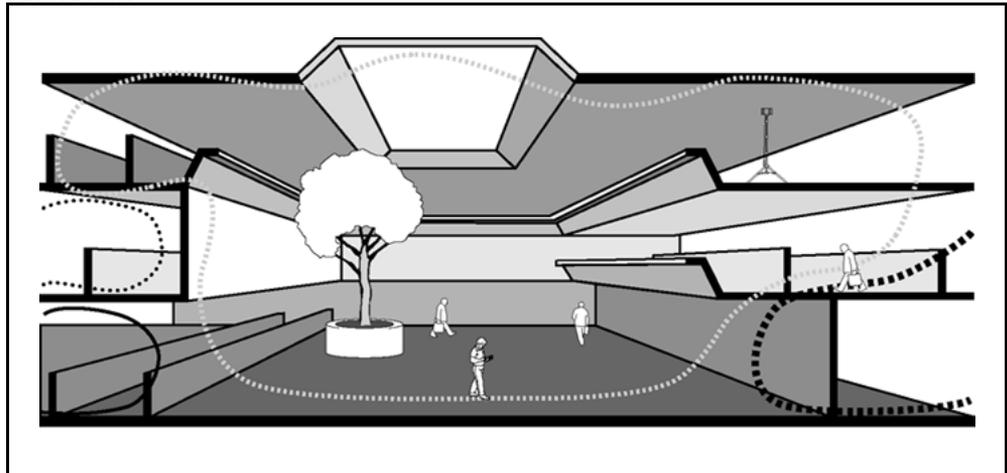
The following situations require multi-floor coverage.

- [“Atriums” \(page 80\)](#) .
- [“High rise buildings” \(page 81\)](#) .
- [“Unusual conditions” \(page 81\)](#) .

Use the multi floor coverage procedure, if required. for more information, see [“Gather building information” \(page 24\)](#).

Atriums Cells in an atrium, as shown in [Figure 47 “An atrium” \(page 80\)](#), are usually larger than the cells of the rest of the building. This section gives guidelines on how to plan an atrium. There are no precise steps to follow if deploying an atrium, but there are points to consider. See [“Unusual conditions” \(page 81\)](#) .

Figure 47
An atrium



Consider the following if deploying an atrium.

- Plan atriums to their full height.
- Plan an atrium as one full size room, not floor by floor.
- Place cell centers within an atrium only if you intend for them to cover the atrium.
- Do not put cell centers in an atrium if you intend for them to serve adjacent areas.
- To serve adjacent areas, put the cell centers into these areas.
- Deploy the atrium first if the atrium is more than a third the size of the building, or more than one cell in size.
- If cell centers in adjacent dense areas serve one floor of an atrium, verify the coverage of the cell on all of the floors that meet with the atrium.

High rise buildings Deploy high rises buildings as unusual conditions of multi-floor deployment.

Test through-the-floor coverage first. If there is no through-the-floor coverage, deploy each floor. Repeat for as many floors as possible where the floor layout is the exact same as any other. In all other cases deploy floor by floor. A floor with many meeting rooms deploys differently from a building with cubicle style offices.

Unusual conditions There are no precise steps to follow if deploying for an unusual condition, but there are points to be considered.

To plan an unusual condition, consider the following situations.

- [“Cell centers are too close ” \(page 81\)](#)
- [“Cell centers are too far apart ” \(page 81\)](#)
- [“Too many cell centers ” \(page 82\)](#)

Cell centers are too close If cell centers are deployed less than 10 metres apart, the handsets can initiate unnecessary hand over. Unnecessary hand over result in excessive internal messaging and degraded speech quality.

Cell centers are too far apart If cell centers are deployed too far apart, the edge of a cell does not overlap the coverage from another cell.

Cell centers must be located within the edge of other cell centers to provide satisfactory overlap.

Overlap can be difficult to achieve where coverage is received from the floor above or the floor below. Internal structures can cause overlap deficiencies.

Cell centers do not need to be located on the same floor or an adjacent floor of the area that it is covering. Place cell centers within the cell boundary, as indicated by the deployment tool.

The installation of basestations in places other than the location shown on the plan can cause coverage problems; for example, if the basestation is mounted on the opposite side of a wall from its planned location.

Consider the following for basestation locations.

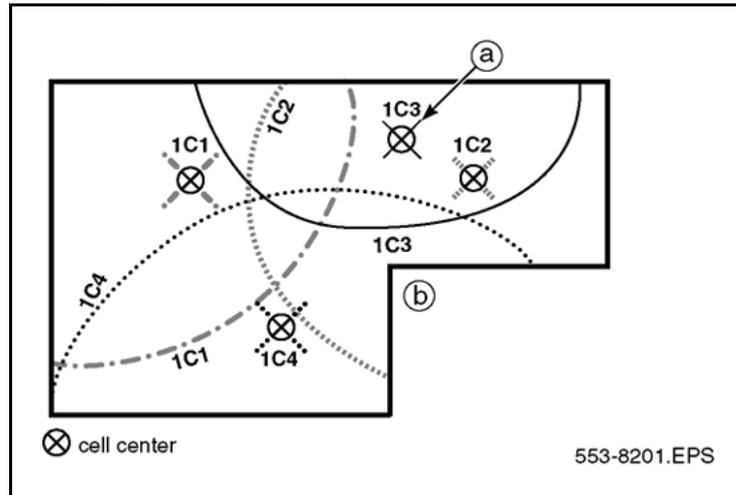
- Choose locations only where it is possible to mount basestations.
- Install basestations as close as possible to planned locations.
- Follow safety codes or aesthetic considerations.
- Allow sufficient access for installation of basestations.
- Provide clear installation instructions.
- Test the coverage during post-deployment checks.

Too many cell centers The primary concern with deploying too many cell centers is cost. To deploy the correct number of cell centers and reduce cost, perform the following.

- Verify the coverage and traffic volume before adding additional cells.
- Remove a cell served by other cells unless it is required for high handset density.
- Verify the coverage area of each cell.
- Verify that there is at least one area that each cell serves that is not served by another cell.

In the example shown in [Figure 48 "Locating redundant cells" \(page 83\)](#), cell 1C3 is redundant unless required for high handset density.

Figure 48
Locating redundant cells



Reengineer cells for high traffic areas

To accommodate the demand in high traffic areas, follow the “[The cell reengineering process](#)” (page 83).

Traffic volume

The deployment process ensures coverage throughout the service area. It does not, however, take into account the effect of traffic. To support the volume of telephone calls in cells that carry high traffic, it is necessary to increase the number of cells deployed.

ATTENTION

If you install two DAPs close to each other for extra traffic density, ensure the distance between the DAPs is always more than one meter and preferably more than five meters.

The calculation of expected telephone traffic includes an allowance for the user population in a cell, and the roaming user.

The cell reengineering process

The cell reengineering process involves the following.

- “[Estimating traffic within a cell](#)” (page 84).
- “[Separating the coverage area and recording the number of offices](#)” (page 85).
- “[Creating an estimate table](#)” (page 85).
- “[Calculating the number of users inside the cell with an office](#)” (page 86).

- “Calculating the number of users with an office outside the cell who walk into the cell” (page 87).
- “Calculating the number of users without an office” (page 88).
- “Totalling the estimate for users in a cell” (page 89).
- “Calculating the data for all remaining cells” (page 89).
- “Creating a table to document telephone types in a cell” (page 90).
- “Determining cell reengineering” (page 91).

Estimating traffic within a cell

Modify the previous deployment procedure to adjust the estimated number of users. To carry out this procedure, perform the following.

- Determine the number of handset users with an office within each cell.
- Determine how many of these users have wired phones.
- Determine how many users without an office are normally in each cell.

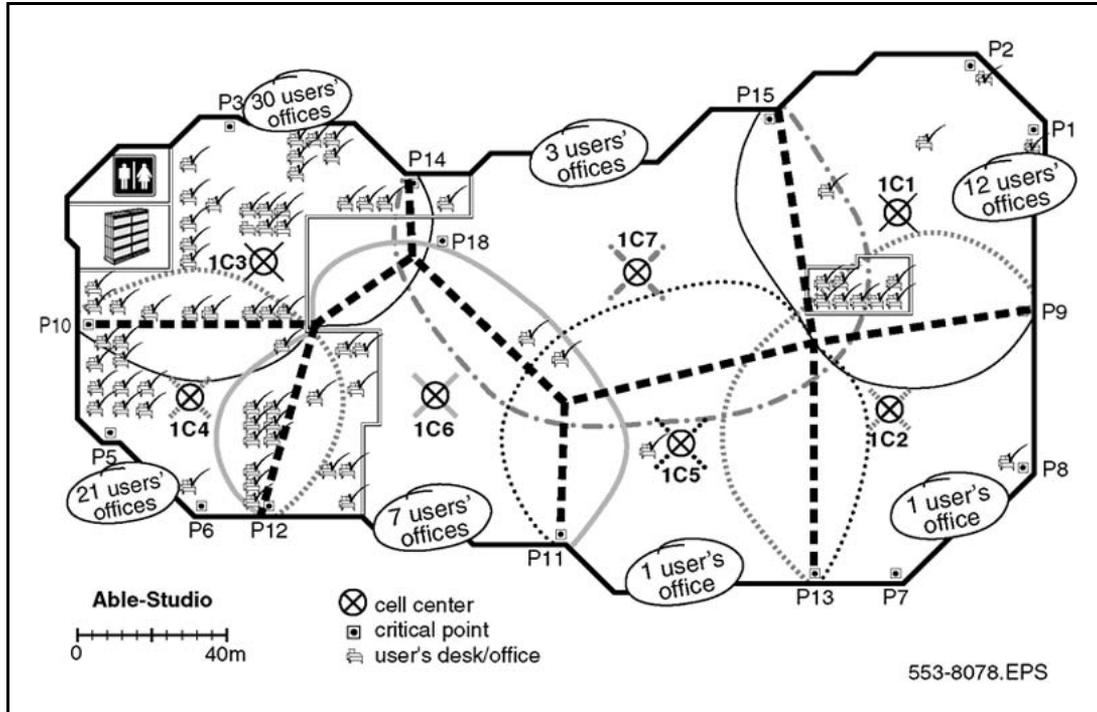
Some users have both wired and handset phones; other users rely on handsets only.

Reengineered cells for high traffic areas are represented by an adjusted estimate for the two groups: handset and wireless, and handset only. Use the adjusted estimate to determine whether the cell sizes, indicated by the earlier deployment procedure, can handle the telephone traffic.

If the traffic handling capacity of the cells is not adequate, use 12-channel basestations and subdivide them into smaller cells to ensure the traffic is handled properly in accordance with these instructions.

Separating the coverage area and recording the number of offices

Figure 49
Example of dividing the coverage area and recording offices



Procedure 18 Separating the coverage area and record the number of offices

Step	Action
1	<p>Divide the floor plan into cell areas.</p> <p>Mark the cell areas on the floor plan, one area for each cell, splitting cell overlap areas in half, shown in Figure 49 "Example of dividing the coverage area and recording offices" (page 85) as heavy dotted lines.</p>
2	<p>Count the number of user offices in each cell area.</p> <p>Record the number of user offices on the floor plan in each cell area.</p>

--End--

Creating an estimate table

Use the following table to estimate the number of handset users for each cell.

Table 9
Estimate users in a cell

Estimate for:	1C1	1C2	1C3	1Cn
Users inside the cell with an office				
Users with an office outside of a cell who walk into the cell				
Users without an office				
Users in a cell				

Procedure 19
Creating an estimate table

Step	Action
1	Make an estimate table. Include as many columns as there are cell centers.
2	Label the rows. Example shown in Table 9 "Estimate users in a cell" (page 86) .
3	Label each column heading with the cell center indicator. Use this table to determine how many times to subdivide each cell to carry the handset telephone traffic.
--End--	

Calculating the number of users inside the cell with an office

Table 10
Example of the table first row calculation

Estimate for:	1C1	1C2	1C3	1C4	1C5	1C6	1C7
Users inside the cell with an office	8.4						
Users with an office outside of a cell who walk into the cell							
Users without an office							
Users in a cell							

Procedure 20
Calculating the number of users inside the cell with an office

Step	Action
1	Calculate the estimate for users in the first cell with an office.

- Use the formula: (users with an office in the cell × 0.7)
- 2 Enter the result in the row, users inside the cell with an office.
- In the example shown in [Figure 49 "Example of dividing the coverage area and recording offices" \(page 85\)](#), twelve users in cell 1C1 spend 70% of their time in their offices (12 × 0.7 = 8.4) .

--End--

Note: Traffic engineering has determined that handset users with an office spend seventy percent of their time within their home cell.

Calculating the number of users with an office outside the cell who walk into the cell

Table 11
Example of the table second row calculation

Estimate for:	1C1	1C2	1C3	1C4	1C5	1C6	1C7
Users inside the cell with an office	8.4						
Users with an office outside of a cell who walk into the cell	3.2						
Users without an office							
Users in a cell							

Procedure 21

Calculating the number of users with an office outside the cell who walk into the cell

Step	Action
1	Calculate the estimate for users in the first cell with an office outside of the cell who walk into the cell.
2	Use the formula: $\frac{(\text{Total users with an office} - \text{Users with an office inside the cell}) \times 0.3}{(\text{Total number of cells} - 1)}$
3	Enter the result in the row, users with an office outside the cell who walk into the cell. For the example shown in Figure 49 "Example of dividing the coverage area and recording offices" (page 85) , there are a total of 75 telephone users in Able-Studio, minus the 12 users already in cell 1C1. Therefore, 63 users can walk into cell 1C1. However, the 63 walk in users only spend 30% of their time outside their offices. There are seven cells on the floor plan

minus cell 1C1. Accordingly, an estimate of 3.2 walk-in users can be in cell 1C1.

$$\frac{(75 - 12) \times 0.3}{(7 - 1)} = 3.2$$

--End--

Calculating the number of users without an office

Table 12
Example of the table third row calculation

Estimate for:	1C1	1C2	1C3	1C4	1C5	1C6	1C7
Users inside the cell with an office	8.4						
Users with an office outside of a cell who walk into the cell	3.2						
Users without an office	0						
Users in a cell							

Procedure 22
Calculating the number of users without an office

Step	Action
------	--------

- | | |
|---|--|
| 1 | Calculate the estimate for users in the first cell without an office. Use the formula: |
|---|--|

$$\frac{\text{Total number of users without an office}}{\text{Number of cells}}$$

- | | |
|---|---|
| 2 | Enter the result in the row, users without an office.
In the example shown in Figure 49 "Example of dividing the coverage area and recording offices" (page 85), there are no users without an office. |
|---|---|

--End--

Totalling the estimate for users in a cell

Table 13
Example of the table first column total

Estimate for:	1C1	1C2	1C3	1C4	1C5	1C6	1C7
Users inside the cell with an office	8.4						
Users with an office outside of a cell who walk into the cell	3.2						
Users without an office	0						
Users in a cell	11.6						

Procedure 23 Totalling the estimate for users in a cell

Step	Action
------	--------

- | | |
|---|--|
| 1 | Total the estimate for the number of users in the first cell by adding the three rows in the first column. |
| 2 | Enter the result in the bottom row users in a cell.

For the example shown in Figure 49 "Example of dividing the coverage area and recording offices" (page 85), the 1C1 handset estimate equals 11.6.

$8.4 + 3.2 + 0 = 11.6$. |

--End--

Calculating the data for all remaining cells

Table 14
Example of a completed estimate table

Estimate for:	1C1	1C2	1C3	1C4	1C5	1C6	1C7
Users inside the cell with an office	8.4	0.7	21.0	14.7	0.7	4.9	2.1
Users with an office outside of a cell who walk into the cell	3.2	3.7	2.3	2.7	3.7	3.4	3.6
Users without an office	0	0	0	0	0	0	0
Users in a cell	11.6	4.4	23.3	17.7	4.4	8.3	5.7

Procedure 24
Calculating the data for all remaining cells

Step	Action
1	Repeat the last four tasks to calculate all the remaining user cell estimates.
2	Enter the result in the estimate table. The information in Figure 49 "Example of dividing the coverage area and recording offices" (page 85) , is shown entered into Table 14 "Example of a completed estimate table" (page 89) . This table is used to note the results of the calculations for cells that require reengineering.
--End--	

Creating a table to document telephone types in a cell

Use a table like [Table 15 "Telephone types in a cell" \(page 90\)](#) to record the different telephone types in each cell.

Table 15
Telephone types in a cell

Telephone type	1C1	1C2	1C3	1Cn
User telephone types				

Use the following symbols in each cell to denote the type of telephones in use in the cell.

- **H&W** for a cell in which all the users have both wired and handsets (wireless phones).
- **H** for a cell in which users have only handsets (wireless phones).
- **M** for a mix of H and H&W users

Procedure 25
Creating a table to document telephone types in a cell

Step	Action
1	Make a Telephone types table.
2	Label the row, User telephone types and include as many columns as there are cell centers.
3	Label each column heading with the cell center indicator.

The information in this table is used to determine the number of cells that require reengineering.

--End--

Determining cell reengineering

Table 16
Example of a completed estimate table

Estimate for:	1C1	1C2	1C3	1C4	1C5	1C6	1C7
Users inside the cell with an office	8.4	0.7	21.0	14.7	0.7	4.9	2.1
Users with an office outside of a cell who walk into the cell	3.2	3.7	2.3	2.7	3.7	3.4	3.6
Users without an office	0	0	0	0	0	0	0
Users in a cell	11.6	4.4	23.3	17.7	4.4	8.3	5.7

Table 17
Example of a completed telephone types table

Telephone type	1C1	1C2	1C3	1C4	1C5	1C6	1C7
User telephone types	H&W	H&W	M	M	H&W	H&W	H&W

Table 18
Cell reengineering

Estimate for:		
Users with both a handset and a wired telephone	Users with only a handset	Action
From 0 up to 20	From 0 up to 12	Keep cell size as deployed.
Greater than 20 but no more than 80	Greater than 12, but no more than 40	Install a 12-channel basestation or subdivide the cell ^a .
Greater than 80	Greater than 40	Subdivide the cell ^a to meet the preceding conditions.

a. For details about how to subdivide cells, see [“High handset density deployment”](#) (page 95). Use a 12-channel basestation in areas of high traffic capacity. Cell subdivision is appropriate if it helps to improve coverage where the loop resistance exceeds 100 ohms or if a Digital Mobility Controller (DMC) cannot support more than two 12-channel units.

Note: Use [Table 18 “Cell reengineering”](#) (page 91) only for user types H&W and H. For user type M see [“A mix of users with and without wired telephones in a cell”](#) (page 93).

Procedure 26
Determining cell reengineering

Step	Action
1	Locate the estimate for users in the first cell. In the example shown in Table 16 "Example of a completed estimate table" (page 91) , the handset estimate is 11.6.
2	Determine the telephone types in the first cell. In the example shown in Table 16 "Example of a completed estimate table" (page 91) , the telephone type is H&W.
3	Locate the telephone type column in Table 16 "Example of a completed estimate table" (page 91) . In the example H&W is the users with both a handset and a wired telephone.
4	Find the handset estimate range in Table 18 "Cell reengineering" (page 91) . In the example, 11.6 falls within the From 0 up to 20 category.
5	Determine if a cell requires division or uses a 12-channel basestation. In the example From 0 up to 20, division is not required.
6	Repeat the preceding steps to determine the required number of cells that need subdivision, except for telephone types M. For M see "A mix of users with and without wired telephones in a cell" (page 93) .
7	Transfer the results into the provisioning records.

--End--

Cell division requirements in special cases

This section describes how to determine cell division in the following special cases.

- Where no office information is available.
- Where there is a mix of handset users with and without wired telephones.

No office information

If the location of the offices of users is not known, calculate the estimated number of handsets for each cell using this formula.

$$\frac{\text{Number of handsets}}{\text{Number of cells}}$$

The formula assumes that users are located evenly throughout the cells. However, most users offices are clustered in specific areas of a building.

The formula has limitations, as cells can vary in size. The method described starting on [“The cell reengineering process”](#) (page 83) gives more accurate cell division results.

A mix of users with and without wired telephones in a cell

Use this procedure for mixed handset users. This procedure lets the telephone traffic generated by handset users to be equated to that of handset and wired users. Combine the two groups for cell size recalculation purposes.

Table 19
Adjustment for users without wired telephones

Estimated number of handsets for users without wired telephones	Adjusted estimated number of handsets for each cell
0	0
1	2
2	3
3	5
4	7
5	9
6	11
7	12
8	14
9	16
10	18
11	20
12	22
13	24
14	25
15	27
16	29
17	31
18	34
19	36

Table 19
Adjustment for users without wired telephones (cont'd.)

Estimated number of handsets for users without wired telephones	Adjusted estimated number of handsets for each cell
20	38
21	40
22	42
23	44
24	46
25	48
26	49
27	50
28	53
29	55
30	57
31	60
32	62
33	64
34	66
35	69
36	71
37	73
38	76
39	78
40	80

Procedure 27
Adjusting for users without wired telephones

Step	Action
1	Count the number of user offices with handsets and wired telephones (H&W), and record the number.
2	Count the number of user offices that have only wireless handsets, (H).
3	Use Table 19 "Adjustment for users without wired telephones" (page 93) to determine the equivalent number of H&W users and record this number.
4	Add the numbers received from steps 1 and 3 to determine and adjust the value for the number of users with wired telephones.

- 5 Use [Table 19 "Adjustment for users without wired telephones" \(page 93\)](#) to determine the criteria shown in the left column to determine if the cell has to be re-sized in the same manner described in the section Determine cell reengineering.

--End--

High handset density deployment

The high handset density deployment includes limiting the expected number of handsets for each cell center.

Note: Use the high handset density procedure if instructed to do so from [Table 18 "Cell reengineering" \(page 91\)](#). Do not use more than one basestation for each cell center.

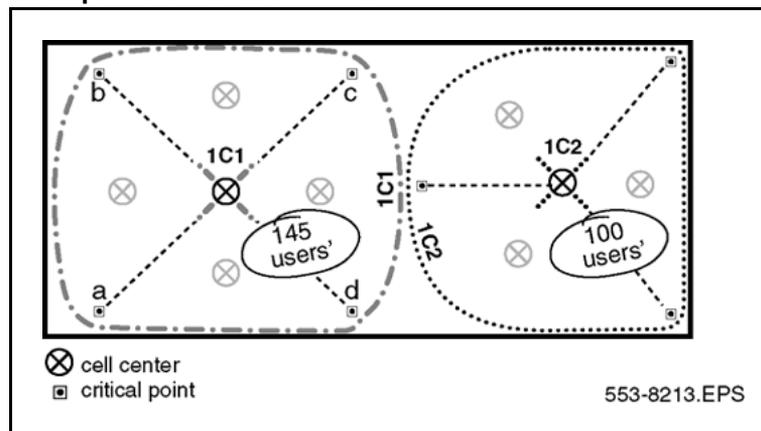
Limit the anticipated number of handsets

Limit the number of handsets you anticipate for each cell center to the limits shown in [Table 18 "Cell reengineering" \(page 91\)](#). Only subdivide high handset density areas. If a cell falls into the category of a high density area, use [Procedure 28 "High handset density deployment" \(page 96\)](#) to subdivide the cell.

Subdivide a cell

To subdivide the area for smaller cells, divide the cell into as many smaller cells as necessary to provide for the number of users in the area.

Figure 50
Example of a subdivided cell



In [Figure 50 "Example of a subdivided cell" \(page 95\)](#), cell 1C1 has 140 handset users and cell 1C2 has 100 handset users. For example, [Table 18 "Cell reengineering" \(page 91\)](#) indicates the following.

- If the handset users in cell 1C1 are all handset only users, one cell can support 39 handset only users. Therefore, four cells are needed to support 140 users ($140 \div 39 = 3.5$ cells).
- If the handset users in cell 1C1 are handset and wired telephone users, and one cell can support 83 users, two cells are needed to support 140 handset and wired telephone users ($140 \div 83 = 1.6$ cells)

Procedure 28
High handset density deployment

Step	Action
1	Determine the number of handset users in the high handset density cell. Count the number of users. Include users served by through-the-floor coverage of this cell.
2	Calculate the cell subdivisions as required. Divide the number of users by the appropriate value (12 or 20) shown in Table 18 "Cell reengineering" (page 91) . Round up the result to the next whole number. The result equals the number of cells required after subdividing the cell.
3	Divide the cell. Draw lines from the cell center to the critical points on the cell boundary. Shown in Figure 50 "Example of a subdivided cell" (page 95) , the cell 1C1 divides into four sectors and cell 1C2 divides into three sectors.
4	Relocate new cell centers. Mark new cell centers within the sectored areas.
5	Determine the number of handset users in the new cell areas. Count the number of user offices within each smaller sector. Ensure there are fewer user offices within the cell than the traffic limit.
6	Verify locations. Take the deployment tool to the locations calculated on the floor plan. Ensure that there is a location that meets the guidelines in "Rules and guidelines to locate cell centers" (page 35) .
7	Ensure the new cells have complete coverage. Use the deployment handset to check coverage.

- 8 Repeat the anticipated handsets for each cell calculation to ensure that each smaller cell provides appropriate traffic coverage to the users in the area.

--End--

Deployment review

Review the plan to ensure that the sales group can use it. The plan must be complete for the installer, legible for maintenance purposes, and acceptable to the customer.

Floor plan completion

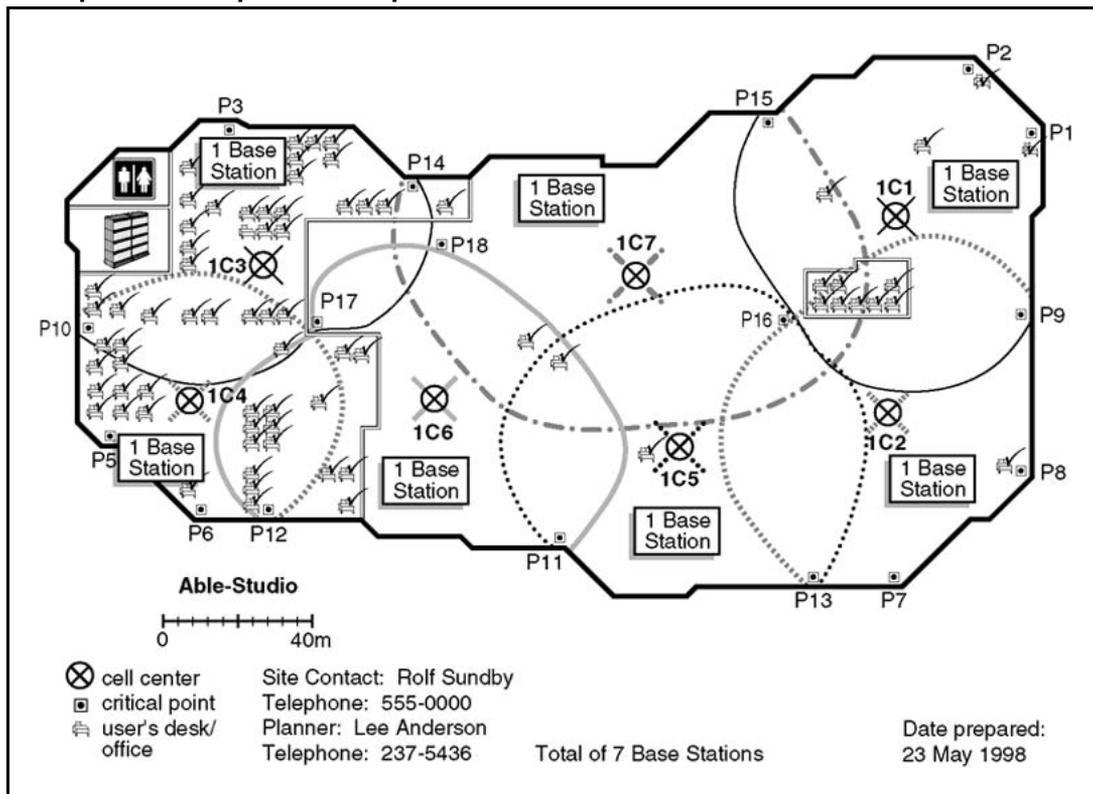
Procedure 29

Completing a floor plan

Step	Action
1	Record the name and telephone number of the planner on the floor plans.
2	Record the name of the customer company on the floor plans.
3	Record the site contact name and telephone number on the floor plans.
4	Record installation restrictions.
5	Record the details of the installation of an identified cell on the floor plans, recording 12-channel basestations.
6	Record the positions of user offices on the floor plans.

--End--

Figure 51
Example of a completed floor plan



Hardware installation

Navigation

This chapter contains information about the following topics.

- “Call server” (page 99)
- “Signaling server” (page 99)
- “PC (DAP controller)” (page 100)
- “DECT Access Points” (page 100)

Call server

Install and connect the appropriate call server to your local Ethernet network.

Communication server types are supported.

- Communication Server 1000E
- Communication Server 1000M

For details about Communication Server 1000S CP PM hardware installation, see *Communication Server 1000E Upgrade - CS 1000S to CS 1000E* (NN43041-470) .

For details about Communication Server 1000E hardware installation, see *Communication Server 1000E Installation and Commissioning* (NN43041-310) .

For details about Communication Server 1000M hardware installation, see *Communication Server 1000M and Meridian 1 Large System Installation and Commissioning* (NN43021-310) .

Signaling server

Install and connect the appropriate signaling server to your local Ethernet network.

Signaling Server types are supported.

- ISP1100
- CP PM signaling server
- COTS IBM X306m
- COTS HP DL320-G4

For details about Signaling Server hardware installation, see *Signaling Server Installation and Commissioning* (NN43001-312) .

PC (DAP controller)

Minimum specifications for the PC are as follows.

- 2.4 GHz CPU speed
- 256 MB RAM
- CD-ROM drive
- 1GB free hard disk space

DECT Access Points

Two models of DECT Access Points are currently available for the Nortel SIP DECT system, C4710 and C4710E. C4710E can use external antenna.

- C4710 DECT Access Point:
 - PEC: NTCW26AAE5
 - CPC: N0162007
- C4710E DECT Access Point:
 - PEC: NTCW26BAE5
 - CPC: N0162008

ATTENTION

Only the G711 codec is supported on the C4710 and C4710E DAP models. Ensure that the G711 codec is available in your system and that the G711 codec can be used for any call involving a DECT handset.

It is not possible to make calls between the Nortel IP Softphone 2050 and DECT handsets when the following check box in the Audio settings of the softphone is selected: **I use a modem to connect to the network**. This setting forces the Nortel IP Softphone 2050 to use the G729 codec for all calls.

When using Multimedia PC Client, ensure that you select **Medium Speed** or **High Speed** in the Multimedia PC Client Connection preferences if you plan to make calls between DECT handsets and Multimedia PC Clients.

Ensure that the DAPs are installed according to the location recommendations. For more information, see [“DAP deployment rules and requirements” \(page 27\)](#).

Software requirements

Navigation

This chapter contains information about the following topics.

- “Call server software” (page 103)
- “Signaling server software” (page 103)
- “DAP controller software” (page 103)

Call server software

For details about Communication Server 1000S CP PM software installation, see *Communication Server 1000E Upgrade - CS 1000S to CS 1000E* (NN43041-470) .

For details about Communication Server 1000E software installation, see *Communication Server 1000E Installation and Commissioning* (NN43041-310) .

For details about Communication Server 1000M software installation, see *Communication Server 1000M and Meridian 1 Large System Installation and Commissioning* (NN43021-310) .

Signaling server software

For details about Signaling Server software installation, see *Signaling Server Installation and Commissioning* (NN43001-312) .

DAP controller software

This section contains the steps you must follow to configure the SIP DECT system. Before you can use SIP DECT, you must install and configure the following software on the DAP controller PC.

- Microsoft Windows

You can install any of the following operating systems on the DAP controller or manager PC.

- Windows 2000 Professional or Windows 2000 Server (SP4 required)
- Windows 2003 Server (SP1 or SP2 required)
- Windows 2003 R2
- Windows XP Professional (SP2 required)

This document does not provide the steps you must follow to install the operating system. For information about installing Windows, see the documentation that accompanied the Windows software.

Note: If a firewall is installed on your DAP Controller PC, ensure the firewall does not block the ports used for different services. For details, see [“Firewall protection” \(page 104\)](#).

- Internet Explorer 6.0 or higher
- Internet Information Services (IIS)
For information about installing IIS, see [“Internet information services” \(page 105\)](#).
- DHCP and TFTP servers
For information about installing DHCP and TFTP servers, see [“DHCP and TFTP servers” \(page 111\)](#).
- DAP Controller (IP DECT Configurator and DAP Manager)
For information about installing the DAP Controller, see [“DAP Controller” \(page 130\)](#).

Firewall protection

Both Windows XP Professional and Windows 2003 Server have a built-in firewalls.

Note: By default, the firewall under Windows XP Professional does not allow incoming access. However, the DAP Configurator can automatically change the firewall settings. Verify the firewall settings after installation.

If a third-party firewall program is installed on your DAP Controller PC, ensure the firewall does not block the ports used for the SIP DECT system. Some of the ports are defined by default in IP DECT Configurator.

The ports defined by default:

- From 3000 to 22229 – multicast
- From 28000 to 28017 – DAP Controller services
- 30160 – CDA services

Note: If you change default ports in the IP DECT Configurator, ensure that the firewall settings are updated correctly.

Internet information services

The DAP controller or manager runs as a service under Windows. Because the management interface is available through a Web interface, the Web Server IIS must be installed.

In Windows 2000 Professional, Windows XP Professional and Windows 2003 Server, IIS is not installed by default. The next sections guide you through the IIS installation process for Windows XP Professional, Windows 2000 and Windows 2003.

Install and maintain IIS on Microsoft Windows 2000

Use the information in this section to install IIS on Windows 2000, and to ensure that IIS is started.

Install IIS on a PC with Windows 2000

Use the steps in the next procedure to install IIS.

Prerequisites

- You must have the appropriate Windows installation CD-ROM available to complete this procedure.

Procedure 30 Installing IIS for Windows 2000 Professional

Step	Action
1	Click Start > Settings > Control Panel . The Control Panel appears.
2	Double-click Add/Remove Programs . The Add/Remove Programs window appears.
3	Click Add/Remove Windows Components . The Windows Components window appears.
4	In the Windows Components window, select the IIS check box.
5	Click Next .

- 6 Insert the Windows CD-ROM and follow the on-screen instructions.

--End--

Check IIS on PC with Windows 2000

Use the steps in the next procedure to determine whether IIS is started, and to start it if necessary.

Procedure 31

Checking IIS on PC with Windows 2000

Step	Action
1	Open Internet Explorer on the PC where IIS is installed.
2	In the address bar in Explorer, enter localhost/iisHelp/ and then press enter . IIS is running if Help Information appears. You are finished with this procedure. If you cannot reach the Web server through Internet Explorer, check Windows Help and search for IIS. Follow the instructions on Windows Help to check whether or not IIS is started. If IIS is started, you are finished with this procedure. If IIS is not started, go to step 3.
3	If IIS is not started after following the instructions in steps 1 and 2 of this procedure, click Start , go to Settings , and click Control Panel to start IIS manually. Double-click Administrative Tools and then double-click Computer Management .
4	Expand the Services and Applications node in the console tree of the MMC and select Internet Information Services .
5	Click the right mouse button on Internet Information Services to restart the services. Click the right mouse button on the lower levels of Internet Information Services to stop or start the individual services.

--End--

Install and maintain IIS on Microsoft Windows 2003

Use the information in this section to install IIS on Windows 2003, restart IIS, or verify that IIS is operating.

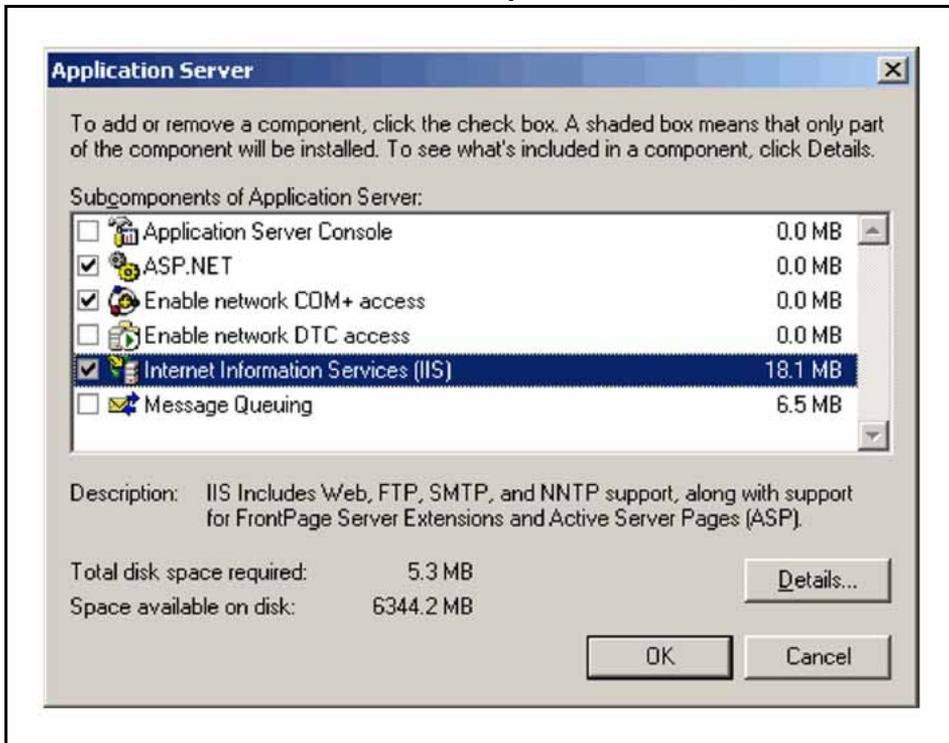
Installing IIS on a PC with Windows 2003

Use the steps in the next procedure to install IIS function on a PC with Windows 2003.

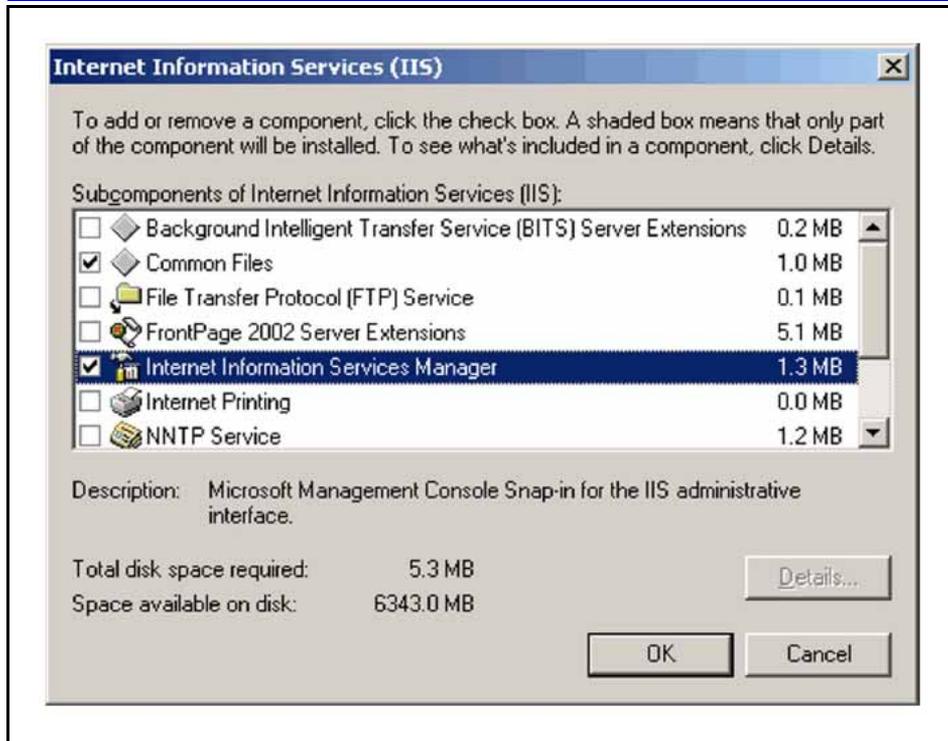
- You must have the appropriate Windows installation CD-ROM available to complete this procedure.

Procedure 32
Installing IIS on a PC with Windows 2003

Step	Action
1	Click Start > Control Panel .
2	Select Add/Remove Programs . The Add/Remove Programs window appears.
3	Click Add/Remove Windows Components .
4	In the Components window, double-click Application Server
5	In the Components window, check ASP.NET .



- 6 Select **Internet Information Services** and click **Details**.
- 7 The following window appears. Select the check boxes for **Internet Information Services Manager** and **Common Files**. Leave the remaining check boxes as they are.



- 8 Click **OK**.
- 9 Click **OK** again.
- 10 Follow the instructions provided by the install Wizard, and insert the Windows CD-ROM as prompted.
- 11 Close the Add/Remove Programs window and close the Control panel window.

--End--

Restart IIS on a PC with Windows 2003

Use the steps in the next procedure to restart IIS.

Procedure 33 Restarting IIS

Step	Action
1	Click Start and open the Control Panel .
2	Click Administrative Tools .
3	Click Computer Management .
4	Expand the Services and Applications node in the MMC and select Internet Information Services .
5	Right-click the Internet Information Services and select All Tasks . The All Tasks menu appears.

- 6 Select **Restart**.
IIS is now restarted.

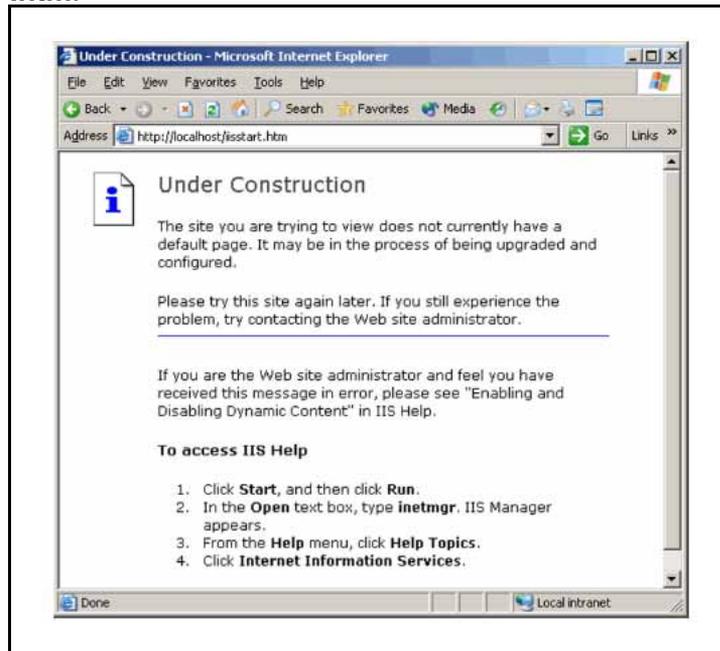
--End--

Check IIS on a PC with Windows 2003

Use the steps in the next procedure to determine whether IIS is started.

Procedure 34 Checking IIS on a PC with Windows 2003

Step	Action
1	Open Internet Explorer on the PC where IIS is installed.
2	In the address bar in Internet Explorer, enter localhost/iisstart.htm .



If IIS is not running properly you can restart IIS. See [Procedure 33 "Restarting IIS"](#) (page 108).

--End--

Install and maintain IIS on Microsoft Windows XP

Use the information in this section to install IIS on Windows XP or verify that IIS is operating.

Install IIS on PC with Windows XP

Use the steps in the next procedure to install the IIS function on a PC with Windows XP.

- You must have the appropriate Windows installation CD-ROM available to complete this procedure.

Procedure 35**Installing WEB Server IIS with Windows XP**

Step	Action
1	Click Start > Settings > Control Panel .
2	double-click Add/Remove Programs . The Add/Remove Programs window appears.
3	Click Add/Remove Windows Components .
4	Select Internet Information Services . <i>Note:</i> Do not select the check box beside Internet Information Services.
5	Click the button Details .
6	In the details window, select the check box World Wide Web Service .
7	Click OK .
8	Click Next .
9	Insert the Windows XP Professional CD. After the system prompts to you insert the CD, click OK . If the Welcome to Microsoft Windows XP window pops up, click Exit in the bottom left corner of the window. The appearance of the window is result of the auto run on the CD.
10	In the Windows Components wizard, click Finish .
11	Close the Add/Remove Programs window and close the Control panel window.
12	If present, remove the CD, DVD, and floppy from your system. Close all windows and restart your computer. After the computer restarts, check that IIS is running. If not, consult the Microsoft web site. To check if IIS is running, see “Check IIS on PC with Windows XP” (page 111) .

--End--

Check IIS on PC with Windows XP

Use the steps in the next procedure to determine whether IIS is started.

Procedure 36

Checking IIS on a PC with Windows XP

Step	Action
1	Open Internet Explorer on the computer where you want to install the DAP manager.
2	Enter the URL localhost/localstart.asp .
3	Ensure that the Internet Information Services (IIS) page appears.



If the IIS start page does not appear, continue to [“Install IIS on PC with Windows XP”](#) (page 110) and install IIS on your computer.

If the IIS start page appears, IIS is installed and is running. Close the window and proceed to [“DHCP and TFTP servers”](#) (page 111).

--End--

DHCP and TFTP servers

Each DAP receives an IP addresses, configuration file and firmware from the IP network using a DHCP server and a TFTP server. Choose whether you want to use the Microsoft Windows DHCP server or the TFTP server or both, or the built-in DAP controller DHCP and TFTP servers.

DHCP servers and TFTP servers are the network components of the Microsoft Windows 2003 Server and the Microsoft Windows 2000 Server. Install these servers as services for SIP DECT system functioning. See [“DHCP and TFTP servers” \(page 111\)](#) for details about Microsoft Windows 2000, 2003 DHCP and TFTP server installation and configuration.

The DAP controller software Release 4 includes DHCP and TFTP servers that can be configured from the IP DECT Configurator. See [“Built-in DHCP and TFTP servers” \(page 124\)](#) for details about built-in DHCP and TFTP servers.

You can create a DAP configuration without DHCP or TFTP, however DHCP and TFTP must be available to program or reprogram DAPs. See [“DAP configuration without DHCP or TFTP servers” \(page 129\)](#) for details about DAP configuration without DHCP or TFTP.

If you prefer to use Microsoft Windows DHCP and TFTP servers, follow the steps in [Procedure 37 “Installing and configuring Microsoft Windows DHCP server” \(page 112\)](#) to install and configure DHCP servers. Follow the steps in [Procedure 40 “Installing the TFTP server” \(page 122\)](#) to install and configure TFTP servers.

If your DHCP server supports Vendor Class Identification option 60, use a specific IP address range for the DAPs. The Vendor Class Identification of the DAPs is **D(ECT)AP 49**.

Procedure 37
Installing and configuring Microsoft Windows DHCP server

Step	Action
1	Ensure that your DHCP server provides the following data to the DAP. <ul style="list-style-type: none">• IP Address• Subnet Mask• Default Gateway IP address• Next Boot Server IP address that is the IP address of the TFTP server (DHCP option 066)• Configuration file name (dapcfg.txt) available through the TFTP server (DHCP option 067)

The DHCP server can be installed on the same server or on another PC that runs the TFTP server.

Note: The Microsoft DHCP server installation files are located on the Microsoft Windows 2000/2003 Server CD-ROM package. Licensing or registration charges or both may apply.

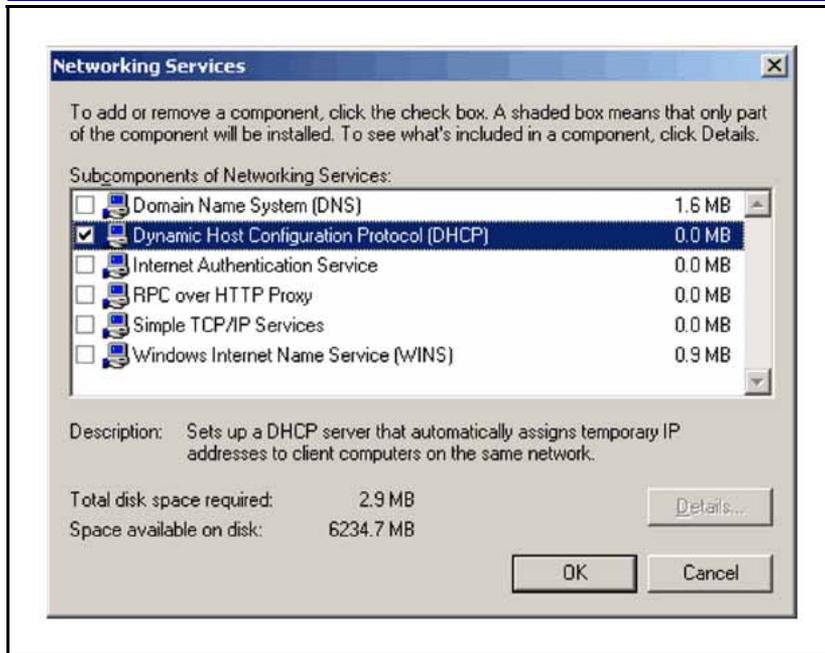
--End--

The DHCP server can be installed on the same server or on another PC that runs the TFTP server. The Microsoft DHCP server (Windows 2000/2003) is in the Microsoft Windows 2000/2003 Server CD-ROM package.

The following procedures give an example of setting up the DHCP server under Windows 2003 Server. This procedure is also applicable for Windows 2000 DHCP server, but there are some minor differences.

Procedure 38
Configuring DHCP server under Windows 2000/2003 server

Step	Action
1	From the Start menu, through the settings in Windows 2000, open the Control Panel in Windows.
2	Open Add/Remove Programs .
3	Click on Add/Remove Windows Components .
4	Select Networking Services and click Details . The Components window appears.
5	Select the check box Dynamic Host Configuration Protocol (DHCP) .

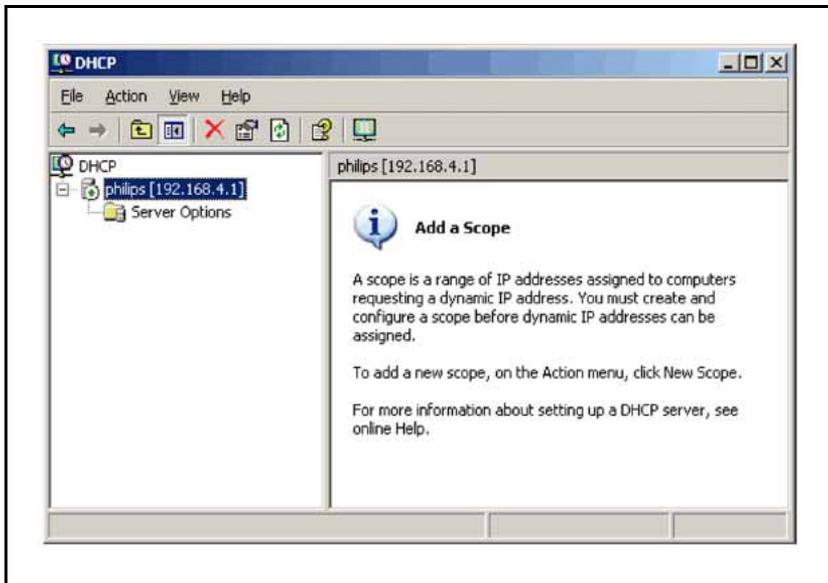


- 6 Click **OK**.
- 7 Click **Next**.
- 8 Insert the Windows 2003 CD-ROM as prompted.
- 9 Finish the procedure using the instructions on the screen.
- 10 Close the **Add/Remove Programs** window and close the Control panel window.

--End--

Procedure 39 Configuring the Settings for SIP DECT

Step	Action
1	Start the DHCP manager: Start > Programs > Administrative Tools > DHCP . The DHCP Administration Tools window appears.



- 2 Select the active DHCP server and create a new scope: **Menu-bar > Action > New Scope**. The New Scope Wizard starts.
- 3 Click **Next** in the first screen of this wizard.
- 4 Enter a name and description for the new scope, for example, SIP DECT.
- 5 Click **Next** in the naming screen of this wizard to get the IP address range.
The window **New Scope Wizard—IP address range** appears.

The screenshot shows a Windows-style dialog box titled "New Scope Wizard" with a close button (X) in the top right corner. The main heading is "IP Address Range" with a folder icon to its right. Below the heading is the instruction: "You define the scope address range by identifying a set of consecutive IP addresses." The main area contains the text: "Enter the range of addresses that the scope distributes." followed by two input fields: "Start IP address:" with the value "192 . 168 . 100 . 200" and "End IP address:" with the value "192 . 168 . 100 . 210". Below this is another instruction: "A subnet mask defines how many bits of an IP address to use for the network/subnet IDs and how many bits to use for the host ID. You can specify the subnet mask by length or as an IP address." This is followed by two input fields: "Length:" with a dropdown menu showing "24" and "Subnet mask:" with the value "255 . 255 . 255 . 0". At the bottom of the dialog are three buttons: "< Back", "Next >", and "Cancel".

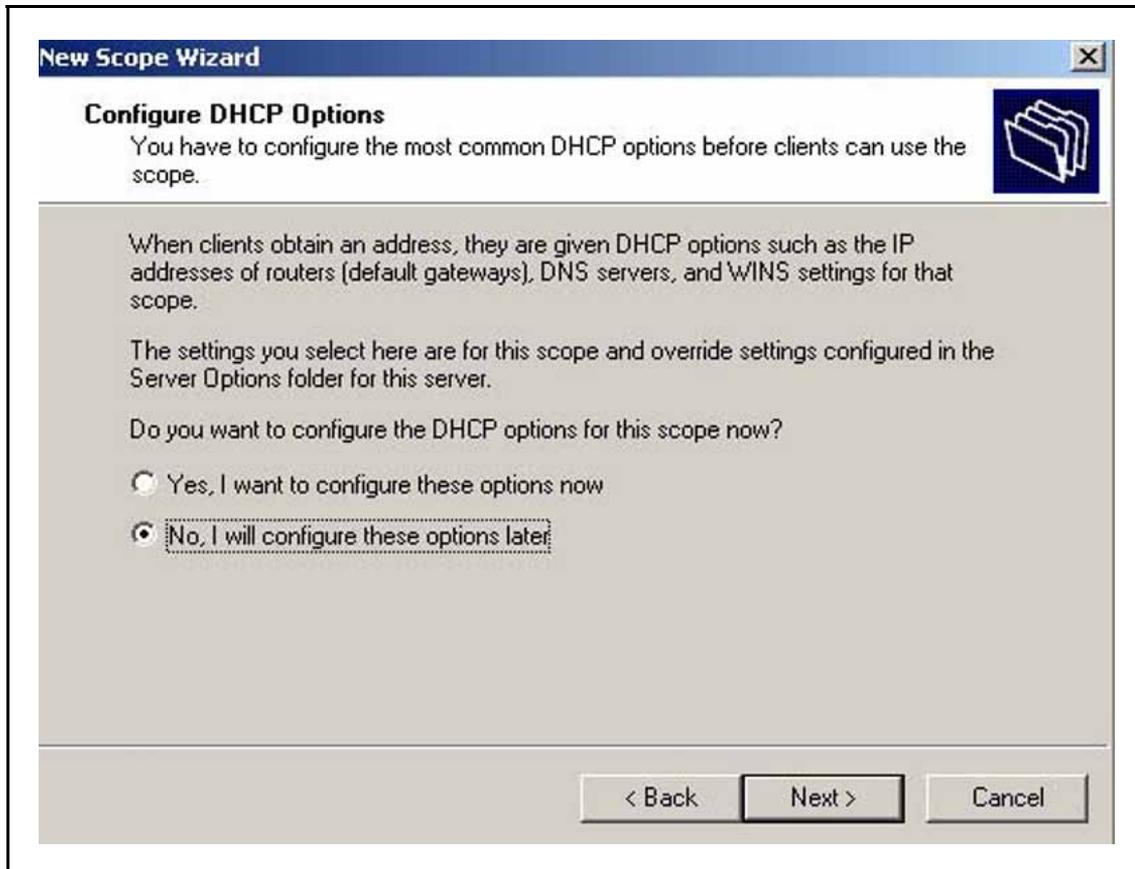
- 6 Define a range of IP addresses for the DAPs used, for example, 192.168.100.200- 210.
- 7 Define the associated subnet mask, for example 255.255.255.0.
- 8 Click **Next**.

The window **New Scope Wizard—Exclusion of an IP address range** appears.

- 9 Enter the Start IP address and End IP address values to exclude, for example the IP addresses of DHCP server and the TFTP server.
This is only necessary if the IP address or addresses of equipment with a fixed IP address is within the DHCP address range. If they are not within the DHCP address range, leave this field blank.
- 10 If you entered IP address ranges in the step above, click **Add** to save the exclusion list.
- 11 Click **Next**.
The **Lease Duration** window appears.



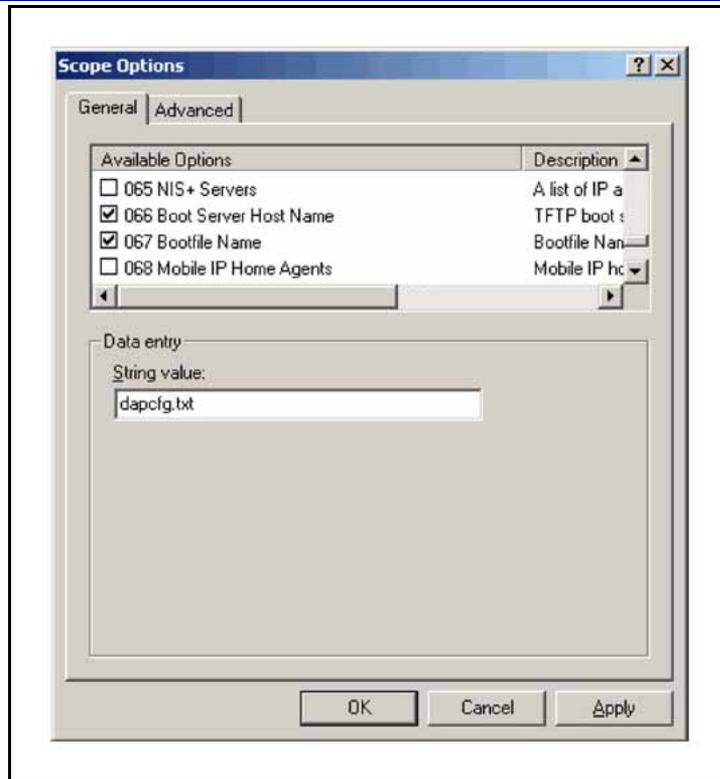
- 12 Set the desired lease duration of the granted IP addresses to the desired value.
- 13 Click **Next**.
The **New Scope Wizard—Configure DHCP options** appears.



- 14 Select **No** and click **Finish**.

The newly created scope appears. Under the newly created scope there is a sub line called Scope Options.

- 15 Right-click **Scope Options** and select **Configure Options**. The **Scope Options** page appears.

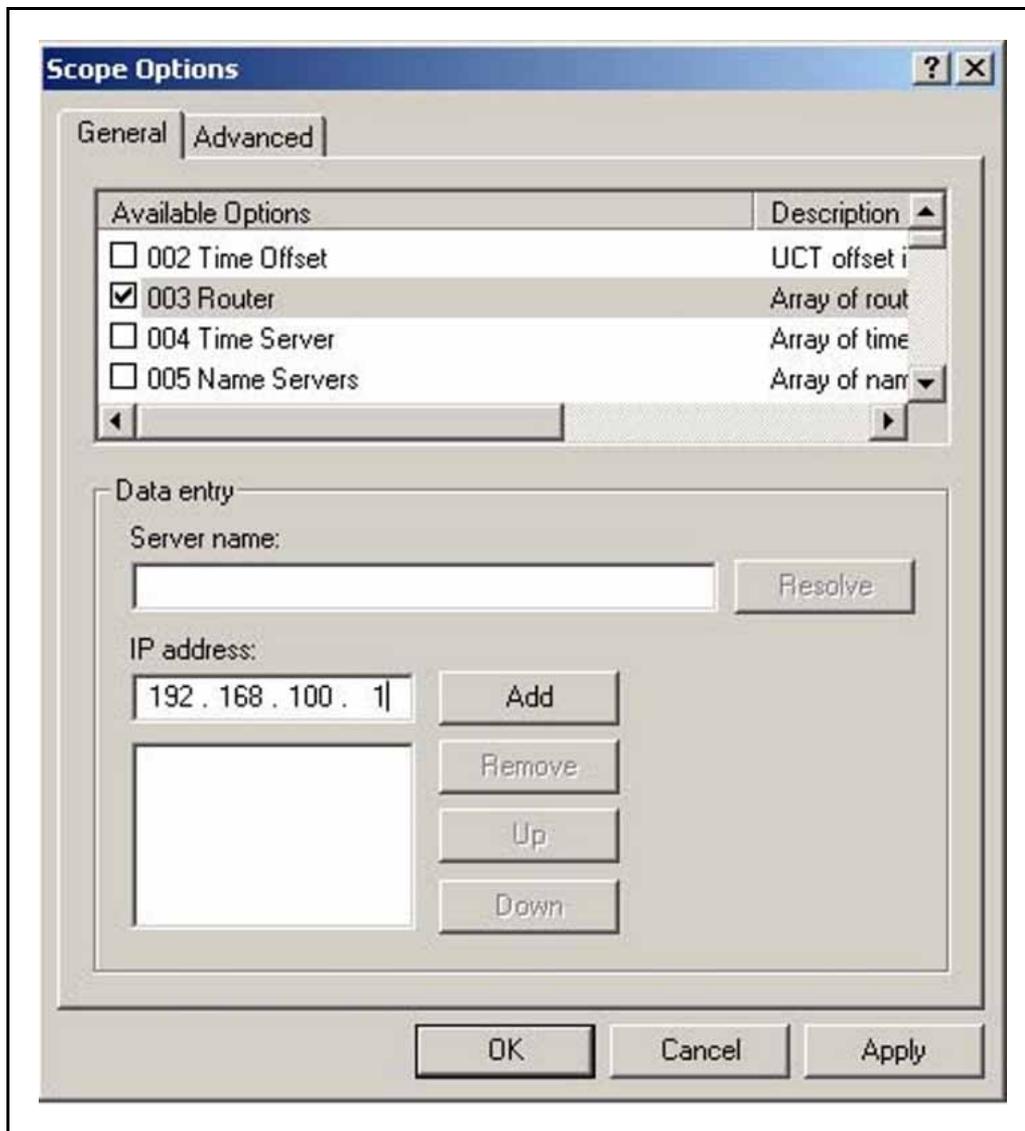


- 16 Select the check box Option 066 and enter the IP address of the TFTP server, for example 192.168.100.10.

This can be the IP address of your DAP controller or manager, if the TFTP server is running there. Do not click OK yet, but continue with the next step.

- 17 Check **Option 067** for the boot file name. Enter **dapcfg.txt**.

- 18 Select the check box **Option 3** and enter the Router or Default Gateway IP address, for example 192.168.100.1. Click **Add**.



- 19 Click **Apply** to save the changes and **OK** to leave the screen.
- 20 Right-click **Scope** and select **Activate**.
Now your DHCP server is configured correctly.
- 21 Close the DHCP window

--End--

TFTP server

There are many types of TFTP servers available, including shareware and freeware. A TFTP server must handle several accesses at the same time, because several accesses take place at the same time when the

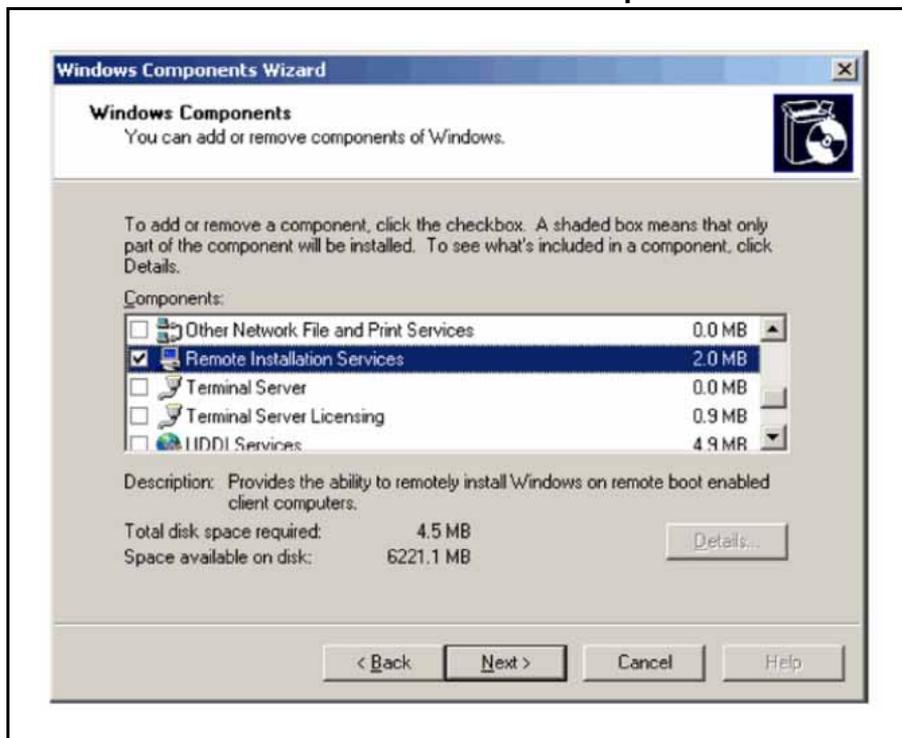
DAPs start up simultaneously. Only a few TFTP servers can handle more than one access at the same time. Some of these crash if the number of accesses is too high.

Follow the steps in the next procedure to install a TFTP server on the Windows 2000 Server and the Windows 2003.

Procedure 40 Installing the TFTP server

Step	Action
1	If you have Windows 2003, go to Start > Control Panel in Windows. If you have Windows 2000, go to Control Panel through Settings.
2	Open Add/Remove Programs .
3	Click on the Add/Remove Windows Components .

The **Windows Components Wizard** window appears.



- 4 In the Components window, select the check box beside Remote Installation Services.
- 5 Click **Next**.
- 6 Insert the Windows 2000 or Windows 2003 CD-ROM as prompted.
- 7 Finish the procedure following the instructions on the screen.

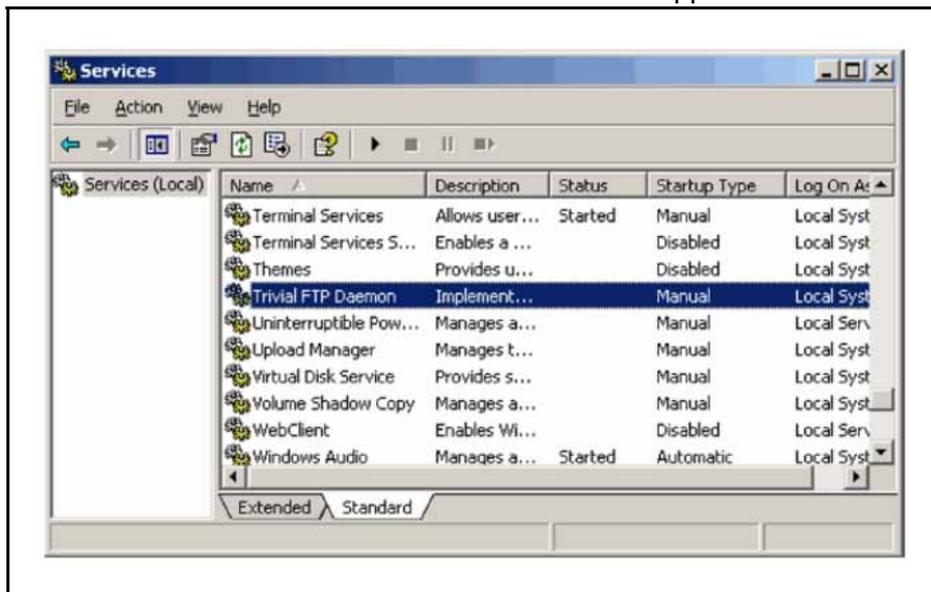
- 8 Close the Add/Remove Programs window and close the Control panel window.
- 9 Click **yes** after you are prompted to restart the computer.

--End--

Procedure 41 Starting the TFTP server

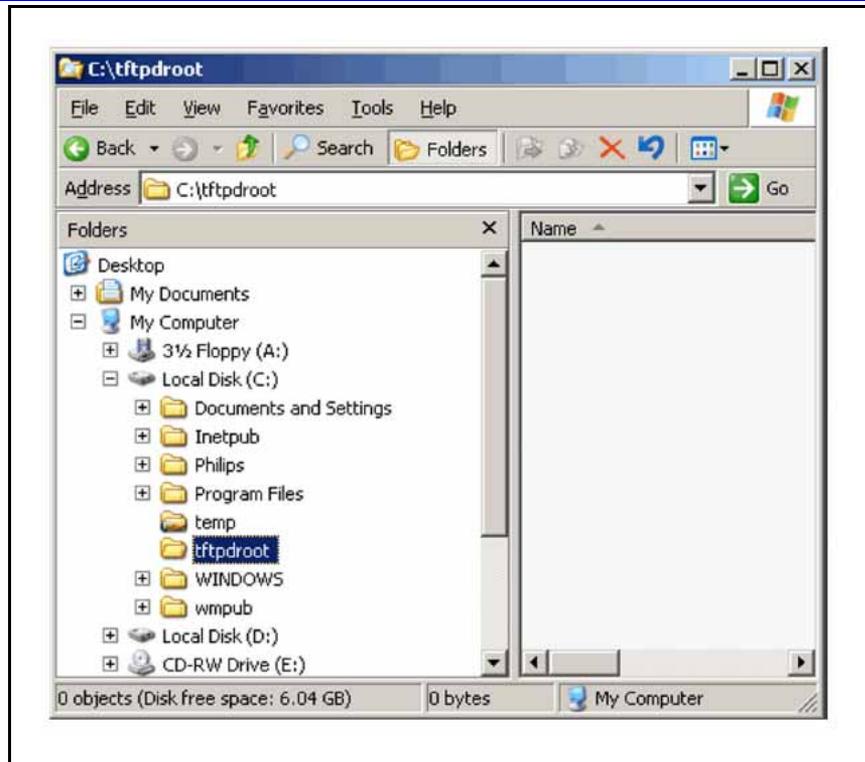
Step	Action
1	If you have Windows 2003, go to Start > Control Panel . If you have Windows 2000, go to Settings > Control Panel .
2	Open Administrative Tools .
3	Open Services .

The **Services** window appears.



- 4 Select Trivial FTP Daemon.
- 5 Right-click the **Trivial FTP Daemon** and then select Start.
- 6 Right-click the **Trivial FTP Daemon** and then select **Properties**.
- 7 Change the Startup Type setting to Automatic.
- 8 After TFTP is successfully installed on your PC with Windows 2000, a folder named tftpdroot is created.

Note: If you are running Windows 2003, a tftpdroot folder is not automatically created. You must create this folder yourself on drive C:, as shown in the following figure.



--End--

Built-in DHCP and TFTP servers

The DAP controller software Release 4 comes with a built-in DHCP and TFTP server. The built-in DHCP and TFTP servers do not require manual configuration, because the IP DECT Configurator sets up the configuration.

ATTENTION

You can configure a Built-in DHCP and TFTP server only after you install the IP DECT Configurator. See [“DAP Controller” \(page 130\)](#) for details.

Built-in DHCP server

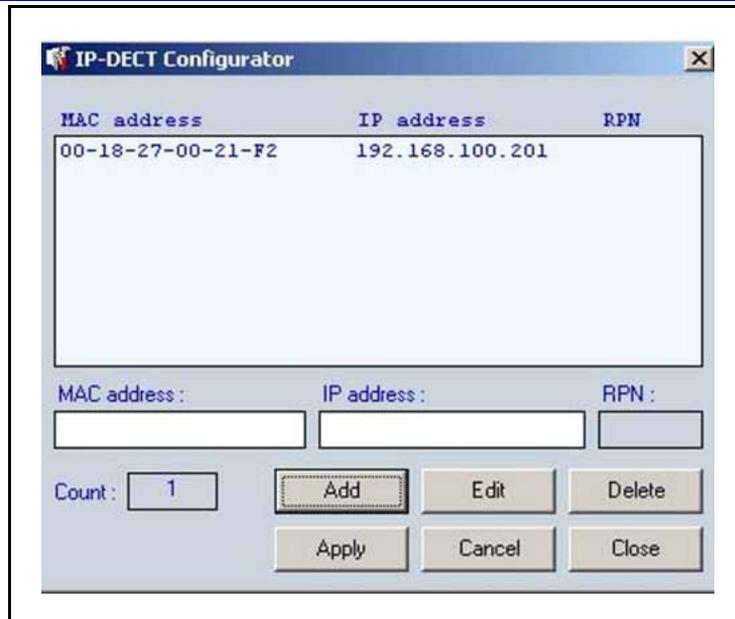
The DAP controller software Release 4 comes with a built-in DHCP server. This server runs as an application that requires you to log in to Microsoft Windows. You can use the IP DECT configurator tool available under DAP controller 4 to start or stop the DHCP server program.

Note: This DHCP server only responds to DHCP requests from DAPs because it checks on Vendor Class Identification D(ECT) AP 49 coming from a DAP.

You can configure built-in DHCP server using the Network Settings window of IP DECT Configurator.

Procedure 42
Configuring the built-in DHCP server using the IP DECT Configurator
Network Settings Window

Step	Action
1	Start the IP DECT Configurator and select Modify the system .
2	Choose the system to modify. Note: If you are configuring a new system, follow the steps in these procedures before setting up built-in DHCP server. <ul style="list-style-type: none">• Procedure 46 “Launching the IP DECT Configurator” (page 137)• Procedure 47 “Adding a new system using the IP DECT Configurator” (page 138)• Procedure 51 “Configuring SIP Settings” (page 141)
3	Select the check box next to Run DHCP server on this PC .
4	Enter the DAP IP range , for example, 192.168.100.200-210.
5	Select the DAP IP Range exclusive for DAPs only .
6	Enter the Subnet Mask , for example, 255.255.255.0.
7	Enter the Default gateway , for example, 192.168.100.1.
8	Enter the TFTP IP address on the PC where the DAP controller software is installed, for example, 192.168.100.10.
9	If it is necessary to assign manually IP addresses to the DAP, click More .
10	Enter MAC address of the DAP and the IP address assigned to the DAP. You can add DAPs to the list, delete DAPs from the list, or edit the addresses.
11	Click Apply to save the changes or Close to exit.



- 12 Click **Apply**.
- 13 Start the DHCP server with **Start > All Programs > DAP controller**.
- 14 Reboot the DAPs.

Note: If you are configuring a new system, follow the steps in [Procedure 51 “Configuring SIP Settings” \(page 141\)](#) instead of rebooting DAP

--End--

Built-in TFTP server

The DAP controller 4 comes with a built-in TFTP server that runs as a service under Microsoft Windows. You can use the IP DECT Configurator tool available under the DAP controller 4 to start or stop the TFTP server program. You can start or stop the service through the services window in Microsoft Windows.

Configuration without DHCP or TFTP

ATTENTION

DAP configuration without DHCP or TFTP requires DHCP and TFTP to be temporarily available to program or reprogram DAPs.

You can perform DAP configuration without DHCP or TFTP only after you have installed IP DECT Configurator. See [“DAP Controller” \(page 130\)](#) for details.

The DAPs can be installed in an IP environment without a DHCP server, a TFTP server, or both. Such an IP environment can be a VLAN within the company network where the IT manager does not allow a DHCP server. This IP environment can also be a branch office where a few DAPs are installed, without a DHCP server.

If a DAP must operate without a DHCP server, a TFTP server, or both, the DAP requires that the IP address and configuration data are stored in the DAP on a semipermanent basis, in FEPRM.

Storing the data on the DAP requires a DHCP server and a TFTP server once only. The DHCP and TFTP server can be on a stand alone PC with a network interface and a DAP connected. The DHCP and TFTP server can also be on any other computer in the network.

The DHCP server and TFTP server are required while you configure the DAP, but are not required during normal operation.

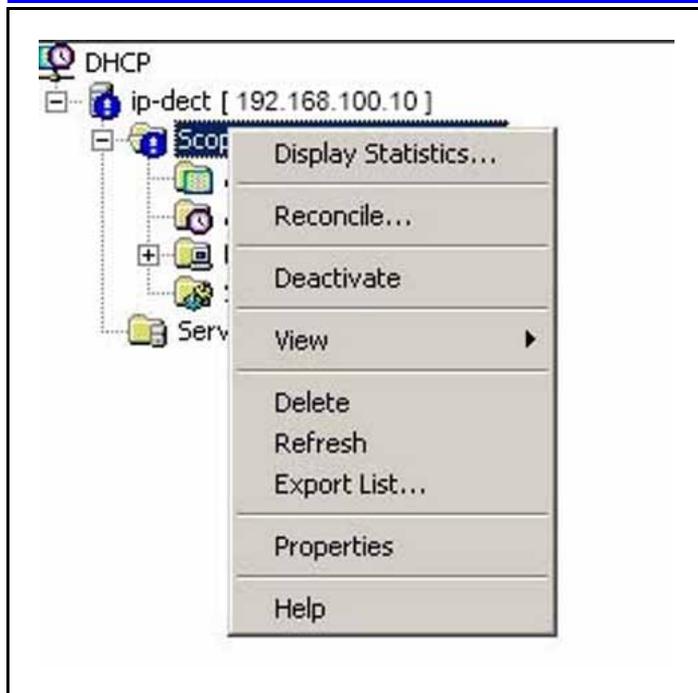
ATTENTION

To store the data in the DAP, it is necessary that the DAP get a DHCP offer with an Unlimited or Infinite lease. Ensure the DHCP server issues an Unlimited or Infinite lease. The DHCP server that comes with IP DECT Release 4 issues such a lease by default.

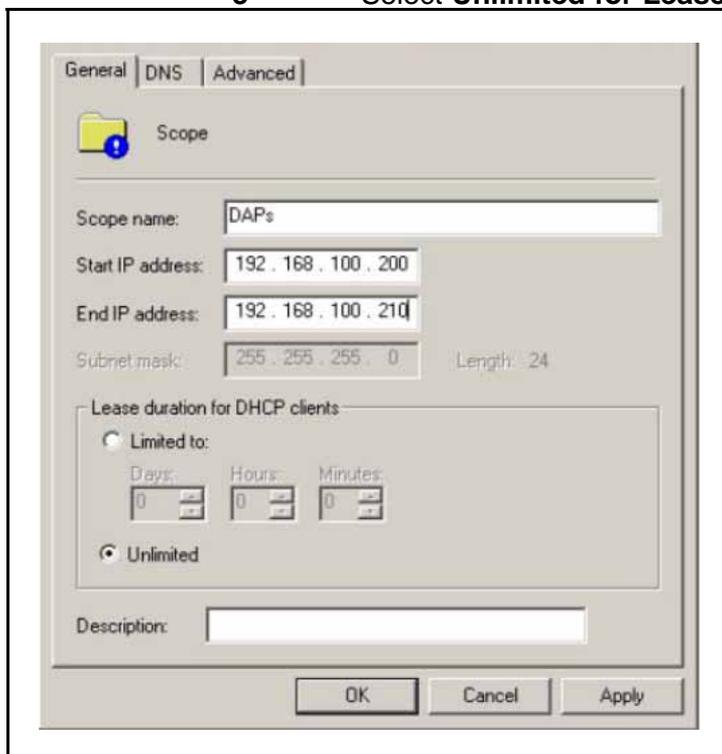
If an MS Windows DHCP server is configured, follow the steps in the next procedure to enable unlimited lease.

Procedure 43 **Enabling unlimited lease**

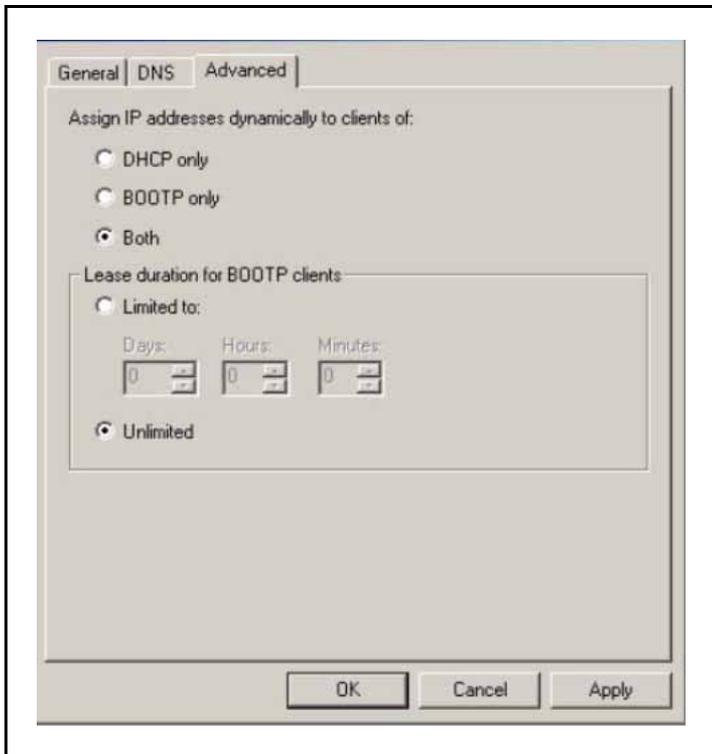
Step	Action
1	Start the DHCP manager: Start > Programs > Administrative Tools > DHCP .
2	Right-click Scope and select Properties . The DHCP Administrative tools page appears.



3 Select **Unlimited** for Lease duration for DHCP clients.



4 Click on the **Advanced Tab** and select **Both** for Assign IP addresses dynamically to clients of and **Unlimited** for Lease duration for OOTP clients.



5 Click **OK** to save changes.

--End--

DAP configuration without DHCP or TFTP servers You can set up DAP configuration without DHCP or TFTP servers using the Network Settings window of the IP DECT Configurator.

Use the following procedure to configure a DAP to store IP address and the configuration data.

Procedure 44
Storing IP address and configuration data on a DAP

Step	Action
1	Start the IP DECT Configurator and select Modify the system .
2	Choose the system to modify.
3	Click More .
4	Select the check box next to DAP Boot Options .
5	Select Store IP configuration into flash memory .
6	Click Apply .
7	Click the Save system button in the left section.

- 8 Ensure that the DHCP server is running and that the TFTP server is running.
- 9 Reboot the DAPs. The IP data and configuration data is now stored into the DAPs and the DAPs can function without the DHCP and TFTP servers.

--End--

DAP Controller

Use the information in this section to install the DAP Controller from the CD. You only need to execute this procedure once because the installation can be used for as many system configurations as you want. Changing settings can be always be done later.

Prerequisites

- Install and configure IIS software.
For more information, see [“Internet information services” \(page 105\)](#).
- Install and configure DHCP and TFTP servers if you are using MS Windows DHCP and TFTP servers. For more information, see [“DHCP and TFTP servers” \(page 111\)](#).
- Ensure that you have DAP controller or manager software, Release 4 or later.
- Ensure that you have DAP firmware 4910c4xx.dwl or later.
- Ensure that you have configured the IP addressing on the network adaptor.

Procedure 45 Installing the DAP Controller

Step	Action
1	<p>Insert the CD-ROM in the CD drive and run setup.exe.</p> <p>Depending on the directory structure on the CD-ROM, the setup.exe file is found in the directory Disk1. The InstallShield Wizard appears. This window remains visible during the installation of the DAP controller components and gives you information about the installation progress.</p> <p>If Microsoft .NET Framework 1.1 is already installed, the Welcome to the InstallShield Wizard for DAP controller window appears. Go to step 6.</p> <p>If the Microsoft .NET Framework 1.1 software is not yet installed, an Installshield dialog appears, with the following statement: DAP Controller optionally uses the Microsoft (R)</p>

.NET 1.1 Framework. Would you like to install it now?

2 Click **Yes** to install Microsoft .NET Framework 1.1 software. The **Microsoft .NET Framework 1.1 Setup: End User License Agreement** page appears.

3 Click **I agree** and then click **Install**.

After the Microsoft .NET Framework 1.1 is successfully installed, **Microsoft .NET Framework 1.1 Setup: Setup Complete** page appears.

Note: Wait while the installation completes; this can take several minutes. The DAP controller - InstallShield Wizard indicates activity with a progress bar.

A message appears when the installation is complete.

4 Click **OK**.

A message appears requesting that you restart the PC.

5 Click **OK** to restart the PC.

After the PC is restarted, it automatically continues with the DAP controller installation. The **DAP controller - InstallShield Wizard** page appears.

6 Click **Next**.

The **System Type** page appears.

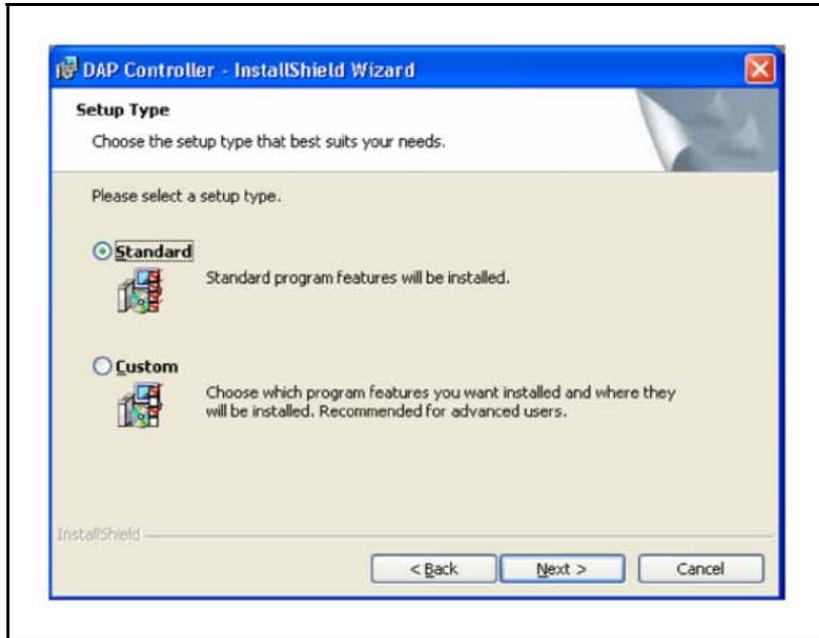
7 There are two types of DAP Controller installation. Select one of the following:

- Select **Single System** if you do not need to manage more than one SIP DECT system.
OR
- Select **Multiple Systems** if you plan to manage more than one SIP DECT system with your PC.

If you select Single System, the built-in DHCP server and TFTP server are not installed, by default. However, if you want to install them anyway, select the option Custom in step 8, and select DHCP server and TFTP server to install.

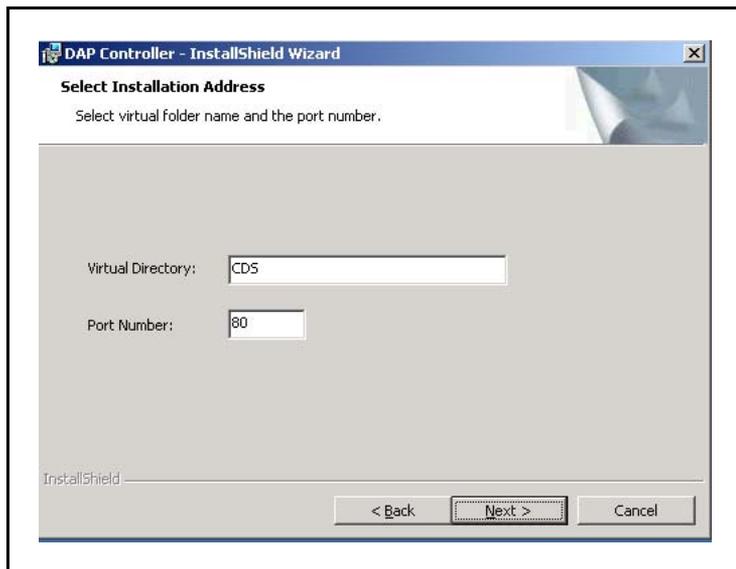
8 Click **Next**.

The **Setup Type** page appears.



9 Select **Standard** and click **Next**. If you want to customize the installation, select **Custom**.

10 Click **Next**.
The **Select Installation Address** page appears.



Do not change the default values in the fields CDS and Port Number. The system has collected enough information to install the software.

11 Click **Next**.
The **Ready to install the program** page appears.

12 Click **Install** to start the installation.
The system installs the software.

- 13 The **InstallShield Wizard Completed** page appears when the installation is complete.
- Click **Finish**.
- The DAP Configurator starts automatically so that you can configure your SIP DECT system.

--End--

System configuration

Navigation

This chapter contains information about the following topics.

- [“Simple SIP DECT configuration” \(page 135\)](#)
- [“Routed Head Quarter configuration” \(page 173\)](#)
- [“Multi site mobility network configuration” \(page 175\)](#)
- [“Central directory access tool” \(page 208\)](#)

Simple SIP DECT configuration

The SIP DECT system implies the configuration of three main components, the Call Server, the Signaling Server and the DAP controller or manager, which is required to create, monitor, or modify the configuration of DAPs.

Use the following tools to configure a SIP DECT system.

- Element manager or overlay program for Call Server
- Element manager and NRS manager for Signaling Server
- IP DECT Configurator and DAP manager IP DECT, which are available as a part of the DAP controller software package

In this document the following parameters are used to show an example of configuring a SIP DECT system.

- Call server IP address: 192.168.32.70
- Signaling server ELAN IP address: 192.168.32.41
- Signaling server Node IP address: 192.168.100.105
- Signaling server NRS IP address: 192.168.100.104
- DAP IP address: 192.168.100.200
- PC IP Address, where DAP controller is installed: 192.168.100.1
- Customer: 0

- D-Channel: 5
- Route: 6
- Access Code: 9
- Location code: 442
- SIP Route ACOD: 6
- SIP domain name: mera.ru
- Signaling Server hostname: SS_Node55_Ildr

Configuration of settings using IP DECT Configurator

The IP DECT Configurator is a tool for creating configuration files for the DAP controller and DAPs. The IP DECT Configurator is installed and launches automatically with the installation of the DAP controller software. The IP DECT Configurator can also be launched using the shortcut to the IP DECT Configurator tool found under the Start menu at Programs > DAP controller > DAP Applications.

For more information about IP DECT configurator installation, see [Procedure 45 “Installing the DAP Controller” \(page 130\)](#).

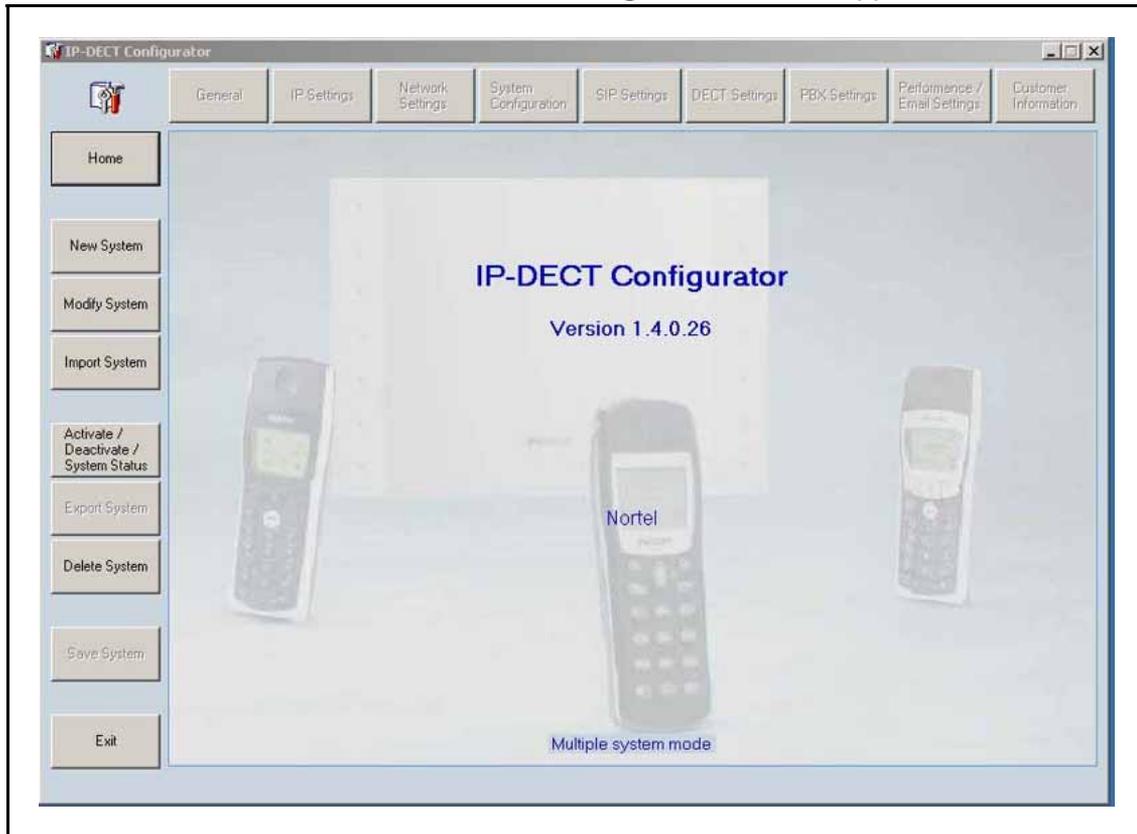
Use the steps in the following procedures to configure the settings in the IP DECT Configurator.

- [Procedure 46 “Launching the IP DECT Configurator” \(page 137\)](#)
- [Procedure 47 “Adding a new system using the IP DECT Configurator” \(page 138\)](#)
- [Procedure 48 “Configuring IP Settings” \(page 139\)](#)
- [Procedure 49 “Configuring Network Settings” \(page 140\)](#)
- [Procedure 51 “Configuring SIP Settings” \(page 141\)](#)
- [Procedure 52 “Configuring DECT Settings” \(page 143\)](#)
- [Procedure 53 “Configuring other settings—Performance/Email Settings” \(page 145\)](#)
- [Procedure 54 “Configuring other settings—Customer Information settings” \(page 148\)](#)
- [Procedure 55 “Saving the system” \(page 149\)](#)
- [Procedure 56 “Enabling or re-enabling the DAPs” \(page 150\)](#)

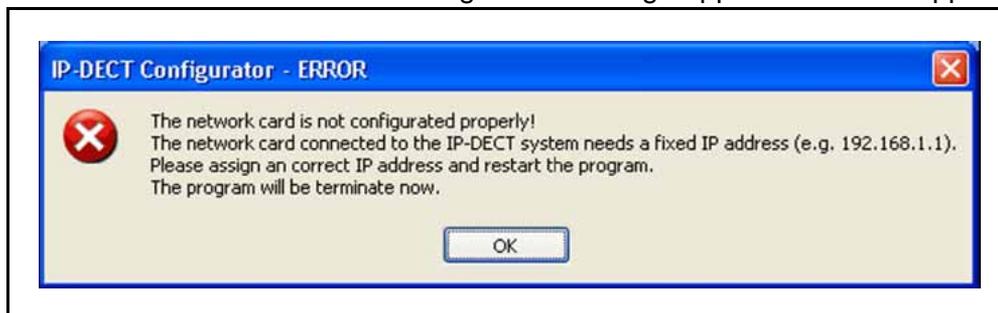
Procedure 46
Launching the IP DECT Configurator

Step	Action
1	Select Start > Programs > DAP controller > DAP Applications > DAP Configurator .

The **IP DECT Configurator** window appears.



If your network card does not have a fixed IP address, the following error message appears after the application launches.



To correct this error, assign a fixed IP Address to the network card in your DAP controller PC and launch the application again.

The IP DECT Configurator main window shown in [Figure 1 "SIP DECT configuration"](#) (page 11) has three sections.

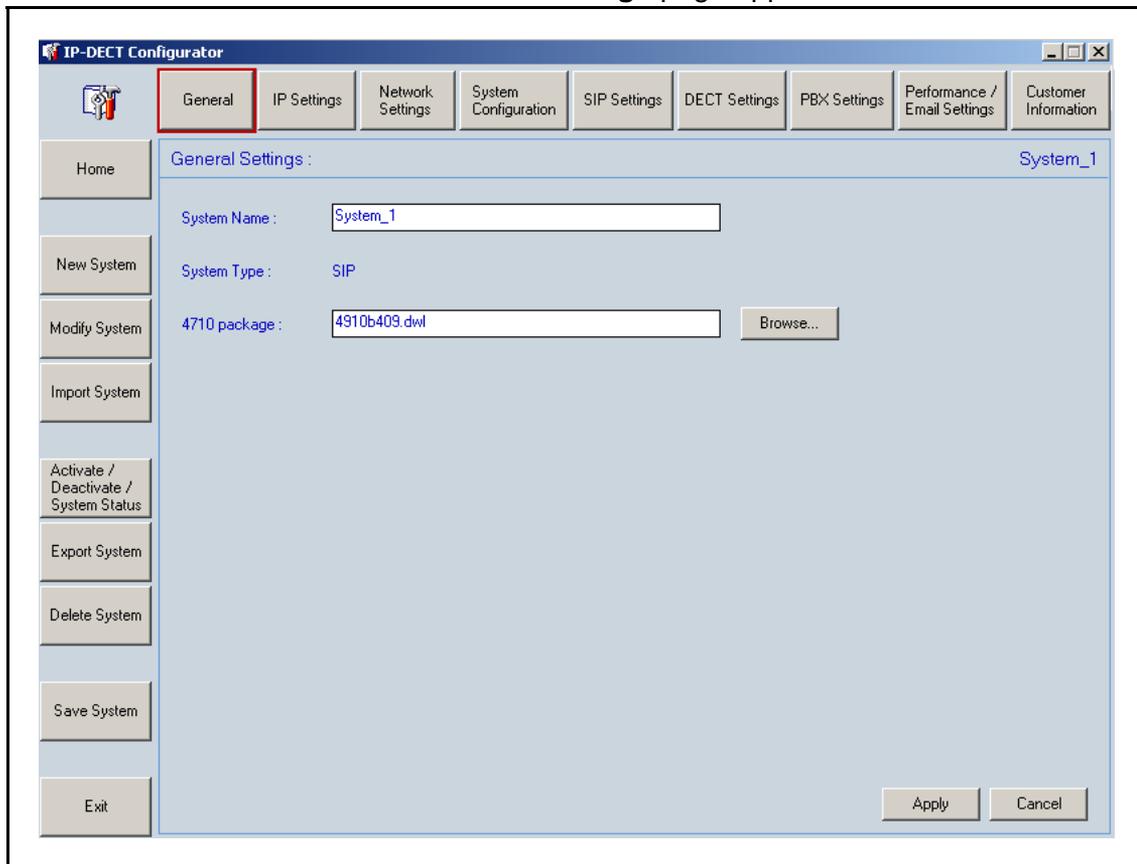
1. The top section shows the Settings buttons.
2. The left section shows the System Control buttons.
3. The middle section shows the data information.

--End--

Procedure 47
Adding a new system using the IP DECT Configurator

Step	Action
1	In the IP DECT Configurator main window, click the New System button in the System Control settings on the left of the window.

The **General settings** page appears.



- 2 Enter the System name, for example, System_1.

Note: Do not enter any special characters in the name of your SIP DECT system that cannot be used in the name of the folder you create for the SIP DECT system. The folder and the SIP DECT system share the same name.

- 3 In the **General Settings** window, enter the path to the firmware, the DAP package file, for example, C:\tftpdroot\4910b420.dwl.
- 4 Click **Apply**.

--End--

Procedure 48 Configuring IP Settings

Step	Action
------	--------

- 1 In the Settings section, click the **IP Settings** button.

The **IP Settings** page appears.

The screenshot shows the 'IP-DECT Configurator' window with the 'IP Settings' tab selected. The configuration fields are as follows:

Configuration Section	Field	Value	Additional Info
DAP IP configuration	Multicast address	239.192.49.49	Port range from: 3000 to 22229, Default MCA
	DC IP address	192.168.100.1	Port range from: 28000 to 28017, This PC IP
Proxy IP configuration	Proxy IP address	192.168.100.105	Proxy Port: 5060

- 2 In the **Multicast address** field, enter **239.192.49.49**.

- 3 Enter the **DAP controller Configuration: DC IP address**, which is the PC IP address where your DAP controller is installed. An example of this address is 192.168.100.10.

ATTENTION

The DAP Controller PC must have a static IP address and be in the same subnet as the DAPs. If the DAP Controller PC is in a different subnet, you must configure the Routed Head Quarter. See [“Routed Head Quarter configuration”](#) (page 173).

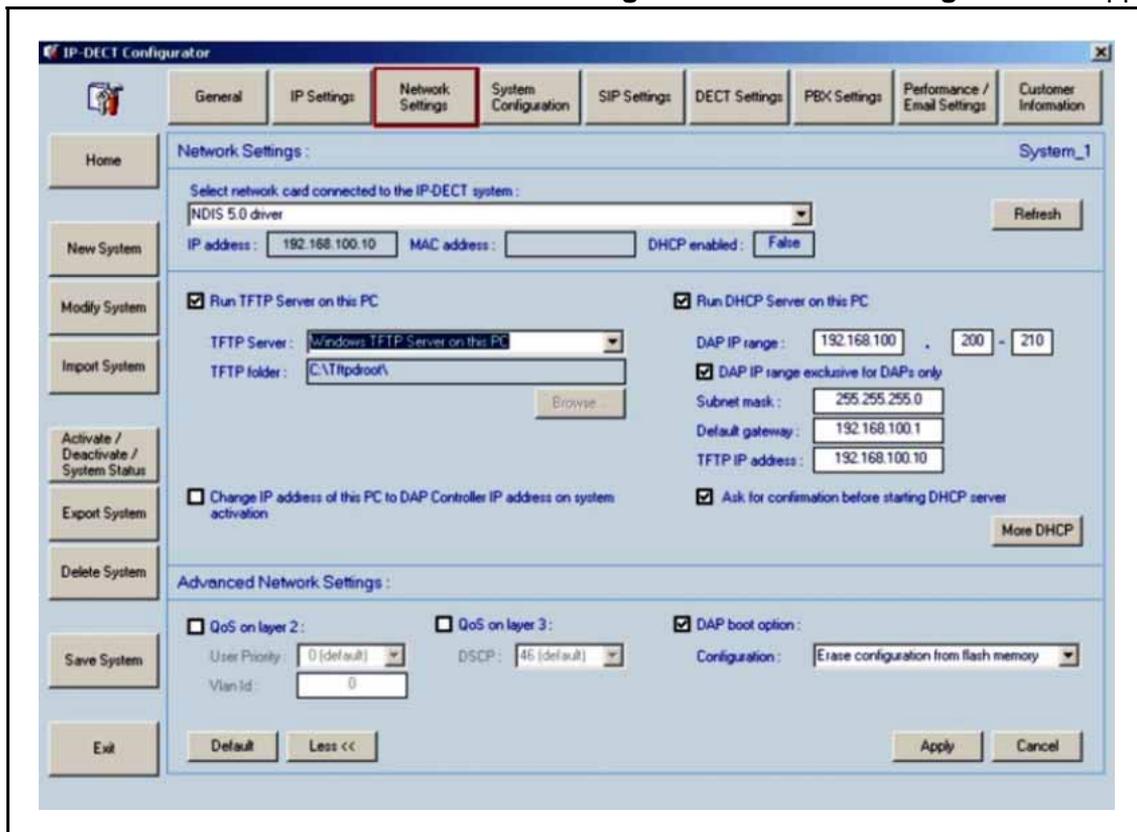
- 4 Enter the **Proxy IP address**, which is the Signaling Server Node IP, for example, 192.168.100.105.
- 5 Click **Apply**.

--End--

**Procedure 49
Configuring Network Settings**

Step	Action
------	--------

- | | |
|---|--|
| 1 | In the Settings section, click the Network Settings button.
The IP DECT Configurator Network Settings window appears. |
|---|--|



- 2 Select the network card connected to the SIP DECT system.
- 3 Select the check box next to **Run TFTP server on this PC** and select the following.
 - **Windows TFTP server on this PC** if you use an MS Windows TFTP server.
OR
 - **3com TFTP server on this PC** if you use a built-in TFTP server.
- 4 Configure the DHCP server.
 - If you use an MS Windows DHCP server, click **Apply**.
OR
 - If you use a built-in DHCP server, see [“Built-in DHCP server” \(page 124\)](#).

ATTENTION

If you plan to create a configuration without DHCP and TFTP servers, see [“Configuration without DHCP or TFTP” \(page 126\)](#).

--End--

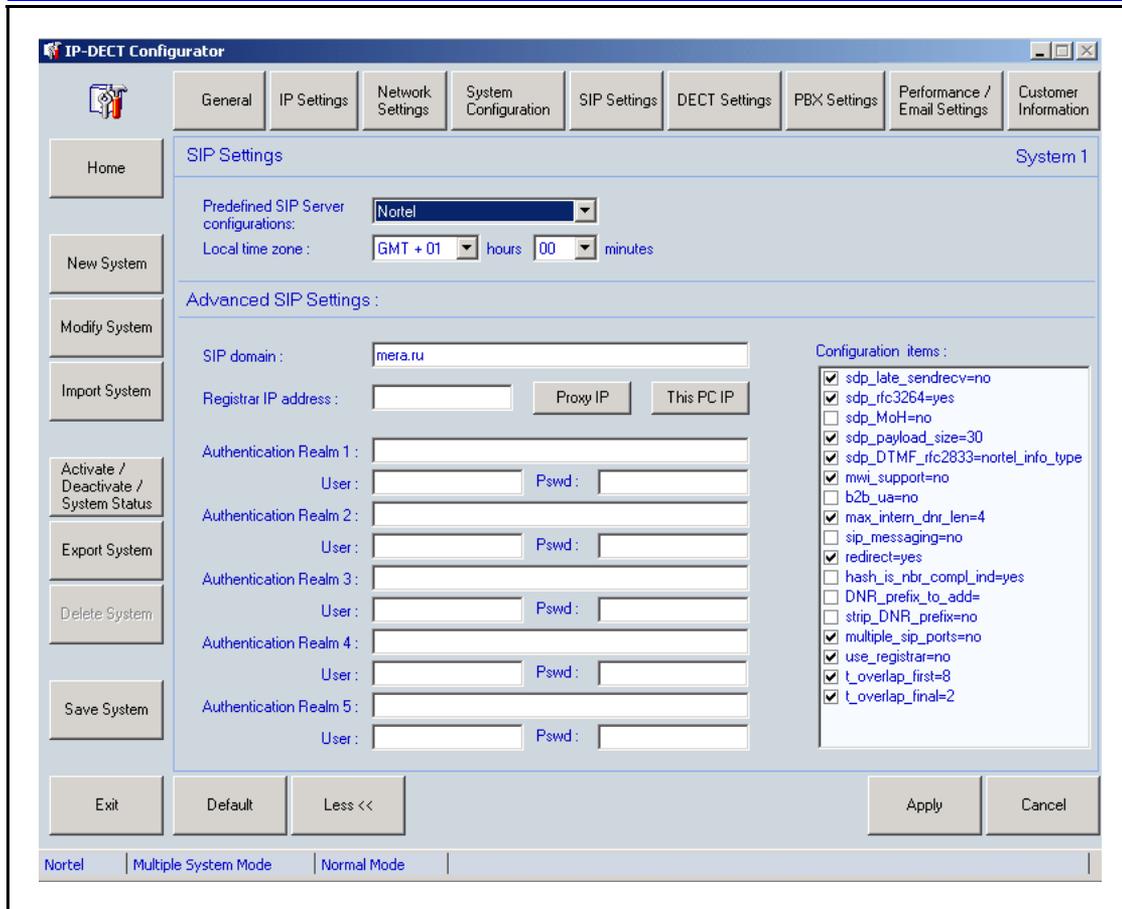
Procedure 50
Configuring System Configuration Settings

Step	Action
1	In the Settings section, click System Configuration .
2	Select Simple configuration for System configuration and click Apply . If you need to configure Routed Head Quarter, see “Routed Head Quarter configuration” (page 173) .

--End--

Procedure 51
Configuring SIP Settings

Step	Action
1	In the Settings section, click the SIP Settings button. The SIP Settings window appears.



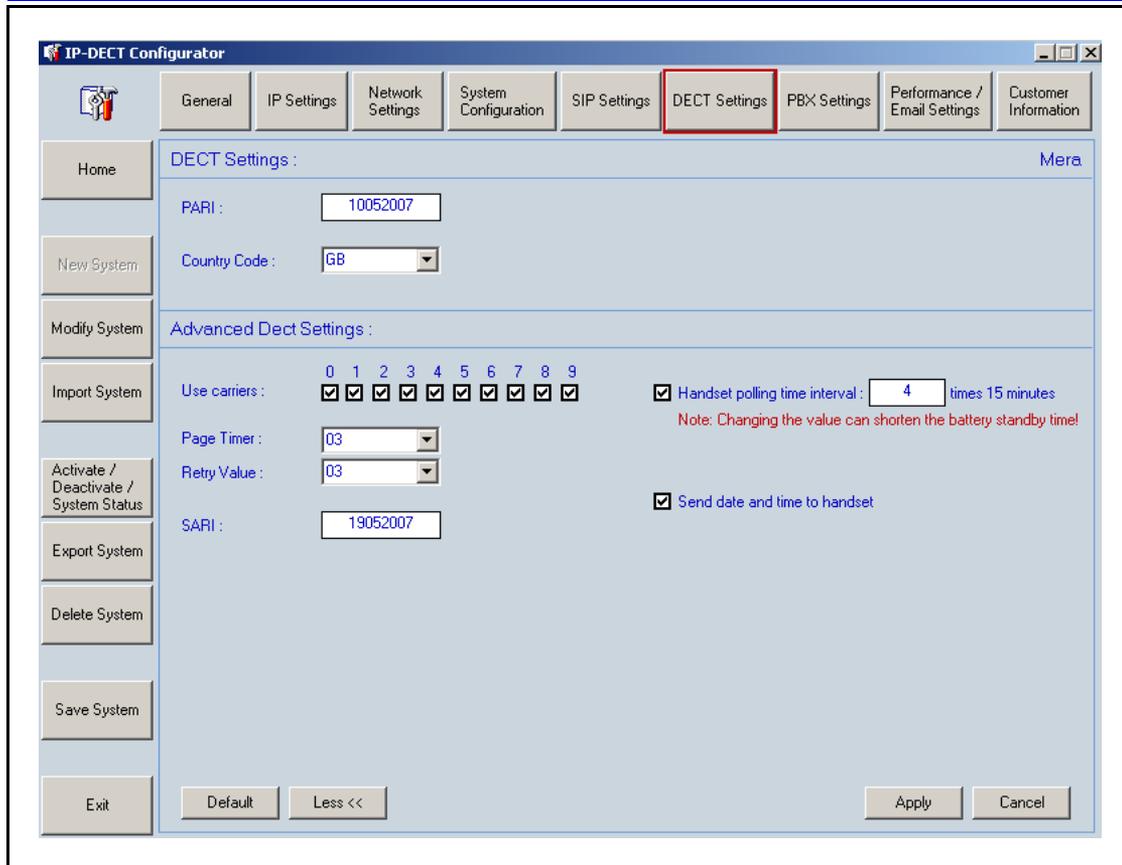
- 2 Select **Nortel** for **Predefined SIP Server configurations**.
- 3 In the Advanced SIP Settings window, enter the domain name.
- 4 Select the check box for **sdp_late_sendrecv** and select **no**.
- 5 Select the check box for **sdp_payload_size** and select **20** or **30** as required. You must configure the same payload value for the G711 codec in Signaling Server.
- 6 Select the check box for **sdp_DTMF_rfc2833** and select **nortel_info_type**.
- 7 Select the check box for **max_intern_dnr_len** and select the maximum number of digits in the internal DNs.
DNs that contain more digits than configured for this parameter are defined as external. Depending on DECT handset capabilities, different ringing melodies can be used for internal and external calls.
- 8 Select the check box for **mwi_support** and select **yes**.
- 9 Select the check box for **use_registrar** and select **no**.
- 10 Select the check box for **multiple_SIP_ports** and select **no**.
- 11 Select the check box for **redirect** and select **yes**.

- 12** Optionally, select the check box for **t_overlap_first** and enter the value (in seconds) to define how long the DAP waits for the user to dial the first digit.
- If no new digit is dialed within the specified period of time, the DECT handset goes on-hook automatically.
- 13** Optionally, select the check box for **t_overlap_final** and enter the value (in seconds) to define how long the DAP waits for the user to dial the next digit of the number (when the user has already dialed in at least one digit).
- If no new digits are dialed within the specified period of time, the dialed number is called.
- Note:** This setting is applied to the predial mode as well
- 14** Click **Apply**.

--End--

Procedure 52
Configuring DECT Settings

Step	Action
1	In the Settings section, click the DECT Settings button. The DECT Settings window appears.



- 2 Enter an 8 digit hexadecimal string for the Primary Access Right Identity or **PARI**, for example, 10052007.

Note: The worldwide unique PARI for your DECT system must be issued by the European Telecommunications Standards Institute (ETSI). For more information, see www.etsi.org.

ATTENTION

Ensure you enter the correct PARI. You need to reinstall the DAP Controller software and re-subscribe all DECT handsets if you change the PARI.

- 3 Click **More** and enter an 8 digit hexadecimal string for the Secondary Access Right Identity or **SARI** for example, 19052007.

Note: SARI is necessary only in Multi Site Mobility Network configuration.

- 4 Optionally, you can turn off or on some of the 10 carriers available to the DAPs in the system.

If there are independent DECT systems that have overlapping areas of coverage and the rate of calls in them is high, Nortel recommends that you consider allocating a unique subset of

carriers for each system. When you allocate a unique subset of carriers for each system, you avoid unnecessary collisions between them.

For example, if there are two independent DECT systems, you can turn off carriers 0-4 in one system and turn off carriers 5-9 in the other system. Turning off carriers reduces the maximum number of simultaneous calls. For this reason, you can be required to install extra DAPs to achieve the desired call capacity of the DECT system.

ATTENTION

If there are two or more independent Nortel SIP DECT systems with overlapping areas of coverage, it is always preferable that you configure these systems so that each system has a unique subset of carriers.

Note that reducing the number of available carriers reduces the maximum number of simultaneous calls in the DECT system. For this reason, you can be required to install extra DAPs to achieve the desired call capacity.

5 Click **Apply**.

--End--

Procedure 53
Configuring other settings—Performance/Email Settings

Step	Action
1	Click the Performance/Email Settings button located to the right of the PBX Settings button. The Performance/Email Settings window appears.

IP-DECT Configurator

General IP Settings Network Settings System Configuration SIP Settings DECT Settings PBX Settings **Performance / Email Settings** Customer Information

Home Performance Settings : System_1

NOTE: PCR Service must be running for performance retrieval and automatic e-mail generation!

Performance Counters Configuration :

Interval UPM generation every : 1440 minutes

Interval EPM generation every : 15 minutes

Start measurement at : 7:00:00 AM

Stop measurement at : 7:00:00 PM

Create performance counters every :

Sun Mon Tue Wed Thu Fri Sat

Keep performance data for : 14 days

HTTP execution time out : 90

Use client resolution

Advanced Email Settings :

SMTP Server : gmail.merann.ru

Email from : dect.manager@your_domain.com

Send alarm emails

Email address(es) : kalexand@mera.ru

Email nightly created archive

Email address(es) : kalexand@mera.ru

Channel occupation : Threshold : 1 % Time : 5 Sec

G729 occupation : Threshold : 80 % Time : 60 Sec

Alarm reaction time : 1 Hours

Send archive every :

Sun Mon Tue Wed Thu Fri Sat

Stop sending archive after : 1 /24/2008

Max. attachment size : 5 Mb

Default Less << Apply Cancel

In this window, you can configure the following:

- Performance Settings
 - Performance Counters Configuration
 - Interval UPM generation every _____ minutes
 - Interval EPM generation every _____ minutes
 - Start measurement at
 - Stop measurement at
 - Create performance counters every _____
 - Keep performance data for _____ days.
- Advanced Email Settings
 - SMTP Server
 - Send alarm emails
 - Email addresses
 - Email from
 - Channel Occupation
 - G729 occupation (not applicable to Nortel SIP DECT)

- Threshold/Time
- Alarm reaction time

- 2 In **Performance Settings**, under **Performance Counters Configuration** fill the field in **Interval UPM generation every _____ minutes** or accept the default of 1440 minutes, which equals one day.
This interval specifies how often User Performance Measurement files are generated.
- 3 Fill in the field in **Interval EPM generation every _____ minutes** or accept the default of 15 minutes.
This interval specifies how often Equipment Performance Measurement files are generated.
- 4 Fill in the field next to **Start measurement at:** with the time you want performance measurement to start each day.
- 5 Fill in the field next to **Stop measurement at:** with the time you want performance measurement to stop each day.
- 6 Under **Create performance counters every**, select the check boxes under the days of the week you want performance counter retrieval to take place.
- 7 In the field **Keep Performance data for _____ days** fill in the number of days you want the performance data stored on the hard disk.
- 8 Click **More >>** to access **Advanced Email Settings**.
- 9 In **Advanced Email Settings**, fill in the field next to **SMTP Server** with the DNS name or the IP address of your SMTP mail server.

Note: With **Advanced Email Settings**, emails can be sent automatically if a DAP fails or if the channel occupation threshold is exceeded for more than a specified number of seconds. Automatic emails can be sent only if the DAP controller or manager is running, and the PCR service is running on the DAP controller or manager PC.

If you enter the DNS name of your SMTP Server, ensure that the DNS server address is configured for the network connection on the DAP Controller.

- 10 Select the **Send alarm emails** check box, which enables SIP DECT to send emails to the SMTP Server.
- 11 Fill the field next to **Email addresses:** with one or more destination email addresses.

- 12 Fill in the field next to **Email from:** with the email address of the originator.

Note: Normally, the SMTP server does not verify the email address of the originator. This means you can enter any email address in this field.
- 13 Fill in the two boxes after **Channel Occupation**. In the Threshold box, specify the percentage. In the Time box, specify a time in seconds.

Channel Occupation defines the conditions for generating an email on DAP channel occupation. If the channel occupation is higher than the 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 seconds.

G729 Occupation does not apply to Nortel SIP DECT.
- 14 Fill in the box next to **Alarm reaction time** with an amount of time in hours as an interval for sending emails.
- 15 Select the **Email nightly created archive** check box , which lets you automatically receive archives for each email.
- 16 Fill in the field next to **Email addresses** with one or more destination email addresses.
- 17 Select the days to receive archives, the date to stop sending archives, and the maximum size of the attached archive.
- 18 Click **Apply**.

--End--

Procedure 54
Configuring other settings—Customer Information settings

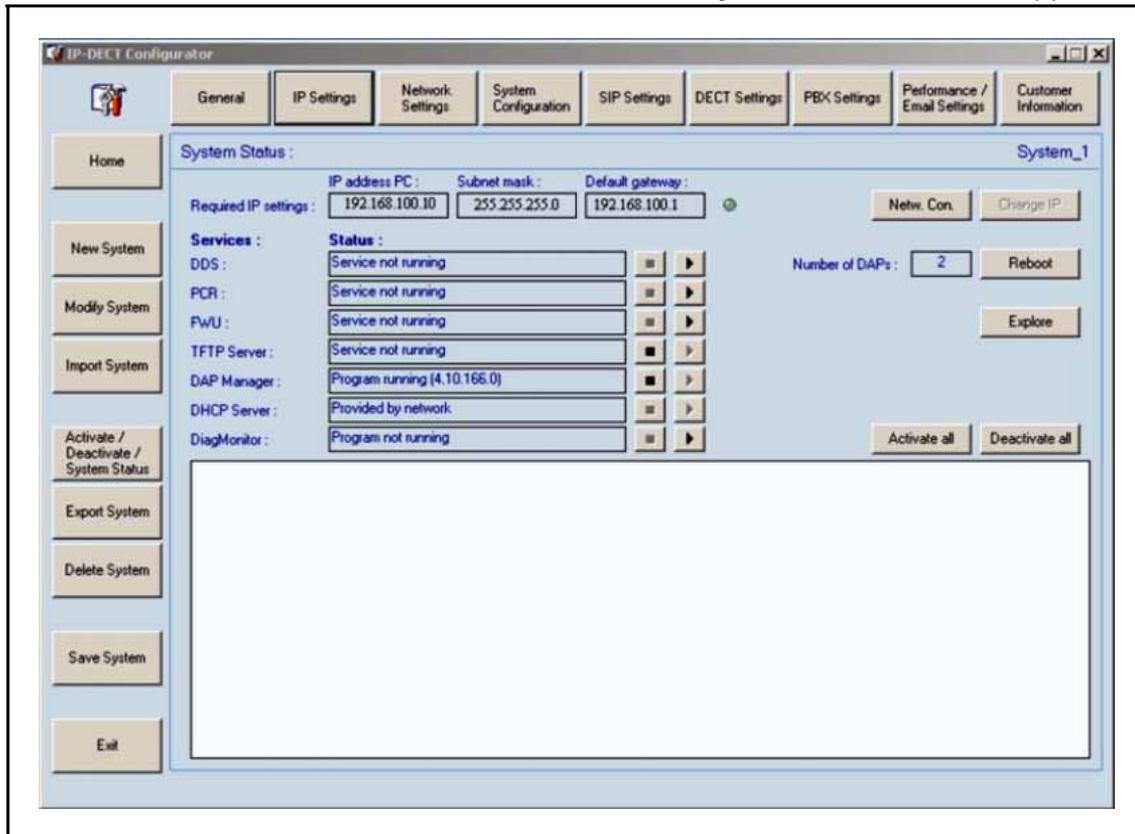
Step	Action
1	Click the Customer Information button located to the right of the Performance/Email Settings button. The Customer Information window appears.
2	In the Customer Information window, enter customer information. This window is for administrative purposes only. The system does not use this information

--End--

Procedure 55 Saving the system

Step	Action
1	To save the new system you created with the IP DECT Configurator, click Apply and then select Save system from the menu on the left.
2	In the System Control section in the left of the IP DECT Configurator main window, click the Activate/Deactivate/System Status button

The **Activate/Deactivate/System Status** window appears.



3 Click the **Activate all** button.

--End--

Procedure 56
Enabling or re-enabling the DAPs

Step	Action
1	To enable or re-enable the DAPs, power on the DAPs.
--End--	

DAP manager configuration

The following procedures are described in this section.

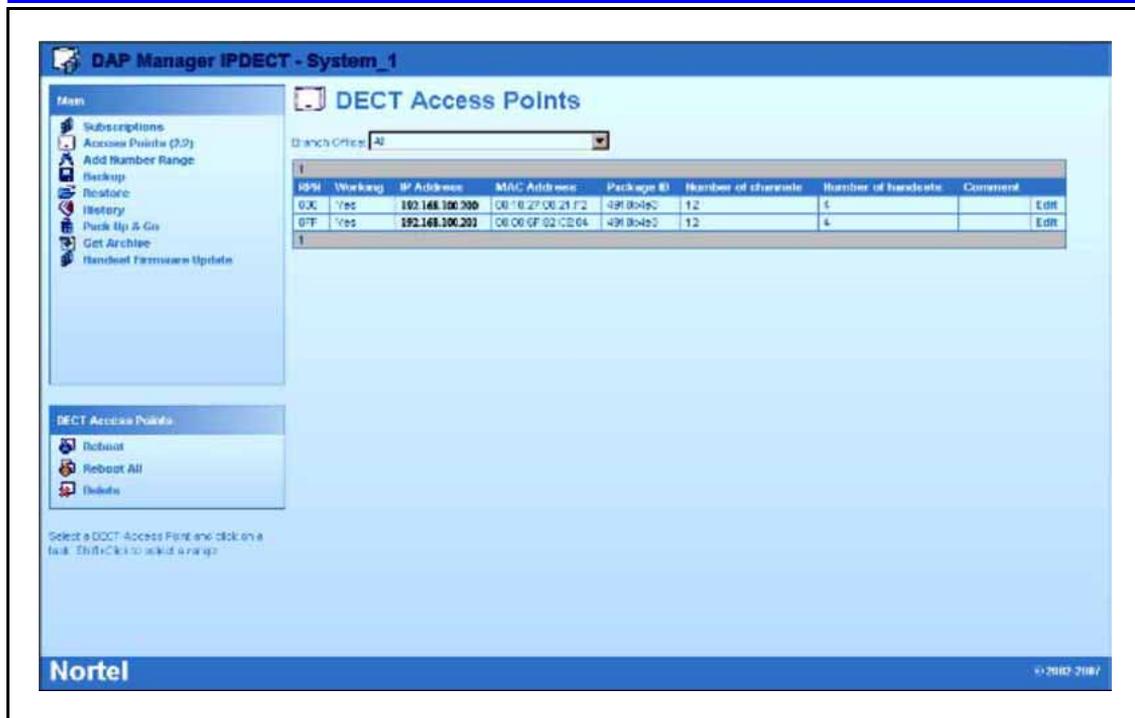
- [“Rebooting DECT Access Points” \(page 150\)](#)
- [“Adding number range” \(page 151\)](#)
- [“Subscribing a DECT handset” \(page 152\)](#)

Rebooting DECT Access Points

DECT Access Points need to be rebooted following software upgrades. To reboot a DECT Access Point, complete the following procedure.

Procedure 57
Rebooting DECT Access Points

Step	Action
1	Launch DAP manager by entering the following URL into an internet browser: localhost/cds The DAP manager IP DECT page appears.
2	Select Access Points from the menu list on the left. The Access Points page appears information about the DAPs.



DECT Access Points are identified by their Radio Part Number (RPN). In the work space, the DECT manager shows the status of the present DAPs. The RPN of a DAP is modified by editing the RPN field.

In the DAP manager task area, choose one of the following options.

- Reboot—Select this option to reboot a selected DAP.
- Reboot All—Select this option to reboot all DAPs in the list.
- Delete—Select this option to remove a DAP from the list.

The DAP takes a few minutes to reboot.

- 3 Confirm the DAP is active by checking the status of the device under the **Working** column. Active DAPs have **Yes** in this column.

--End--

Adding number range

To add a Number Range, complete the following procedure.

Procedure 58
Adding Number Range

Step	Action
1	Select Add Number Range from the menu list on the left.
2	Define DNs for the DECT handsets.

ATTENTION
The length of all DNs subscribed on DAPs must be the same.

--End--

Subscribing a DECT handset

Before you can use a handset (also known as portable telephone, portable part or PP), subscribe each handset to the system, and ensure that each handset is registered by the DECT manager.

ATTENTION
If you plan to create a multi site configuration, see [“Subscribe a multi site DECT handset” \(page 176\)](#), before you complete this procedure.

Procedure 59
Subscribing a DECT handset

Step	Action
1	Select Subscriptions from the menu list on the left. The Subscriptions page appears.

DAP Manager IPDECT - System_1

Subscriptions

Use DNR Filter

Number	Status	PIN	RPH	Presence	Registration status	Handset type	SW version	Comment	Edit
3000	Subscribed	OFF		Present	Registered	4060	51.20.53		Edit
5001	Subscribed	000		Present	Registered	4070	1.40		Edit
5002	Subscribed	000		Present	Registered	4070	1.40		Edit
5003	Subscribed	OFF		Present	Registered	4027	1.40		Edit
5004	Subscribed	OFF		Present	Registered	4027	1.40		Edit
5005	Subscribed	000		Present	Registered	4065R	72.24.14		Edit
5006	Subscribed	000		Present	Registered	4065R	89.24.30.31		Edit
5011	Subscribed	OFF		Absent	Registered	4025			Edit

Select a Subscription and click on a task.
Shift+Click to select a range.

Park : 31100051000347

Nortel © 2002-2007

- 2 Select the required available extension number or numbers.
If the required number is not visible, select another page. The page number is displayed in the top and bottom rows of the subscriptions table.
- 3 Click **Enable**.
The status of the configuring subscription record changes from "Free" to "Enabled" and the PIN is shown. A Personal Identification Number (PIN) is generated by the DECT manager on each subscribe operation and only displayed while the subscription status is enabled.
It is also possible to disable and terminate subscriptions. For more information about subscription management see the section "[Subscription management](#)" (page 187).
A DECT handset is required for the remainder of this procedure.
- 4 Find **System configuration** in the DECT handset menu.
- 5 Choose **New** and enter the displayed PIN code.

Sometimes it is necessary to enter PARK code first. The PARK code is displayed on the left at the bottom of the Subscriptions page.

Note: If the PIN is not entered within 16 minutes, the subscription mode is terminated for that specific extension number and the subscription process must be started from the beginning.

- 6 Enter the name and DN of the SIP-DECT system.

The DN is displayed on the handset screen. The status of the configuring subscription record changes from "Enabled" to "Subscribed".

Note: For more information, see ["Subscription management" \(page 187\)](#).

--End--

Configuration on Element manager

To log on to Element manager, open a browser and enter as an HTTP address the ELAN or TLAN address of the Signaling Server. If you are logging in for the first time, the call server IP address field is empty. Enter the ELAN address of the Call Server.

This section describes the following procedures.

- [Procedure 60 "Creating a new customer or modifying information about an existing customer" \(page 155\)](#)
- [Procedure 61 "Configuring the Zone" \(page 155\)](#)
- [Procedure 62 "Adding a D-Channel" \(page 156\)](#)
- [Procedure 63 "Adding a route" \(page 156\)](#)
- [Procedure 64 "Adding a trunk" \(page 157\)](#)
- [Procedure 65 "Configuring network access" \(page 158\)](#)
- [Procedure 66 "Creating ESN Control Block" \(page 159\)](#)
- [Procedure 67 "Adding digit manipulation block" \(page 159\)](#)
- [Procedure 68 "Adding route list block" \(page 159\)](#)
- [Procedure 69 "Adding location code \(for UDP\)" \(page 160\)](#)
- [Procedure 70 "Adding Trunk Steering Code \(CDP\)" \(page 160\)](#)
- [Procedure 71 "Configuring the signaling server" \(page 161\)](#)
- [Procedure 72 "Configuring SIP properties" \(page 162\)](#)

Creating a new customer

Use Element manager and follow the steps in the next procedure to create a new customer or modify information about an existing customer.

Procedure 60

Creating a new customer or modifying information about an existing customer

Step	Action
1	Select Customers from the menu list on the left.
2	Click the Add button on Customers list page. The New Customer X Property Configuration page appears.
3	Fill in customer number , for example 0.
4	Fill in a 3-digit number, for example 000 for ANAT. Fill in a 4-digit number, for example 0000 for ANLD.
5	Click Save .
6	On the Edit screen, select Feature Package and then select package 145 .
7	Select the ISDN check box and enter a number, for example 1, for PNI .
8	Click submit .
--End--	

Zone configuration

To configure the zone in Element manager, complete the following procedure.

Procedure 61

Configuring the Zone

Step	Action
1	Select System > IP Network > Zones .
2	Add a new zone for virtual trunks used for the SIP DECT system. Select the Zone you wish to add, for example 1. Configured zones appear in the list at the bottom of the page. Do not use zone 0.
3	Leave the default values for bandwidth and resource type as it is.
4	Select VTRK for the Zone Intent (ZBRN)
5	For Description (ZDES), type a meaningful description.

- 6 Click **Submit**.

--End--

Adding a D-Channel

To add a D-Channel using Element manager, complete the following procedure.

Procedure 62 Adding a D-Channel

Step	Action
1	Select Routes & Trunk > D-Channels from the menu list.
2	On D-channels list page select a number, for example 5, for D-Channel Number and DCH for type, and then click Add . The D-Channels Y Property Configuration page appears.
3	Select DCIP for CTYP, ISLD for USR and SL1 for IFC.
4	Select BSCOPT and click Edit to configure Remote Capabilities (RCAP).
5	On Remote Capabilities Configuration page select the check box for ND2 and MWI then click return .
6	Click Submit .

--End--

Adding a route

To add a route using Element manager, complete the following procedure.

Procedure 63 Adding a route

Step	Action
1	Select Routes & Trunks > Routes and Trunks from the menu list.
2	On the Route and Trunks page click Add route and Customer X . The New Route Configuration page appears.
3	Select a number, for example 6, for ROUT.
4	Select TIE for TKTP.
5	Select IAO for ICOG and enter a number, for example 6 for ACOD.

- 6 Select the check box for **VTRK** and enter the VTRK zone number, for example 1, for ZONE.
- 7 Select the **Node ID** of the signaling server for NODE.
- 8 Select **SIP** for PCID.
- 9 Select the check box for **ISDN**.
- 10 Select **ISLD** for **MODE**.
- 11 Select the DCH created previously, for example 5.
- 12 Select **SL1** for IFC and **1**, for example, for the Private Network Identifier (PNI).
- 13 Select the check box for **NCNA** and **INAC**.
- 14 Select **CDP** for CTYP.
- 15 In **Network Options** select **ESN5** for SIGO.
- 16 Click **Submit**.

--End--

Adding trunks

To add a trunk using Element manager, complete the following procedure.

Procedure 64 Adding a trunk

Step	Action
1	Select System > Core Equipment > Superloops from the menu list.
2	On Superloops, select 96, for example, for superloop number and Virtual for type.
3	Click Add and then click Save .
4	Select Routes & Trunks > Routes & Trunks from the menu list.
5	On the Route & Trunks page click Customer: X . The customer list expands and Route: Z appears.
6	click Add trunks . The Customer X, Route Z, New Trunk Configuration page appears.
7	Select 32 for MTINPUT.
8	Select IPTI for TYPE.
9	Select VTRK for XTRK.

- 10 Enter the route number you configured previously and the route member, for example 6 1, for RTMB.
- 11 Select **WNK** both STRI/STRO and 1 for CHID.
- 12 Enter a **terminal number (tn)** for TN, for example 96 0 0 0.
Refer to the superloop configured previously in this procedure.

Note: TN format: L s cu, where L = virtual superloop, s = shelf, c = card, and u = unit.
- 13 Click **Edit** to configure Class of Service (CLS).
- 14 Select **Digitone Dial Pulse (DTDP)** for Dial Pulse.
- 15 Click **Return Class of Service**.
- 16 Select **Advanced Trunk Configurations** and select the check box for **Answer and disconnect Supervision required (SUPN)**.
- 17 Click **Save**.

--End--

Configuring network access

To configure network access using Element manager, follow the steps in the next procedure.

Procedure 65 Configuring network access

Step	Action
1	Select Dialing & Numbering Plans > Electronic Switched Network from the menu list.
2	Select Customer X > Network Control & Service > Network Control Parameters (NCTL) > Network Control Basic Parameters and click Edit .
3	Click Submit .

--End--

Creating ESN control block

If the ESN control block is not configured, complete the following procedure to create an ESN control block using Element manager.

Procedure 66
Creating ESN Control Block

Step	Action
1	On the ESN page, select Customer X > Network Control & Service > ESN Access Code & Parameters (ESN) . The ESN Access Codes and the Basic Parameters page appears.
2	Enter 10 for MXDM/MXRL/MXIX/MXFC/MXFS/MXLC/MXSC, 9 for AC1, 6 for ERDT, 0 for MXSD.
3	Click Submit .
--End--	

Adding digit manipulation block

To add digit manipulation block using Element manager, follow the steps in the next procedure.

Procedure 67
Adding digit manipulation block

Step	Action
1	On the ESN page, select Customer X > Network Control & Service > Digit Manipulation Block (DGT) .
2	Select Digit Manipulation Block index 1 , or next available index, and click Add .
3	Click Submit .
--End--	

Adding route list block

To add a route list block using Element manager, follow the steps in the next procedure.

Procedure 68
Adding route list block

Step	Action
1	On the ESN page, select Customer X > Network Control & Service > Route List Block (RLB) .
2	Enter 1 for route list index and click Add .

- 3 Select the route created before, for example 6, for **ROUT** and 1 for **DMI**.
- 4 Click **Submit**.

--End--

Adding location code (UDP)

To add a location code (UDP) using Element manager, follow the steps in the next procedure.

Procedure 69 Adding location code (for UDP)

Step	Action
1	On the ESN page, select Customer X > Numbering Plan (NET) > Access Code 1 > Location Code (LOC) .
2	Enter a 3-digit code, for example 442, and click Submit .
3	Enter 7 for FLEN, select 1 for RLI and enter LOC+0000 for LDN, for example 4420000.
4	Click Submit .

If you plan to create a Branch Office Configuration, see Perform configuration on Element Manager.

--End--

Adding Trunk Steering Code (CDP)

To add a trunk steering code (for CDP) using Element manager, follow the steps in the next procedure.

Procedure 70 Adding Trunk Steering Code (CDP)

Step	Action
1	On the ESN page, select Customer X > Coordinating Dialing Plan (CDP) > Trunk Steering Code (TSC) .
2	Add a 2-digit code, for example 44, and click Submit .
3	Enter 6 for FLEN, select 1 for RLI.
4	Click Submit .

If you plan to create a Branch Office Configuration, see Perform configuration on Element Manager.

--End--

Configuring the signaling server

To configure the Signaling Server using Element manager, follow the steps in the next procedure.

Procedure 71 Configuring the signaling server

- | Step | Action |
|------|---|
| 1 | Select System > IP Network > Node: Server, Media Cards .
The Node Configuration page appears. |

- 2 Select **Edit**.
- 3 Select **SIP GW Settings** and enter Signaling Server NRS IP address, for example 192.168.100.104, for **Primary Proxy or Re-redirect IP address**.
- 4 Select **UDP as Transport Protocol**.

5 Select **SIP URI Map** and enter the domain names.

- SIP URI Map	
Public E.164/National domain name	+7 *
Public E.164/Subscriber domain name	+7831 *
Public E.164/Unknown domain name	
Public E.164/Special Number domain name	
Private/UDP domain name	mera.ru
Private/CDP domain name	cdp.mera.ru
Private/Special Number domain name	
Private/Unknown (vacant number routing) domain name	
Unknown/Unknown domain name	

--End--

Configuring SIP properties

To configure SIP properties using Element manager, complete the following procedure.

Procedure 72
Configuring SIP properties

Step	Action
1	Expand Signaling Servers properties.
2	Enter a Hostname , for example SS_Node55_Ldr.
3	Select the check box for Enable Line TPS .
4	Select SIP Only for Virtual Trunk TPS .
5	Select the check box for Enable IP Proxy/Redirect Server , if SIP Gateway and Redirect Server (NRS) are co-resident.
6	Enter a SIP Domain Name , for example mera.ru.
7	Enter a SIP Gateway endpoint name , for example DAP1.
8	Enter the Authentication Password .
9	Select Primary for Network Routing Service Role
10	Click Save and Transfer .

After the save and transfer is complete, the message **Transfer successful to all elements in the node** appears.

11 Click **OK**.

The **Transfer/Status** page appears. Reboot of signaling server and media cards is mentioned in the warning window.

- Signaling Server 192.168.32.41 Properties
Remove

Role Leader

Type ISP1100

Embedded LAN (ELAN) IP address *

Embedded LAN (ELAN) MAC address *

Telephony LAN (TLAN) IP address *

Telephony LAN (TLAN) gateway IP address

Hostname *

H323 ID

Enable Line TPS

Enable IP Peer Gateway (Virtual Trunk TPS) ▼

If Telephony LAN(TLAN) IP address an
Telephony LAN(TLAN) Node IP address
applications will not run.

Enable SIP Proxy / Redirect Server

Local SIP TCP/UDP Port to Listen to

SIP Domain name

SIP Gateway Endpoint Name

SIP Gateway Authentication Password

Enable Gatekeeper

Network Routing Service Role ▼

Save and Transfer
Cancel

--End--

Use the procedures in “[NRS configuration](#)” (page 163) to configure NRS.

NRS configuration

Use the steps in [Procedure 73 “Logging on to NRS”](#) (page 163) to log on to the Network Routing Service manager (NRS).

Procedure 73 Logging on to NRS

Step	Action
1	Log in to Network Routing Service manager and then log in to Element manager .

- 2 Select **Dialing & Numbering plans > Network Routing Service**.
- 3 Enter the **TLAN address of the Signaling Server**.
- 4 Click **Next**.

--End--

Use the steps in these procedures to configure the NRS.

- [Procedure 74 "Setting the database to standby view" \(page 164\)](#)
- [Procedure 75 "Creating service domain" \(page 165\)](#)
- [Procedure 76 "Adding the UDP domain" \(page 165\)](#)
- [Procedure 77 "Adding the CDP domain" \(page 165\)](#)
- [Procedure 78 "Adding Gateway Endpoint for the signaling server" \(page 166\)](#)
- [Procedure 79 "Adding Gateway Endpoint for DAP redirect server" \(page 167\)](#)
- [Procedure 80 "Configuring routing entries for DAP Redirect Server" \(page 168\)](#)
- [Procedure 81 "Configuring routing entries for the signaling server" \(page 169\)](#)
- [Procedure 82 "Saving changes" \(page 170\)](#)

Setting the database to standby view

The Configuration tab is used to configure NRS for actions such as adding a service domain, L1 (UDP) and L0 (CDP) domains, adding gateway endpoints, or adding routing entries. Set the database to Standby Database view in order to make changes.

Follow the steps in the next procedure to set the database to standby view.

Procedure 74 Setting the database to standby view

Step	Action
1	Select Configuration from the tool bar at the top of the page. A dialog box indicating the status of Active and Standby database is displayed.
2	Click OK .

- 3 Click **set standby DB view**.

--End--

Creating service domain

To create a service domain, complete the following procedure.

Procedure 75

Creating service domain

Step	Action
1	Select Service Domains from the menu list on the left.
2	Click Add .
3	Enter the SIP Domain Name you configured on the signaling server, for example mera.ru, for Domain name and a domain description, for example Mera Lab.
4	Click Save .

--End--

Adding the UDP domain

Procedure 76

Adding the UDP domain

Step	Action
1	Select L1 Domains (UDP) from the menu list on the left.
2	Click Add .
3	Enter the L1 domain name , which is the same as the Private/UDP domain name configured in SIP Gateway, for example mera.ru, for domain name, and a domain description, for example UDP Domain.
4	Click Save .

--End--

Adding the CDP domain

Procedure 77

Adding the CDP domain

Step	Action
1	Select L0 Domains (CDP) from the menu list on the left.

- 2 Click **Add**.
 - 3 Enter the L0 domain name matching the Private/CDP domain name configured on SIP Gateway and a domain description, for example CDP Domain.
For example, enter L0 domain name *cdp* for Private/CDP domain name *cdp.mera.ru*.
- ATTENTION**
Configured L0 domain name must be unique for SIP DECT in the communication system.
- 4 Enter **E.164 country code**, for example 7, and **E.164 area code**, for example 831.
 - 5 Click **Save**.

--End--

Adding Gateway Endpoint for the signaling server

Procedure 78

Adding Gateway Endpoint for the signaling server

Step	Action
1	Select Gateway Endpoints from the menu list on the left.
2	Click Add .
3	Enter the SIP Gateway endpoint name configured in the Node properties on the signaling server, for example SS_Node55_Ldr for Endpoint name.
4	Enter an endpoint description , for example SIP GW on the Signaling Server.
5	Select Static SIP Endpoint for SIP support .
6	Select UDP for SIP Transport .
7	Enter the Static endpoint address (Signaling Server Node IP address) 192.168.100.105.
8	Click Save .

--End--

Adding Gateway Endpoint for DAP redirect server

You need to choose one of the DAPs to which NRS routes all incoming requests from SIP Gateway. This DAP further routes the incoming requests to appropriate DAPs in the SIP DECT system. The selected DAP is called the DAP Redirect Server.

Procedure 79
Adding Gateway Endpoint for DAP redirect server

Step	Action
1	Select Gateway Endpoints from the menu list on the left.
2	Click Add
3	Enter the SIP Gateway endpoint of the DAP , for example DAP1, for Endpoint name.
4	Enter an endpoint description , for example DECT Access Point.
5	Select Static SIP Endpoint for SIP support .
6	Select UDP for SIP Transport .
7	Enter the Static endpoint address (DAP IP address) 192.168.100.200.

The screenshot shows the Nortel Network Routing Service Manager interface. The main content area is titled "Gateway Endpoints" and shows a table of configured endpoints. The table has the following data:

#	ID	Support Protocol(s)	Call Signaling IP	Description	# of routing entries
1	DAP1	Static SIP	192.168.100.200	DECT Access Poi ...	6
2	SS_Node55_Ldr	Static SIP	192.168.100.105	SIP GW on the S. ...	0

8 Click **Save**.

--End--

Configuring routing entries for DAP Redirect Server Procedure 80 Configuring routing entries for DAP Redirect Server

Step	Action
------	--------

- | | |
|---|--|
| 1 | Select Routing Entries from the menu list on the left. |
|---|--|

Location: Configuration > Routing Entries >

Routing Entries

Show Routing Entries for (Service Domain / L1 Domain / L0 Domain / Endpoint)
Select domains and enter a gateway endpoint name to show specified routing entries.
Use the wildcard * by itself for all gateway endpoints :

mera.ru / mera.ru / cdp /

Gateway Endpoint: DAP1 [Look up](#)

With DN Type: < All DN Types > [Show](#)

[Add...](#)

Showing 1 - 1 of 1 < Previous | Next >

#	DN Prefix	DN Type	Route Cost	SIP URI Phone Context
1	442????	Private level 1 regional (UDP location code)	1	mera.ru

[Add...](#)

- Click **Look Up**.
The **Look up path for gateway endpoints** page appears.
- Select the for DAP, for example, DAP1. Enter the **ID of the selected endpoint** in the Gateway Endpoint text box.
- Click **Show** to see all the entries for this endpoint.
This field is empty if there are no entries.
- Click **Add**.
- If you configured UDP, select **Private level 1 regional (UDP location code)** for DN type, enter the **location code (LOC)** and **question marks (?)** equal to number of digits in DN subscribed on the DAP, for example 442????, for DN Prefix and 1 for Route cost and click **Save**.
- If you configured CDP, select **Private level 0 regional (CDP steering code)** for DN type, enter the **Trunk Steering code (TSC)** and **question marks (?)** equal to number of digits in DN subscribed on DAP, for example 44????, and click **Save**.

If you plan to create a Branch Office Configuration, see Perform configuration on NRS.

--End--

Configuring routing entries for the signaling server

Note: If Collaborative servers are not configured on your system, you can configure the default route for CDP for the Signalling Server instead of CDP routing entry.

Procedure 81 Configuring routing entries for the signaling server

Step	Action
------	--------

- | | |
|---|---|
| 1 | Select Routing Entries from the menu list on the left. . |
|---|---|

The screenshot shows the Nortel Network Routing Service Manager (NRS) interface. The main heading is "NORTEL NETWORK ROUTING SERVICE MANAGER". Below the heading is a navigation bar with tabs for Home, Configuration, Tools, Reports, and Administration. The "Configuration" tab is active. The page title is "Routing Entries".

The interface includes a search form with the following fields:

- Service Domain: mera.ru
- L1 Domain: / mera.ru
- L0 Domain: / cdp
- Gateway Endpoint: SS_node55_ldr
- With DN Type: Private level 0 regional (CDP steering code)

There is a "Look up" button and a "Show" button. Below the search form is a table showing the results of the search:

#	DN Prefix	DN Type	Route Cost	SIP URI Phone Context
1	0000 - 9999	Private level 0 regional (CDP steering code)	1	cdp.mera.ru

- | | |
|---|---|
| 2 | Click Look Up .
The Look up path for gateway endpoints page appears. |
| 3 | Select the SIP endpoint for the signaling server, for example SS_Node55_Ldr. |
| 4 | Click Show to see all the entries for this endpoint.
This field is empty if there are no entries. |
| 5 | Click Add . |

- 6 Select **Private level 0 regional (CDP location code)** for DN type, enter **0000-9999** for DN Prefix and **2** for Route cost.

ATTENTION

If using a Trunk Steering Code (TSC) to make calls from Communication Server 1000 to SIP DECT, the cost of the CDP routing entry for the Signaling Server must be higher than the cost of the CDP routing entry for DAP Redirect Server.

- 7 Click **Save**.

--End--

Saving changes

**Procedure 82
Saving changes**

Step	Action
------	--------

- | | |
|---|---|
| 1 | Click Tools on the tool bar. |
| 2 | Click Database Actions on the menu list on the left. |
| 3 | Select Cut over and commit from the list. |
| 4 | Click Submit . |

--End--

Call server configuration

The Call Server is configured using a command line interface with LD overlays.

Use LD 15 to enable Personal Call Assistant before you configure the Personal Call Assistant.

Table 20
LD 15: Enable personal call assistant

Prompt	Response	Description
REQ	CHG	
TYPE	FTR	FTR_DATA
CUST	n	n = customer number
...		
PCA	ON	Enable Personal Call Assistant
...		

Configuring Universal Extension

Universal Extension (UEXT) redirects incoming calls to the DAP. Key 0 corresponds with the DN, configured on the DAP. Key 1 HOT P is the same number with access and location codes (for UDP) or trunk steering code (for CDP).

Use LD 11 to configure UEXT.

Note: Packages 412 and 415 must be enabled on the Call Server.

Table 21

LD 11: Add universal extension (UDP)

Prompt	Response	Description
REQ	NEW	Add new extension
TYPE	UEXT	Universal Extension
CUST	n	n = customer number
TN	L s c u, for example 96 0 1 0	where L = virtual superloop, s = shelf, c = card, u = unit
UXTY	SIPN	UEXT subtype
DES	aaaa	Designator. Any description can be used.
KEY	0 aaa yyyy, for example, 0 SCR 5001 1 HOT P nn yyyy, for example, 1 HOT P 8 94425010	0 aaa yyyy = Primary UEXT DN, where: <ul style="list-style-type: none"> • aaa = MCN, MCR, SCN, or SCR • yyyy = primary DN 1 hot p nn yyyy = Target DN, where: <ul style="list-style-type: none"> • nn = DN length (maximum length is 32) • yyyy = <AC1+LOC+ subscribed DN on DAP>

Table 22

LD 11: Add universal extension (CDP)

Prompt	Response	Description
REQ	NEW	Add new extension
TYPE	UEXT	Universal Extension
CUST	n	n = customer number
TN	L s c u, for example 96 0 1 0	where L = virtual superloop, s = shelf, c = card, u = unit
UXTY	SIPN	SIPN UEXT subtype
DES	aaaa	Designator. Any description can be used.

Prompt	Response	Description
KEY	0 aaa yyyy, for example, 0 SCR 5001 1 HOT P nn yyyy, for example, 1 HOT P 6 445010	0 aaa yyyy = Primary UEXT DN, where: <ul style="list-style-type: none"> • aaa = MCN, MCR, SCN, or SCR • yyyy = primary DN 1 hot p nn yyyy = Target DN, where: <ul style="list-style-type: none"> • nn = DN length (maximum length is 32) • yyyy = <TSC+ subscribed DN on DAP>

Configuring CLID

Before configuring CLID, create a CPND block.

CLID is configured with LD 95.

Table 23
LD 95: Configure CLID

Prompt	Response	Description
REQ	NEW	
TYPE	NAME	
CUST	n	n = customer number
DN	xxxx, for example 5001	DN configured at the DAP and UEXT Key 0 at DN.
NAME	aaaaaa, for example Nick Johns	Handset user name

Enabling message waiting indication

The following configuration in Customer Data Block must be presented to enable Message Waiting Indication (MWI) for IP DECT handsets.

Note: Package 175 must be enabled on the Call Server for this feature.

MWI is configured with LD 15.

Table 24
LD 15: Enable message waiting indication

Prompt	Response	Description
REQ	CHG	
TYPE	IMS	IMS_DATA
CUST	n	n = customer number
...		

Prompt	Response	Description
IMS	YES	Enable IMS
...		

Table 25
LD 15: Enable Message Center

Prompt	Response	Description
REQ	CHG	
TYPE	FTR	FTR_DATA
CUST	n	n = customer number
...		
OPT	MCI	Message Center included
...		

Routed Head Quarter configuration

In this configuration, there is more than one network segment in the Head Quarter. The routers in this configuration must forward IP multicast packages. Network components, such as switches and routers, must be correctly configured for VoIP and IP multicast. The network must support IP multicast between all network components that are used for IP DECT System.

You can edit the following settings:

- **Time to Live (TTL) 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 is not forwarded by a Router. If the Time to Live is higher than 1, multicast packages can be forwarded by the Router, depending on settings in the Router. If the TTL (for the multicast packages) is set to 1, leave this aggregated subnet mask empty. If the TTL (for the multicast packages) is set to a value higher than 1, fill in this aggregated subnet mask to signal to the system which smaller subnets are connected together as one subnet using a router supporting IP multicast.
- **Aggregated Subnet mask**—The aggregated subnet mask is the subnet mask for the DAPs to determine the network boundaries for an IP DECT Network in which seamless hand over is possible. Use G.711, which covers the network segments connected together using routers that support IP multicast.

If there are DAPs outside this aggregated subnet mask, regard the DAP or DAPs as in a branch office. Note that the IP address of the PBX is compared with the IP address or addresses of the DAP or DAPs using this subnet mask. If the IP addresses are in different

subnets according to this mask, the DAP or DAPs are supposed to be in a branch office. If the IP addresses are in the same aggregated subnet according to this mask, the system assumes that the IP addresses are in the same subnet.

The term aggregated means that the subnet consists of smaller subnets connected over a router, but according to the subnet mask, all behave as one subnet. This is applicable for the Routed Head Quarter network solution without branch offices.

Routed Head Quarter configuration implies that different subnets are connected through one or more routers. The subnets in the network are part of one company network.

For setting up Routed Head Quarter configuration, the network components, such as the switches and the routers, must be correctly configured for VoIP and IP multicast. Also, the network must support IP multicast between all network components that are used for SIP DECT System.

Routed Head Configuration is the same as Simple configuration, but includes one more step. See [Procedure 49 "Configuring Network Settings" \(page 140\)](#).

Choice of system configuration

Procedure 83

Choosing system configuration

Step	Action
1	Open the DAP Configurator and click Modify .
2	Select the SIP DECT system that you are running. Click System Configuration .
3	Choose Routed Head Quarter Configuration for System configuration.
4	Enter a Time To Live Value higher than 1 to let the Router forward multicast packages.
5	Calculate and enter the Aggregated Subnet mask .

The Aggregated subnet mask is the subnet mask for the DAPs to determine the network boundaries for a SIP DECT System. The Aggregated subnet mask covers the network segments connected together using routers that support IP multicast.

Example: DAPs in three subnets:

- 192.168.1.0/24
- 192.168.4.0/24
- 192.168.5.0/24

For this example, enter the Aggregated Subnet Mask
255.255.248.0.

6 Click **Apply**.

--End--

Multi site mobility network configuration

Multi site mobility network makes it possible to use portable DECT handsets on different MCDN nodes with installed SIP DECT systems. It is possible for only one subscription to be in the handset for all SIP DECT systems when you are using SARI. In this case SARI on all SIP DECT systems must be the same.

ATTENTION

When the handset is on a remote MCDN node, the ring back tone is given to a party calling to its local DN even if the handset is busy at the moment.

ATTENTION

Before starting multi site Configuration, perform the following.

- Create any type of SIP DECT configuration on each MCDN node selected for MSMN.
- Connect the systems configured for MSMN through trunks. Configure the uniform (UDP) or coordinated (CDP) numbering plan.

The following topics are described in this section.

- “Subscribe a multi site DECT handset” (page 176)
- “Import and export subscriptions” (page 177)
- “Configure NRS for multi site mobility network” (page 178)
- “Call server configuration to MSMN” (page 179)
- “Configuration of Personal Call Assistant” (page 182)
- “Configuration of Universal Extension (UEXT) on the remote system” (page 182)

Subscribe a multi site DECT handset

Use the following procedure to subscribe a multi site DECT handset.

Procedure 84

Subscribing a multi site DECT handset

Step	Action
1	Open Internet Explorer and enter the following URL in the address field: <code>localhost/cds</code> . The DAP manager IP DECT page appears.
2	In the navigation menu, select Pack Up & Go .
3	Select the multi site subscriptions check box.
4	Enter PARI and SARI of the target system
5	Click OK .
6	Enter the number range to define DNs for multi site DECT handsets, for example from 5010 to 5020.
7	Select the required available extension number(s), for example 5010. If the required number is not visible, select another page. The page number is displayed in the top and bottom rows of the subscriptions table.
8	Click Enable for Multi-Site . The status of the configuring subscription record changes from "Free" to "Enabled" and the Personal Identification Number (PIN) is shown. A PIN is generated by the DECT manager on each subscribe operation and only shows while the subscription status is enabled.
9	Take a DECT handset and navigate to the System configuration menu.
10	Choose New and enter the displayed PIN code . Sometimes you need to enter the PARK code first. The PARK code is displayed on the left at the bottom of the Subscriptions page. If the PIN is not entered within 16 minutes, the subscription mode is terminated for that specific extension

number and you must start the subscription process from the beginning.

- 11 Enter the **name of your SIP-DECT system** and the **DN** that appears on handset screen.
- 12 The status of the configuring subscription record changes from "Enabled" to "Subscribed".

--End--

Import and export subscriptions

Use the procedures in this section to import and export subscriptions.

Procedure 85 Exporting subscriptions in a file

Step	Action
1	Select Export (prepared) .
2	Enter the folder where the file with the subscriptions are stored.
3	Copy this file to the DAP controller PC of the remote system or systems.
4	Click Clear host .
5	Click Back to main .

--End--

Procedure 86 Importing subscriptions on the home system

Step	Action
1	Open localhost/cds in you Internet Browser (on DAP controller PC). The DAP manager IP DECT page appears.
2	In the navigation menu, click Pack Up & Go .
3	Click Import .
4	Choose the appropriate file from the folder that stores files with subscriptions
5	Click OK .

--End--

Procedure 87
Importing subscriptions on remote systems

Step	Action
1	Open localhost/cds in you Internet Browser (on DAP controller PC). The DAP manager IP DECT page appears.
2	In the navigation menu, click Pack Up & Go .
3	Click Import .
4	Choose the appropriate file in the folder that stores files with subscriptions
5	Click OK .
--End--	

Configure NRS for multi site mobility network

Procedure 88
Configuring NRS for multi site mobility network

Step	Action
1	Log in to Element Manger, select Dialing & Numbering plans > Network Routing Service and enter the TLAN address of the Signaling Server . Click Next .
2	Select Configuration from the tool bar at the top of the page. A dialog box indicating the status of Active and Standby database is displayed. Click OK .
3	Click set standby DB view .
4	Select Routing Entries from the menu list on the left.
5	Click Look Up and the Look up path for gateway endpoints page is displayed. Select the SIP endpoint for DAP <u>on the current system</u> , for example DAP1, and the ID of the selected endpoint is entered in the Gateway Endpoint text box.
6	Click Show to see all the entries for this endpoint. This field is empty if there are no entries.
7	Click Add .
8	If you configured UDP, select Private level 1 regional (UDP location code) for DN type, enter the location code (LOC) and question marks (?) equal to the number of digits of DN subscribed to DAP, for example 442????, for DN Prefix and 1 for Route cost and click Save .

- 9 If you configured CDP, select **Private level 0 regional (CDP location code)** for DN type, enter the **trunk steering code (TSC)** and **question marks (?)** equal to number of digits of DN subscribed to DAP, for example 44????, for DN Prefix and 1 for Route cost and click **Save**.

- 10 Save changes.

ATTENTION

The described configuration on NRS must be performed on each system for MSMN. Location or Trunk Steering codes must correspond with the codes configured on each system.

--End--

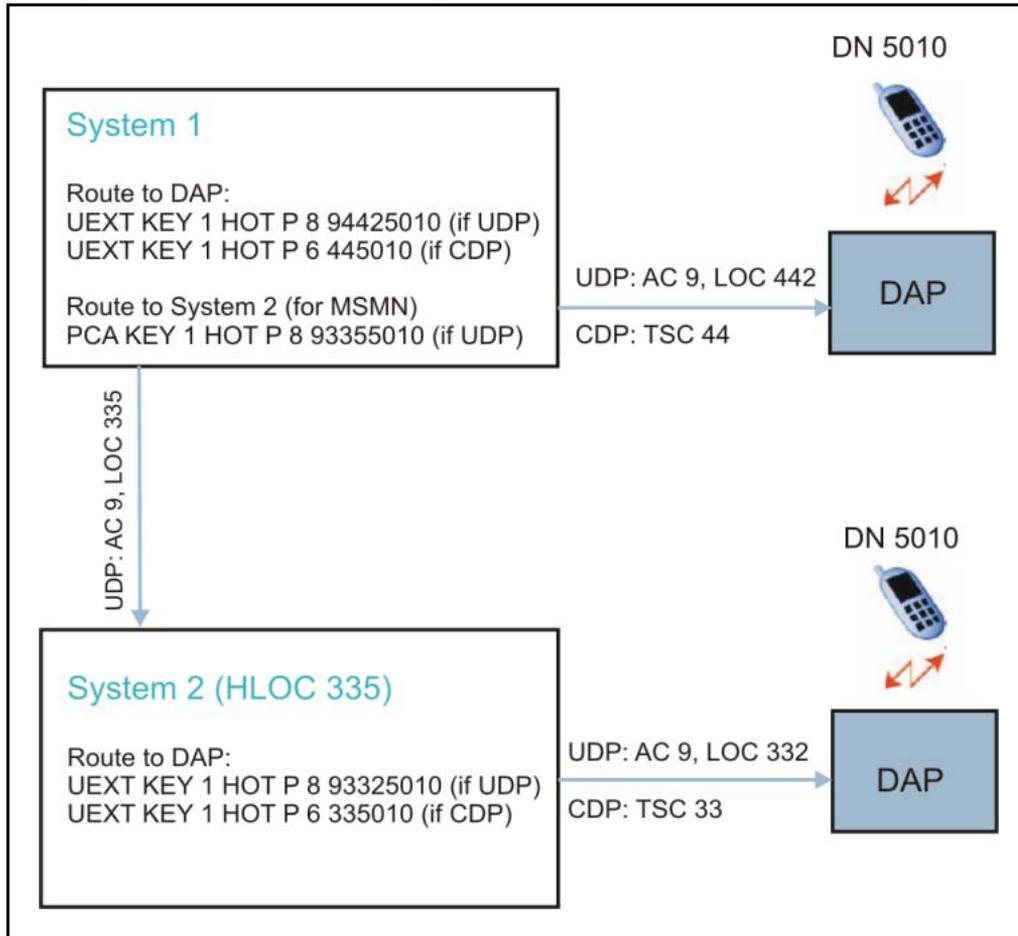
Call server configuration to MSMN

In this document the following parameters are used to show an example of configuring an MSMN SIP DECT system.

- Codes on system 1
 - Access Code: 9
 - Location code to DAP: 442
 - Trunk steering code to DAP: 44
 - Location code to system 2: 335
- Codes on system 2
 - Home location code: 335
 - Access Code: 9
 - Location code to DAP: 332
 - Trunk steering code to DAP: 33

See [Figure 52 "Example of an MSMN SIP DECT system"](#) (page 180).

Figure 52
Example of an MSMN SIP DECT system



Use LD 15 to enable Personal Call Assistant before you configure the Personal Call Assistant.

Table 26
LD 15: Enable Personal Call Assistant

Prompt	Response	Description
REQ	CHG	
TYPE	FTR	FTR_DATA
CUST	n	n = customer number
...		
PCA	ON	Enable Personal Call Assistant
...		

Configuring Universal Extension (UEXT) for multi site handset

Universal Extension (UEXT) redirects incoming calls to the DAP. Key 0 corresponds with the DN, configured on the DAP. Key 1 HOT P is the same number with access and location codes, for UDP, or trunk steering code, for CDP. UEXT is configured with LD 11.

Table 27
LD 11: Add universal extension (UDP)

Prompt	Response	Description
REQ	NEW	Add new extension
TYPE	UEXT	Universal Extension
CUST	n	n = customer number
TN	L s c u, for example 96 0 1 10	where L = virtual superloop, s = shelf, c = card, u = unit
UXTY	SIPN	UEXT subtype
DES	aaaa	Designator. Any description can be used.
KEY	0 aaa yyyy, for example, 0 SCR 5010 1 HOT P nn yyyy, for example, 1 HOT P 8 94425001	0 aaa yyyy = Primary UEXT DN, where: <ul style="list-style-type: none"> • aaa = MCN, MCR, SCN, or SCR • yyyy = primary DN 1 hot p nn yyyy = Target DN, where: <ul style="list-style-type: none"> • nn = DN length (maximum length is 32) • yyyy = <AC1+LOC+ subscribed DN on DAP>

Table 28
LD 11: Add universal extension (CDP)

Prompt	Response	Description
REQ	NEW	Add new extension
TYPE	UEXT	Universal Extension
CUST	n	n = customer number
TN	L s c u, for example 96 0 1 10	where L = virtual superloop, s = shelf, c = card, u = unit
UXTY	SIPN	UEXT subtype
DES	aaaa	Designator. Any description can be used.

Prompt	Response	Description
KEY	0 aaa yyyy, for example, 0 SCR 5010 1 HOT P nn yyyy, for example, 1 HOT P 6 445001	0 aaa yyyy = Primary UEXT DN, where: <ul style="list-style-type: none"> • aaa = MCN, MCR, SCN, or SCR • yyyy = primary DN 1 hot p nn yyyy = Target DN, where: <ul style="list-style-type: none"> • nn = DN length (maximum length is 32) • yyyy = <TSC+ subscribed DN on DAP>

Configuration of Personal Call Assistant

For multi site configuration an additional Personal Call Assistant redirects incoming calls to the remote system. Key 0 corresponds with the DN (MARP), for example 5010, configured on the DAP. Key 1 HOT P is the same number with access and location codes (for UDP) to the remote system.

PCA and UEXT are configured using LD 11.

Table 29
LD 11: Add PCA for multi site DECT Handsets (UDP)

Prompt	Response	Description
REQ	NEW	Add new extension
TYPE	PCA	Personal Call Assistant
CUST	n	n = customer number
TN	L s c u, for example, 96 0 2 10	where L = virtual superloop, s = shelf, c = card, u = unit
DES	aaaa	Designator. Any description can be used.
ZONE	0	zone number
KEY	0 aaa yyyy, for example 0 SCR 5010 1 HOT P nn yyyy, for example 1 HOT P 8 93355010	0 aaa yyyy = Primary UEXT DN, where: <ul style="list-style-type: none"> • aaa = MCN, MCR, SCN, or SCR • yyyy = primary DN 1 hot p nn yyyy = Target DN, where: <ul style="list-style-type: none"> • nn = DN length (maximum length is 32) • yyyy = <AC1+LOC+ subscribed DN on DAP>

Configuration of Universal Extension (UEXT) on the remote system

Universal Extension (UEXT) for multi site handset DNs, for example 5010, must be configured on the remote system to redirect incoming calls to the DAP. Key 0 corresponds with the multi site handset DN, configured on the

DAP. Key 1 HOT P is the same number with access and location codes, for UDP, or trunk steering code, for CDP, to access SIP trunks to the DAP, installed on the remote system.

Table 30

LD 11: Add universal extension for multi site DECT handsets (UDP)

Prompt	Response	Description
REQ	NEW	Add new extension
TYPE	UEXT	Universal Extension
CUST	n	n = customer number
TNI	L s c u, for example 96 0 1 10	where L = virtual superloop, s = shelf, c = card, u = unit
UXTY	SIPN	UEXT subtype
DES	aaaa	Designator. Any description can be used.
KEY	0 aaa yyyy, for example 0 SCR 5010 1 HOT P nn yyyy, for example 1 HOT P 8 93325010	0 aaa yyyy = Primary UEXT DN, where: <ul style="list-style-type: none"> • aaa = MCN, MCR, SCN, or SCR • yyyy = primary DN 1 hot p nn yyyy = Target DN, where: <ul style="list-style-type: none"> • nn = DN length (maximum length is 32) • yyyy = <AC1+LOC+ subscribed DN on DAP>

Table 31

LD 11: Add universal extension for multi site DECT handsets (CDP)

Prompt	Response	Description
REQ	NEW	Add new extension
TYPE	UEXT	Universal Extension
CUST	n	n = customer number
TN	L s c u, for example 96 0 1 10	where L = virtual superloop, s = shelf c = card, u = unit
UXTY	SIPN	UEXT subtype
DES	aaaa	Designator. Any description can be used.
KEY	0 aaa yyyy, for example, 0 SCR 5010 1 HOT P nn yyyy, for example 1 HOT P 6 335010	0 aaa yyyy = Primary UEXT DN, where: <ul style="list-style-type: none"> • aaa = MCN, MCR, SCN, or SCR • yyyy = primary DN 1 hot p nn yyyy = Target DN, where: <ul style="list-style-type: none"> • nn = DN length (maximum length is 32) • yyyy = <TSC+ subscribed DN on DAP>

System administration

Navigation

This chapter contains information about the administration of the SIP DECT system and covers the following topics.

- “DAP manager overview” (page 185)
- “Subscription management” (page 187)
- “DAP management” (page 194)
- “Add a DN range” (page 196)
- “Back up and restore subscriptions” (page 197)
- “Subscription export and import” (page 198)
- “DAP reboot history” (page 202)
- “System archive” (page 202)
- “Handset firmware update” (page 204)
- “Central directory access tool” (page 208)

DAP manager overview

This section provides an overview of the DAP manager application for SIP DECT, and describes the DAP manager interface. DAP manager is a web-based application.

To launch DAP manager, open Internet Explorer and enter the following URL in the address field: **localhost/cds**. The **DAP Manager** appears.

DAP Manager IPDECT - System_1

Subscriptions

Use DNR Filter

Number	Status	PIN	RPH	Presence	Registration status	Handset type	SW version	Comment	Edit
3000	Subscribed		OFF	Present	Registered	4060	51.20.53		Edit
5001	Subscribed	000		Present	Registered	4070	1.40		Edit
5002	Subscribed	000		Present	Registered	4070	1.40		Edit
5003	Subscribed		OFF	Present	Registered	4027	1.40		Edit
5004	Subscribed		OFF	Present	Registered	4027	1.40		Edit
5005	Subscribed	000		Present	Registered	4065R	72.24.14		Edit
5006	Subscribed	000		Present	Registered	4065R	89.24.30.31		Edit
5011	Subscribed		OFF	Absent	Registered	4025			Edit

Select a Subscription and click on a task.
Shift+Click to select a range.

Park : 31100051000347

Nortel © 2002-2007

This DAP manager page is divided into four main panels.

1. Main

- Subscriptions

Use this section for subscription management.

- Access points

Use this section to reboot DECT Access points and view the configuration data. The numbers between brackets indicate the number of present or working Access Points.

- Add number range

Use this section to enter the available extension numbers.

- Backup

Use this section to create a backup of the subscription data.

- Restore

Use this section to restore the subscription data.

- History

Use this section to view history of the DECT Access Points status.

— Pack Up & Go

Use this section to prepare subscription data for use in another system and to export multi site subscriptions.

2. Task list

The Task list shows the available tasks of a feature. For example, the feature Subscriptions has the tasks Enable, Disable, Terminate, and Delete Number.

3. Information area

The Information area provides notes or additional information.

4. Work space

In Work space you can enter or view data.

Subscription management

Use the information in this section to subscribe handsets. Before you can use a handset, you must register the handset and subscribe it to the system.

Subscribe a handset

Prerequisites

- A Directory Number (DN) must be available and free. See [“Add a DN range” \(page 196\)](#) for more information about making DNs available on the system.
- You also must configure the Communication Server 1000 system to which the SIP DECT system is connected.

See [“Call server configuration” \(page 170\)](#) for more information.

Procedure 89

Subscribing a handset

Step	Action
1	Open Internet Explorer and enter the following URL in the address field: localhost/cds . The DAP manager IP DECT page appears.
2	Select Subscriptions from the menu list on the left in the DAP manager IP DECT page. The Subscriptions page appears.
3	Select the required available extension number from the list on the Subscription page, for example, select 5001.

The handset can be subscribed to the extension number only if the status of the handset is free.

If the number you require does not appear, select another page. The page number is displayed in the top and bottom rows of the subscriptions table.

4 Click **Enable**.

The status of the configuring subscription record changes from "Free" to "Enabled" and the Personal Identification Number (PIN) appears. A PIN is generated by the DAP manager on each subscribe operation and is only displayed while the subscription status is enabled.

You can enable up to ten extension numbers for subscription at the same time.

5 Using the handset you are subscribing, Access the **System configuration** menu, and choose **New**.

See the User Guide for the handset for more information about accessing this menu, and other handset configuration information.

6 If the handset requests PARK code, enter the **PARK** code.

You can find the PARK code on the left at the bottom of the **Subscriptions** page. A PARK code is required only if there are overlapping DECT systems in your location; if only one DECT system is available in your location, a PARK code is not required.

7 Enter the **displayed PIN code**.

If you do not enter the PIN within 16 minutes, the subscription mode is terminated for that specific extension number, and you must begin the subscription process from the beginning.

8 Enter the **name of your SIP DECT system** and the **DN**.

You can find the name of the system and the DN on the handset screen. The status of the configuring subscription record changes from "Enabled" to "Subscribed".

--End--

Edit a subscription RPN

If it is necessary to change the DAP RPN to which the handset is subscribed, follow the steps in the next procedure.

Procedure 90
Editing a subscription RPN

Step	Action
1	Open Internet Explorer and enter the following URL in the address field: localhost/cds . The DAP manager IP DECT page appears.
2	Select Subscriptions from the menu list on the left in the DAP manager IP DECT page. The Subscriptions page appears.
3	Select the subscription you want to edit.
4	Click Edit .
5	Enter the RPN of the required installed DAP.
6	Click OK .

Note: The maximum number of subscription records for every DAP is 25.

--End--

Disable a subscription

Use the following procedure to disable a subscription.

After a subscription is disabled, the system attempts to remove the subscription data from the handset. If successful, the DN is available for use by another handset, and the handset can be registered again.

The handset cannot make and receive calls while the subscription is disabled.

Procedure 91
Disabling a subscription

Step	Action
1	Open Internet Explorer and enter the following URL in the address field: localhost/cds . The DAP manager IP DECT page appears.
2	Select Subscriptions . The Subscriptions page appears.
3	Select the DN to delete.

If the DN you want to disable is not visible, go to subsequent pages until you find it. The page number is displayed in the top and bottom rows of the subscriptions table.

4 Click **Disable**.

The status of the configuring subscription record changes from "Subscribed" to "Black Listed". When the SIP DECT system manages to delete the subscription record from the handset, the status changes to "Free".

--End--

Remove a subscription

Use the following procedure to remove subscription data from the system only. This procedure does not clear the subscription from the handset.

ATTENTION

Nortel recommends that you use the following procedure only if a handset has been lost or damaged beyond repair.
--

Procedure 92

Removing a subscription from the system

Step	Action
1	Open Internet Explorer and enter the following URL in the address field: localhost/cds . The DAP manager IP DECT page appears.
2	Select Subscriptions . The Subscriptions page appears.
3	Select the DN to disable. If the DN you want to disable is not visible, go to subsequent pages until you find it. The page number is displayed in the top and bottom rows of the subscriptions table.
4	Click Terminate . The status of the configuring subscription record changes from "Subscribed" to "Free".

--End--

Delete a number

Use the following procedure to delete a number from the added number range.

A number can be deleted only if no handset is subscribed to that number and the status of that number is free.

Procedure 93
Deleting a number

Step	Action
1	Open Internet Explorer and enter the following URL in the address field: localhost/cds . The DAP manager IP DECT page appears.
2	Select Subscriptions . The Subscriptions page appears.
3	Select the DN to disable. If the DN you want to disable is not visible, go to subsequent pages until you find it. The page number is displayed in the top and bottom rows of the subscriptions table.
4	Click Delete .
--End--	

Use the DNR filter

Follow the steps in the next procedure to use the DNR filter. Use the DNR filter if a list of subscriptions is long and it is hard to find certain extension numbers or DNRs, or if you want to look at only a part of the list of extension numbers or DNRs.

Procedure 94
Using the DNR filter

Step	Action
1	Open the DAP manager IP DECT page .
2	Select Subscriptions .
3	Select the check box next to Use DNR filter located at the top of the Subscriptions page. The Filters page appears.

DAP Manager INT - System_1

Subscriptions

Filter: DNR filter (selected)
 From:
 To:
 Exact match Starting with
 OK

Number	Presence	Registration status	Handset type	SW version	Comment			
3000	Present	Registered	4050		Edit			
5001	Subscribed	010	No	Unknown	Absent	4070		Edit
5002	Subscribed	010	No	Present	Registered	4027	1.51	Edit
5003	Subscribed	010	No	Present	Registered	4027	1.51	Edit
5004	Free							Edit
5005	Subscribed	010	No	Present	Registered	4065R	89.24.30.31	Edit
5006	Subscribed	010	No	Present	Registered	4060	51.24.15.03	Edit
5007	Subscribed	010	No	Present	Registered	4060	91.24.30.37	Edit
5008	Enabled	3689						Edit
5009	Free							Edit
5010	Subscribed	010	Yes	Present	Registered	4027	1.48	Edit
5025	Subscribed	010	Yes	Present	Registered	4070		Edit

Select a Subscription and click on a task.
 Shift+Click to select a range.

Park : 31174221505508

Nortel © 2002-2008

- 4 In the case of an Exact match enter the number range you want to see in the To field and in the From field. In the case of a Starting with, enter the first digit or digits in the From field.
 - 5 Select the option that applies, either **Exact match** or **Starting with**.
 - 6 Click **OK**.
- To disable a DNR Filter, clear the check box next to **Use DNR Filter**.

--End--

Handset status

The Subscriptions window in the DAP manager IP DECT shows three columns indicating the status of a handset.

- **Status**

This shows the status of the handset subscription in the DECT system. If no handset is subscribed to the extension number, the status is set to *Free*. *Free* means that this number is available for handset subscription.

If the extension number is activated for subscription, the status is changed to *Enabled* and you must follow the procedure to subscribe the handset.

If a handset is subscribed to the number, the status is changed to *Subscribed*.

If the subscription is disabled, the status is changed to *Black Listed*. *Black Listed* means the subscription is deleted from the handset and then the status is set to *Free*.

- **Presence status**

This shows the presence status of the handset in the DECT system. If the SIP DECT system detects that the handset is no longer present, the status changes from "present" to "absent".

The status changes to absent if one of the following cases occurs.

- The handset is switched off.
- The handset is put in the charger in disconnected charging mode (only for 4070 and 4027 Nortel DECT handsets).
- The handset is out of reach or switched off the system detects that the handset is no longer reachable and the status is automatically changed to absent. When the presence status of the handset is absent, the software version in the column "SW version" may still be displayed, but it is not relevant until the handset is present again.

The Presence status function and timing depends on system customized settings. If Presence status is enabled in the SIP DECT system, it takes 15 to 60 minutes before the system detects that the handset is no longer reachable.

- **Registration status**

The Registration status indicates the status of the handset in the SIP DECT system. The status is Registered or Absent.

- If the Registration status is **Registered**, the handset is registered in the SIP DECT system and usually can be used.
- If the Registration status is **Absent**, the handset is not registered in the SIP DECT system and cannot be used to make calls.

ATTENTION

The Communication Server 1000 system is not aware of the current status of the handset. Therefore, the Communication Server 1000 attempts to ring the handset even if the handset is absent.

- **Handset Type and SW Version**

This shows the type or model of the handset subscribed to the system and the version of software installed on the handset.

ATTENTION

The system loses the information about handset types and software versions subscribed on a DAP when the DAP reboots. To restore this information, turn off and on the handsets subscribed to the rebooted DAP or reboot all DAPs using option "Reboot all" in DAP Manager. See "[Reboot all DAPs](#)" (page 195).

DAP management

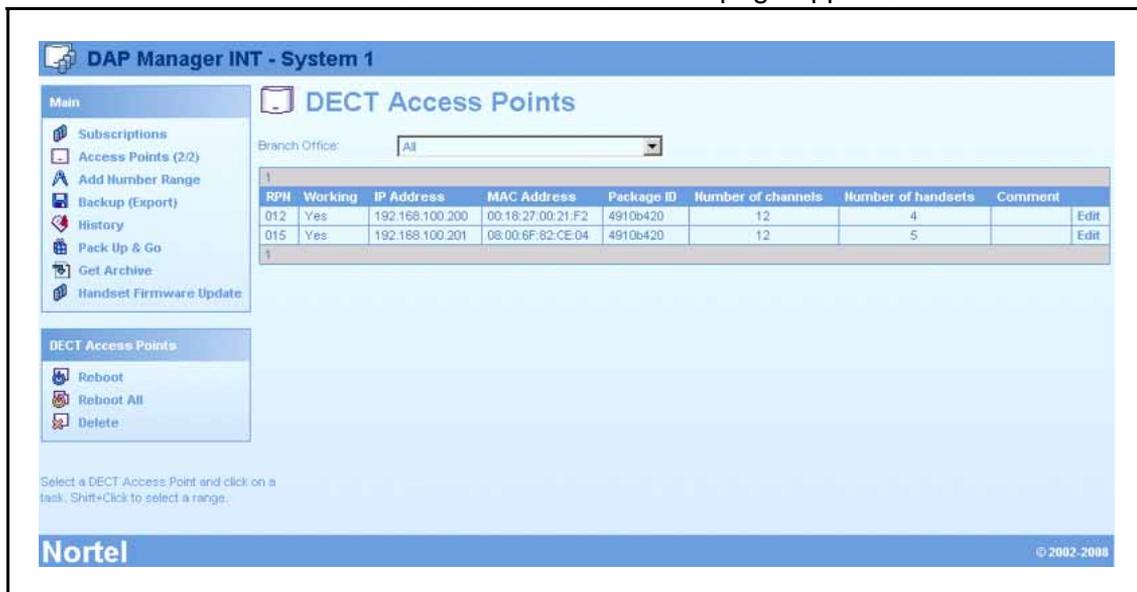
Use the procedures in this section to manage DECT Access Points (DAP).

Change a DAP Radio Part Number (RPN)

Use the following procedure to change the unique Radio Part Number (RPN) of a DECT Access Point (DAP) if you need to manually configure radio synchronization. Each DAP attempts to synchronize to the DAP with the lowest RPN.

Procedure 95 Changing an RPN

- | Step | Action |
|------|---|
| 1 | Open Internet Explorer and enter the following URL in the address field: localhost/cds .
The DAP manager IP DECT page appears. |
| 2 | Click Access points .
The DECT Access Points page appears. |



- | | |
|---|--|
| 3 | Select the DAP you want to edit. |
| 4 | Click Edit . |
| 5 | Enter the new RPN .
The RPN must be a hexadecimal two-digit number in the range 000 . . . 00F . |
| 6 | Click OK .
Wait until DAP reboots and starts working. |

--End--

Reboot a DAP

Use the following procedure to reboot a DAP. This can be required if you are performing a software upgrade, or if a DAP is not functioning properly.

Procedure 96 Rebooting a DAP

Step	Action
1	Open Internet Explorer and enter the following URL in the address field: localhost/cds . The DAP manager IP DECT page appears.
2	Click Access points . The DECT Access Points page appears.
3	Select the DAP you want to reboot.
4	Click Reboot . The DAP restarts. It takes several minutes for the DAP to begin working again after it restarts.

ATTENTION

If you use "Reboot" to restart a DAP, the information about types and software versions of subscribed handsets is lost. To restore this information, turn off and on the handsets subscribed to the rebooted DAP or reboot all DAPs using the option "Reboot all" in DAP Manager. See ["Reboot all DAPs" \(page 195\)](#).

--End--

Reboot all DAPs

Use the following procedure to reboot all the DAPs in a system. This can be required if you are performing a software upgrade, or if the DAPs are not functioning properly.

Procedure 97 Rebooting all the DAPs in a system

Step	Action
1	Open Internet Explorer and enter the following URL in the address field: localhost/cds . The DAP manager IP DECT page appears.
2	Click Access points . The DECT Access Points page appears.

- 3 Click **Reboot All**.

--End--

Use the following procedure to remove a DAP that is damaged beyond repair.

Procedure 98
Deleting a DAP

Step	Action
1	Open Internet Explorer and enter the following URL in the address field: localhost/cds . The DAP manager IP DECT page appears.
2	Select Subscriptions from the menu list on the left in the DAP manager IP DECT page. The Subscriptions page appears.
3	Click Access points .
4	Select the DAP you want to delete.
5	Click Delete .

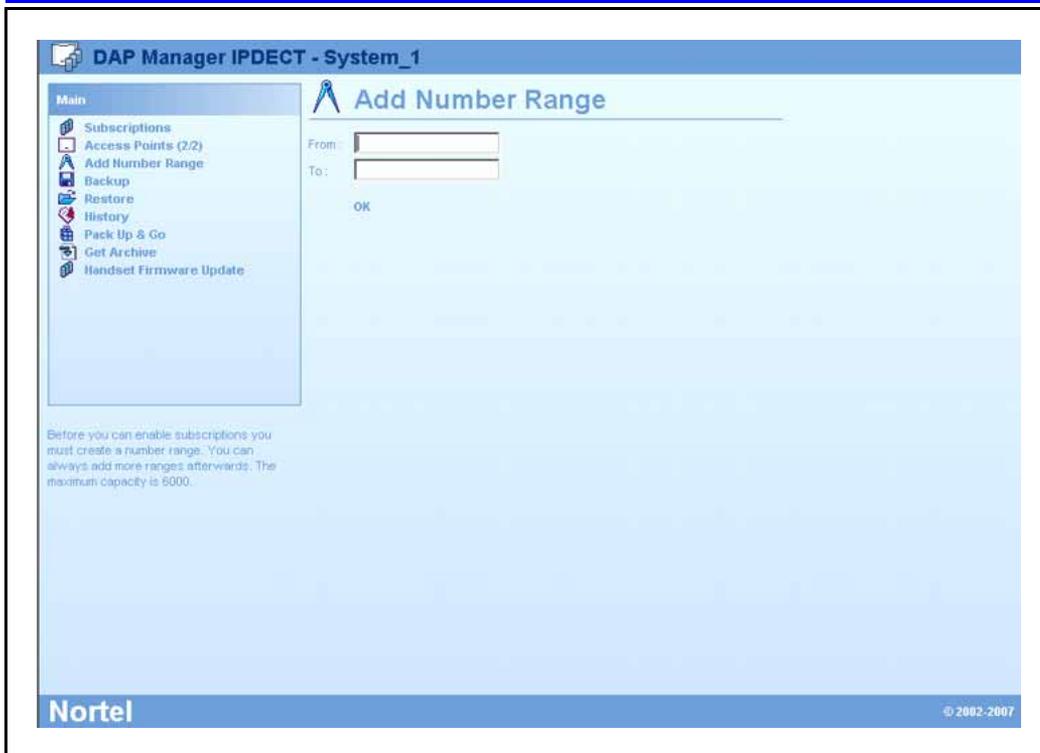
--End--

Add a DN range

Use the following procedure to define a range of available DNs. The numbers you define must also be assigned in the Communication Server 1000 system. You can assign a DN range manually, or by importing a .csv file.

Procedure 99
Assigning a DN range manually

Step	Action
1	Open Internet Explorer and enter the following URL in the address field: localhost/cds . The DAP manager IP DECT page appears.
2	Click Add Number Range . The Add number range page appears.



- 3 In the **From** field, enter the first number in the range. If you are adding a range consisting of one number only, proceed to step 5.

ATTENTION

The length of all DNs subscribed on DAPs must be the same.

- 4 In the **To** field, enter the last number in the range.
- 5 Click **OK**.

--End--

Use the following procedure to import a DN range from a .csv file.

Back up and restore subscriptions

Nortel recommends that you make a backup copy of the subscription database. Use the procedures in this section to back up and restore subscriptions.

Procedure 100 Backing up a subscription

Step	Action
1	Open Internet Explorer and enter the following URL in the address field: localhost/cds . The DAP manager IP DECT page appears.

- 2 Click **Backup**
The **File Download** page appears.
- 3 Click **Save**.
- 4 Select the folder where you want to store the backup file.
- 5 Enter a name for the file.
- 6 Click **Save**.
The file is saved to the selected location.

--End--

Procedure 101 **Restoring a subscription**

Step	Action
1	Open Internet Explorer and enter the following URL in the address field: localhost/cds . The DAP manager IP DECT page appears.
2	Click Restore . The Restore page opens.
3	Click Browse .
4	Browse to the folder where the backup file is stored, and select the backup file.
5	Click Save . The file is uploaded and the DAP controller service is automatically restarted. All DAPs are automatically restarted. A message appears in the information area after the restore is complete.

--End--

Subscription export and import

Use the procedures in this section to transfer subscriptions between SIP DECT systems. You can import and export subscriptions on individual SIP DECT systems, and on multi site SIP DECT systems. In both cases, the export procedure creates an xml file that you then import on the target system. The system remains operational during export procedure.

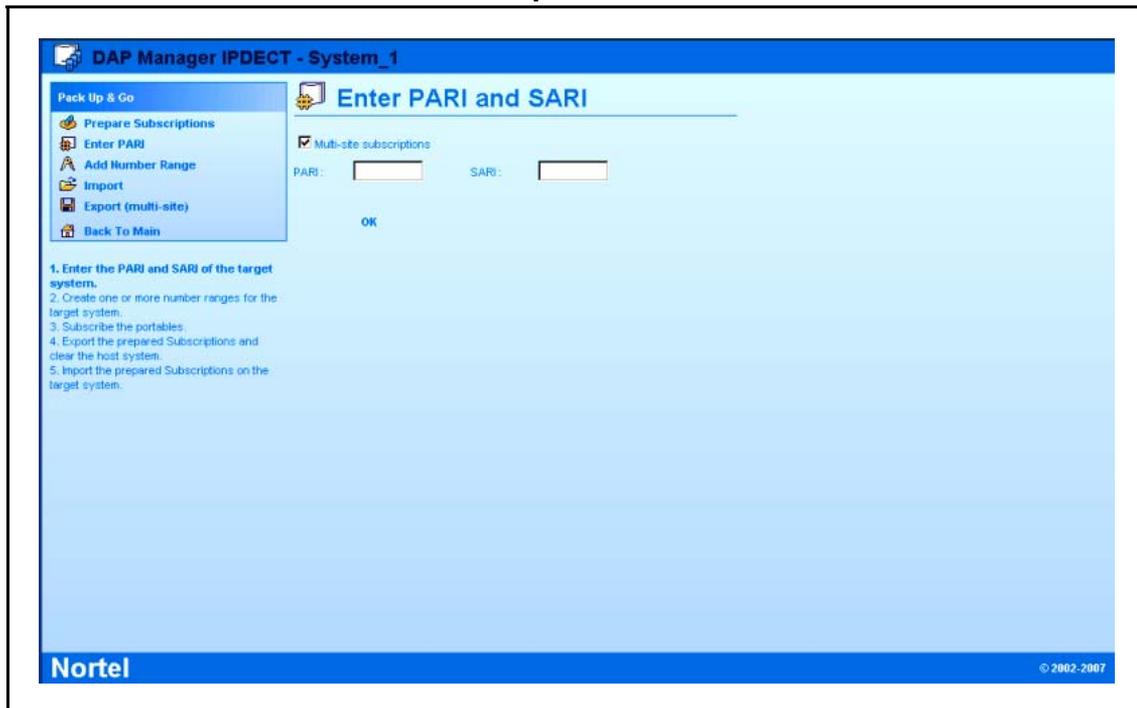
Export subscriptions

Prerequisites

- The PARI of the host system must be different from the PARI in the target system.
- The handsets to be subscribed must be within reach of the host radio signals.

Procedure 102 Exporting subscriptions

Step	Action
1	Open Internet Explorer and enter the following URL in the address field: localhost/cds . The DAP manager IP DECT page appears.
2	Click Pack Up & Go .



- 3 If you are exporting multi site subscriptions, select **Enable for Multi Site**.
- 4 Click **Enter PARI**.
For more information about MSMN, see [“Multi site mobility network configuration”](#) (page 175).
- 5 Enter the **PARI** of the system.

- 6 Click **OK**.
If you are exporting subscriptions to a single system, proceed to step 12.
- 7 Click **Enter SARI**.
- 8 Enter the SARI of the system.
The SARI of the home and remote systems must be the same.
- 9 Click **OK**.
- 10 Click **Add Number Range**.
The **Add Number Range** page appears.
- 11 In the **From** field, enter the first number in the range of DNs where you want to export subscription data.

If you are exporting data for one DN only, proceed to step 16.
- 12 In the **To** field, enter the last number in the range.
- 13 Click **OK**.
- 14 Click **Subscriptions**.
The Subscriptions page appears.
- 15 Select the required available extension number from the list on the Subscription page, for example, select 5001.

If the number you require does not show, select another page. The page number is displayed in the top and bottom rows of the subscriptions table.
- 16 Click **Enable**.

The status of the configuring subscription record changes from "Free" to "Enabled" and the Personal Identification Number (PIN) appears. A PIN is generated by the DAP manager on each subscribe operation and appears only while the subscription status is enabled.
- 17 Using the handset you are subscribing, access the **System configuration** menu, and choose **New system**.

See the User Guide for the handset for more information about accessing this menu, and other handset configuration information.
- 18 If the handset requests a Portable Access Rights Key (PARK) code, enter the **PARK** code.

You can find the PARK code on the left at the bottom of the page.

Note: A PARK code is required only if there are overlapping DECT systems in your location; if only one DECT system is available in your location, a PARK code is not required.

- 19** Enter the **displayed PIN code**.
- If you do not enter the PIN within 16 minutes, the subscription mode is terminated for that specific extension number, and you must begin the subscription process from the beginning.
- 20** Enter the **name of your SIP DECT system** and the **DN**.
- You can find the name of the system and the DN on the handset screen. The status of the configuring subscription record changes from "Enabled" to "Subscribed".
- 21** Click **Export (Prepared)**.
- The Export page appears.
- 22** Navigate to the folder where you want to store the file.
- 23** In the **Name** field, enter a name for the new file.
- 24** Click **OK**.

--End--

Import subscriptions

Prerequisites:

- All portables must be subscribed.
- For multi site subscriptions, all systems must have the same SARI.

Procedure 103 Importing subscriptions

Step	Action
1	Open Internet Explorer and enter the following URL in the address field: localhost/cds . The DAP manager IP DECT page appears.
2	Click Pack Up & Go .
3	Click Import . The Import page appears.
4	Navigate to the folder where the file to be imported is stored.
5	Select the file to be imported.
6	Click OK .

--End--

You must also configure the Communication Server 1000 system to which the SIP DECT system is connected. See [“Call server configuration” \(page 170\)](#) for more information.

DAP reboot history

Use the procedure in this section to review the log of DAP restarts. The information available through this procedure includes development data that is not readable. This information can be requested by the Nortel help desk if you experience certain types of problems with your SIP DECT system.

Procedure 104 Reviewing the DAP reboot history

Step	Action
1	Open Internet Explorer and enter the following URL in the address field: localhost/cds . The DAP manager IP DECT page appears.
2	Click History . The DAP Reboot History page appears.

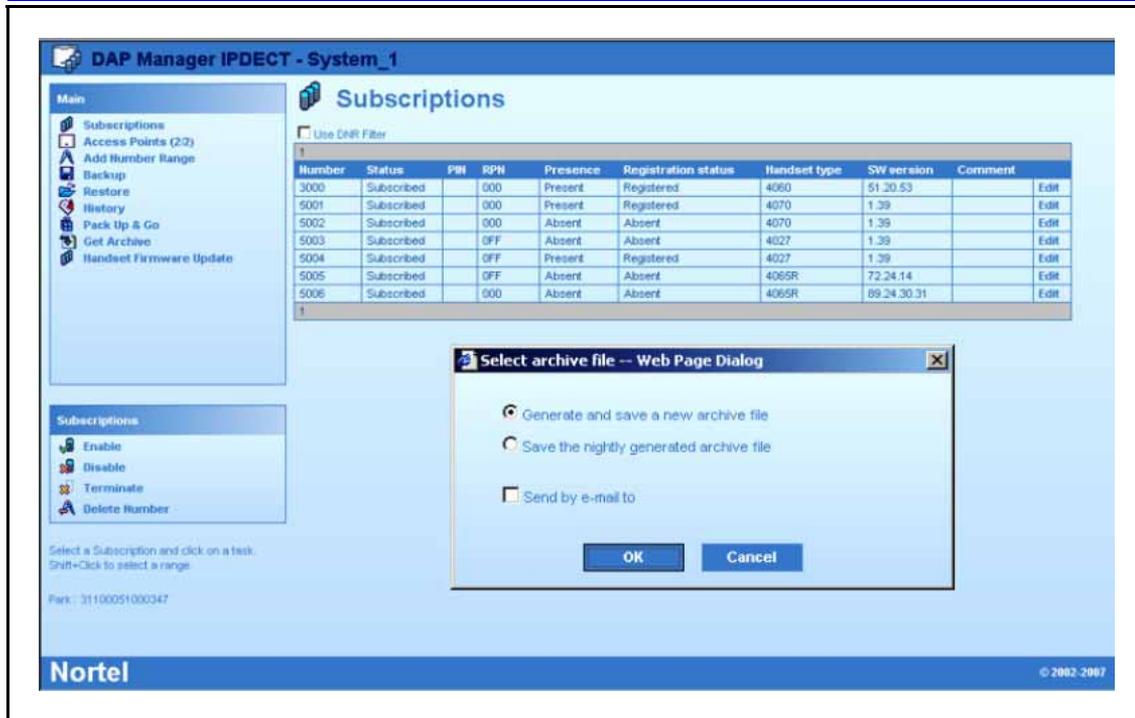
--End--

System archive

Use the procedure in this section to create an archive file containing various system settings, third line maintenance data, and performance data. This information can be requested by the Nortel help desk if you experience certain types of problems with your SIP DECT system.

Procedure 105 Creating a system archive

Step	Action
1	Open Internet Explorer and enter the following URL in the address field: localhost/cds . The DAP manager IP DECT page appears.
2	Click Get Archive . The Select archive file requester appears.



- 3 Select one of **Generate and save a new archive file** to create a new archive file.
OR
Save the nightly generated archive file to save a copy of the automatic archive, which is generated at midnight each day.
- 4 Click **OK** to go to the **File Download** page.
OR
Select the check box next to **Send by email to**, enter the email address to get the archive for each email and click **OK**. You need to configure the SMTP server before you use this feature. For more information, see [Procedure 53 "Configuring other settings—Performance/Email Settings"](#) (page 145).
- 5 Click **Save** on the **File Download** page.
- 6 Navigate to the folder where you want to store the archive file.
- 7 In the **Name** field, enter a name for the archive file.
- 8 Click **Save**.

--End--

Handset firmware update

You can install new firmware and software on the handsets using the Handset Firmware update option.

Note: Handset Firmware update is available only on handsets that support this feature.

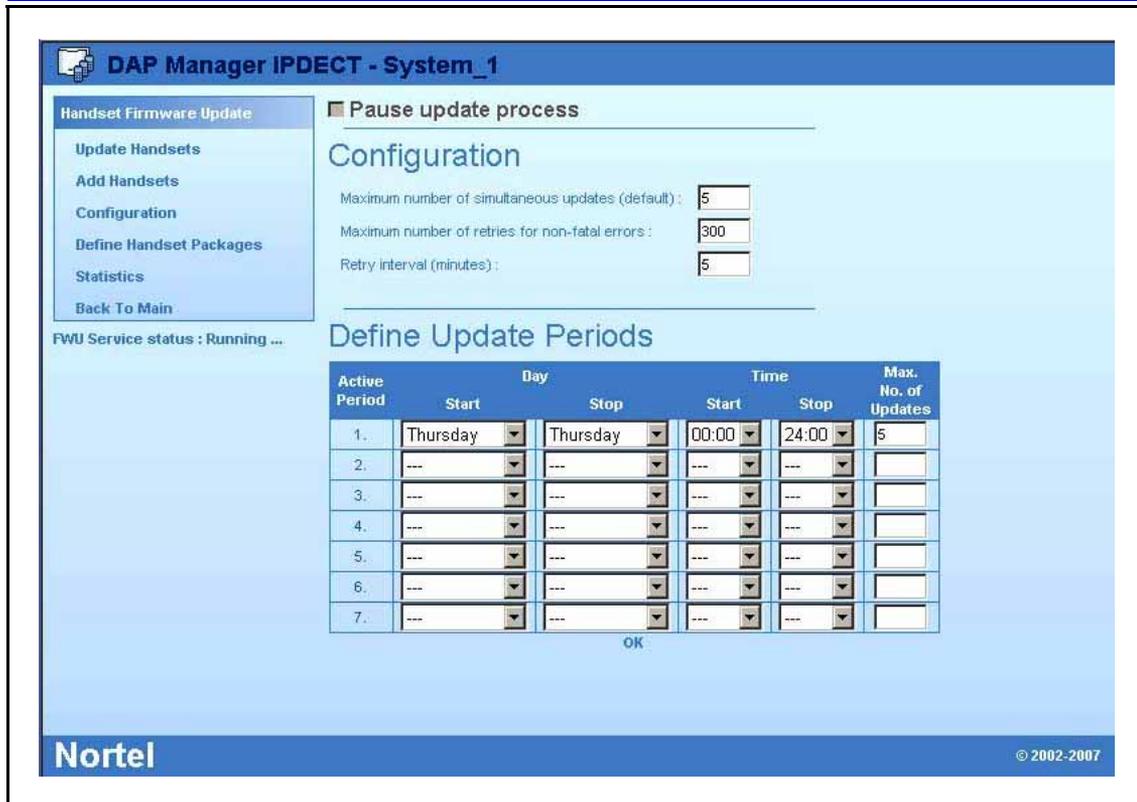
Go to the Define Handset Packages and see the list of handsets that allow firmware upgrading with this feature.

Note: The Firmware Upload service must be running. If the Firmware Upload service is not running, a qualified engineer must first start the service.

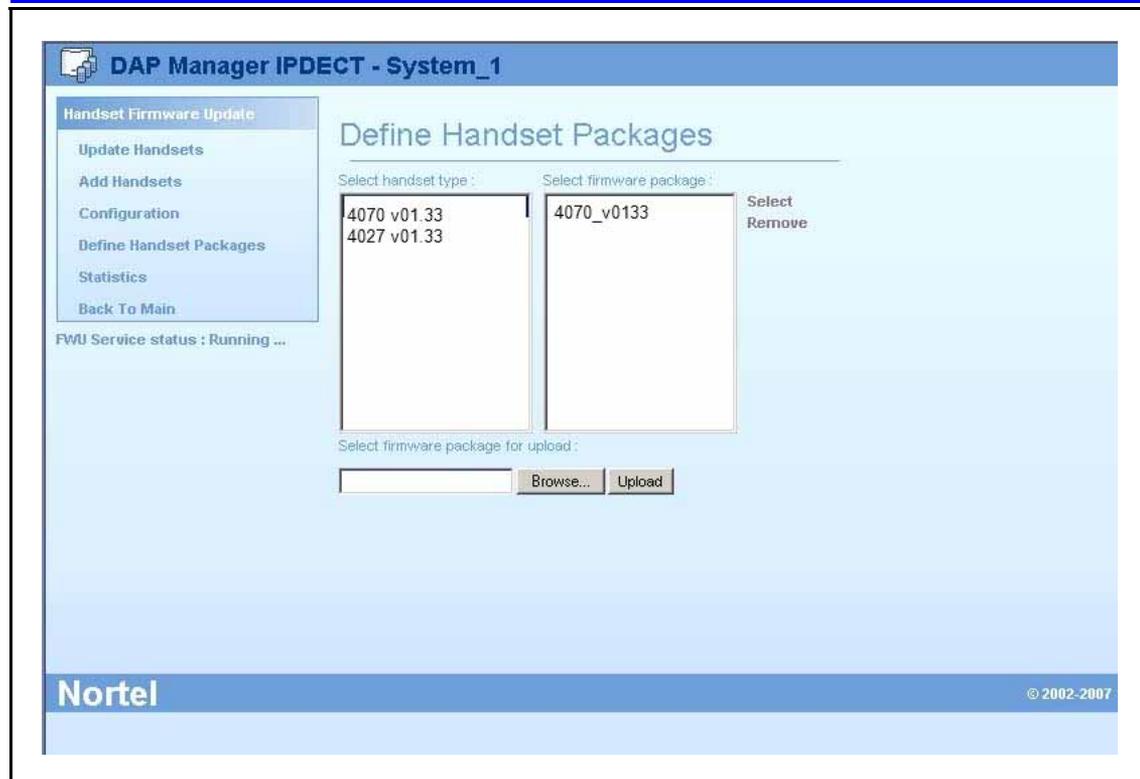
Use the steps in the next procedure to update the handset firmware.

Procedure 106 Updating the handset firmware

Step	Action
1	Click the menu Handset Firmware Update in the Main Window. The Handset Firmware Update window appears.
2	Click the menu option Configuration . The Configuration window appears.



- 3 Enter the following items.
 - Maximum number of simultaneous updates, the default setting, which is the maximum number of simultaneous updates that take place outside the periods you define in Define Update Periods.
 - Maximum number of retries for non fatal errors, which specifies the maximum number of retries for non fatal errors.
 - Retry interval, in minutes.
- 4 In the table Define Update Periods, specify the days of the week and the time period updates are to take place.
Nortel recommends that you let the system do the updating in the out-of-office periods. The handset functions during firmware updating, however firmware updating reduces the number of available channels on a radio.
- 5 Click **OK**.
- 6 Ensure the new firmware packet is available on the hard disk.
- 7 Click the menu option **Define Handset Packages**. The **Define Handset Packages** window appears.



8 In the **Select handset packages** window, select the handset type you want to provide with new software.

9 Browse to the new firmware package, for example, 4070_v0133.bin, and click **upload** .

The firmware filename must be in a specific format, for example, 4027_vXXXX.bin or 4070_vXXXX.bin, where XXXX is the firmware version.

Uploading means that the packet is visible in the right hand panel, and does not indicate an upload to the handsets is taking place.

10 On the left hand side next to the handset type the currently selected firmware version is displayed. Click the handset or package relation in the left hand panel to display the available firmware packages in the right column.

11 In the right hand pane, click the package and then click **Select**.

12 In the menu, click **Add Handsets**.

The **Add handsets** window appears.



13 Add the extension number range of the handset you want to involve in the firmware update in the **Add handsets** window.

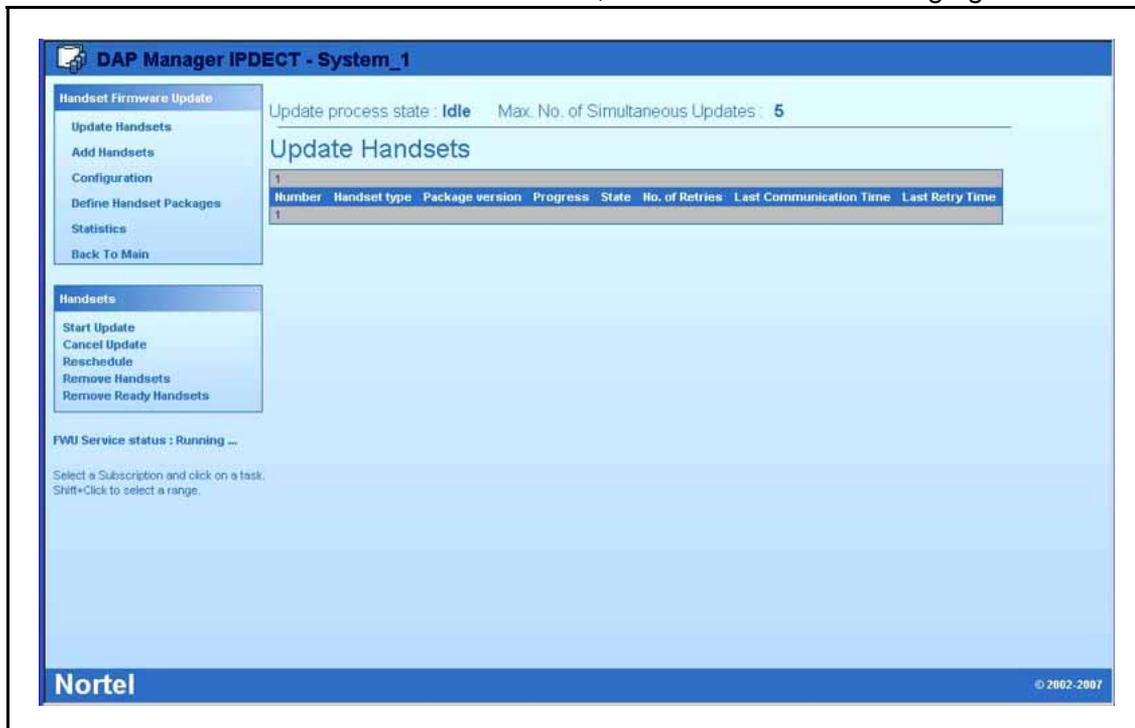
14 Click **OK**.

15 Click the **Update Handsets** menu.

A list of handsets involved in the update process appears.

16 Click **Start Update** in order to start the update process.

The update starts according to the time schedule you defined. The actual status of the update process appears in the **Update handsets** window, as shown in the following figure.



- After the update procedure is finished, the handset continues to use the old firmware packet.
- 17 When the update is complete, click **Remove Ready Handsets**.
- 18 To activate the new firmware, restart the handset.
There are two options in restarting the handset.
- If the handset is in the charger, the handset automatically executes a restart. No manual intervention needed.
 - If the handset is not in the charger and you want to activate the new software immediately, switch off the handset and switch it on again. After the handset switches over to the new firmware packet, the message *Firmware Update in progress. Do not switch off.* appears.
- 19 After the update process is finished, clean up the handsets list using one of the following menu items.
- Remove Handsets
 - Remove Ready Handsets
- 20 Click **Statistics** if you want an overview of the all actions that take place. A window appears.

--End--

Central directory access tool

The Central directory access tool connects a directory to the SIP DECT system.

Note: The Central Directory Access feature is available only for the handsets that support it.

After the Central directory access tool is installed, the tool consists of two services running under MS Windows. There is no user interface available. TCP/IP Port 30160 is open for external access from the IP DECT system.

IP DECT connects to the Central directory access tool through the TCP/IP socket that is defined in the DAP Configurator tool.

For access to the database, the handset type must support access to the database through the menu in the handset. If the handset does not offer a menu option to access the Central Directory, Central Directory cannot be used on that handset type. Consult your SIP DECT supplier to find out the handset types that support Central Directory dialling.

Supported database types

Nortel supports using Flat Excel database as a database type for a Central directory access tool.

Create an Excel file for the central database

You can create a simple Excel sheet containing your central database. During the installation of the Central directory access tool, specify the path to the Excel file and the file name.

To create an Excel file for the central database, follow the steps in the next procedure.

Procedure 107

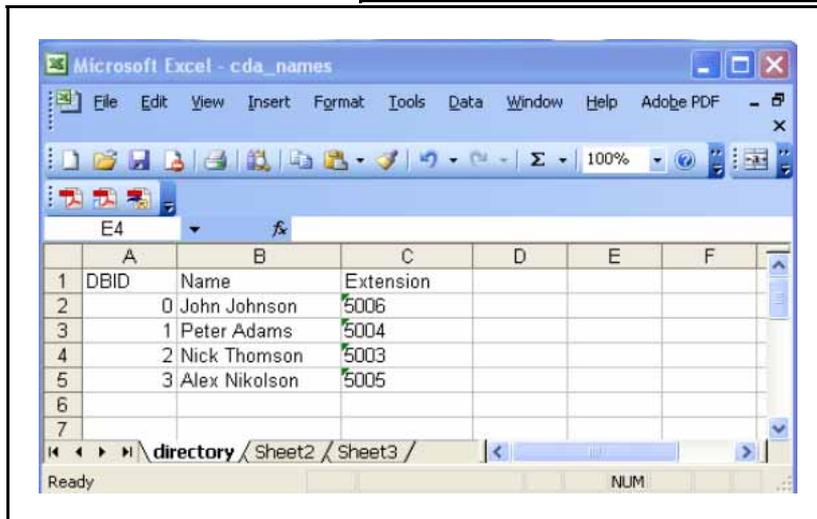
Creating an Excel file for the central database

Step	Action
------	--------

- | | |
|---|---|
| 1 | Open MS Office Excel |
| 2 | Add three columns as shown in the following figure. |

ATTENTION

It is important to use the column headers DBID, Name, and Extension. Also, take note that the first column contains sequence numbers and each number must be unique.



- | | |
|---|------------------------------|
| 3 | Add as many rows as entries. |
|---|------------------------------|

Note: If the number of entries in the spreadsheet is small (about 10), then you can see some of the entries more than once on the handset display while scrolling the list. This is normal.

- | | |
|---|--|
| 4 | Change the name of the Excel sheet from Sheet1 to directory. |
| 5 | Save the database, for example as cda_names.xls . |

After you update the file, it is immediately active in the Central directory access tool. Do not change the file name as you update the file.

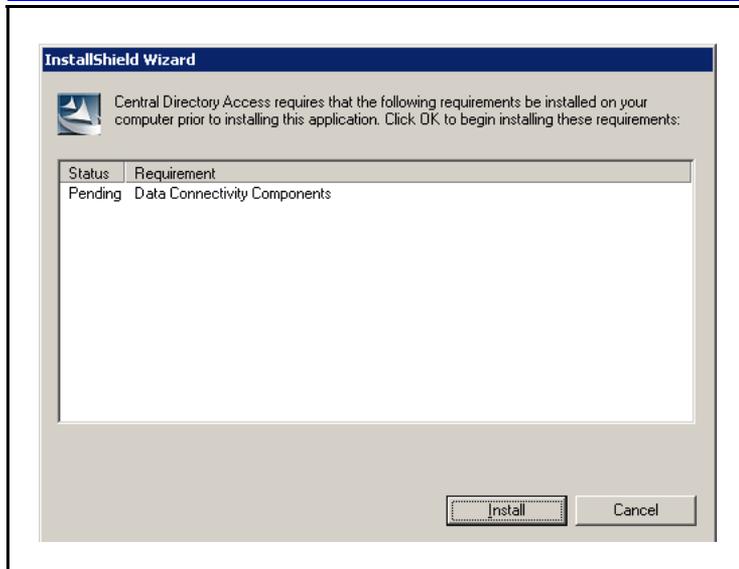
--End--

Installation

Use the steps in the next procedure to install the Central directory access tool.

Procedure 108 Installing the Central directory access tool

Step	Action
1	Ensure that the IP DECT Configurator is installed on the DAP controller PC.
2	Create an Excel file for the Central Database as described in Procedure 107 "Creating an Excel file for the central database" (page 209).
3	Check for the Central directory access tool software. The Central directory access tool software consists of a folder, called DISK1, containing a setup file.
4	Run the setup.exe file, and perform one of the following: If Microsoft Office Access database engine is available on your PC, the Central Director Access Startup window appears. Proceed to step 5. OR If Microsoft Office Access database engine is not available, you are prompted to install Microsoft Office Access database engine 2007. See the following figure.



Note: If you use the MS Windows 2000 Server, you are prompted to install Microsoft Data Access Components 2.8 instead of the Microsoft Office Access database engine.

Press Install and follow the instructions on the screen.

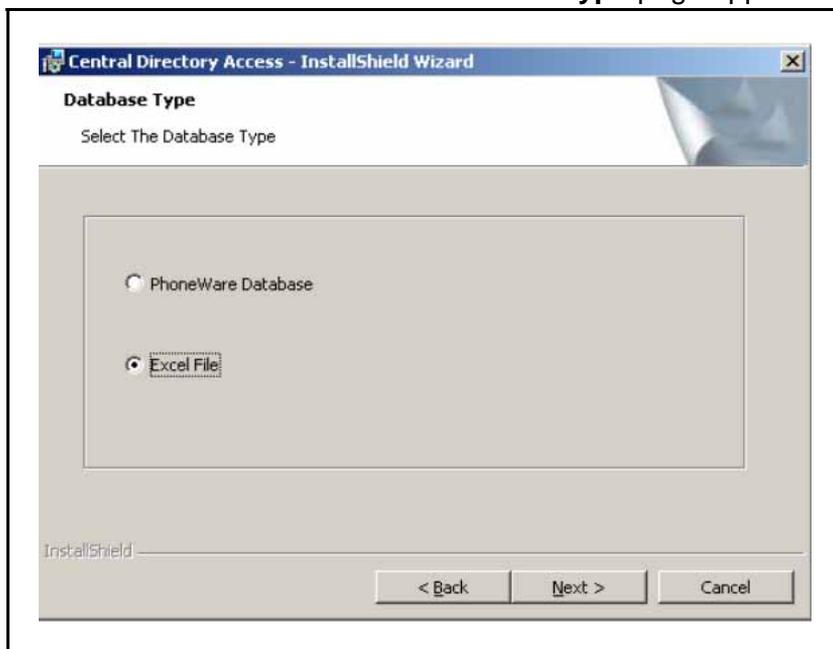
Note: If you use the MS Windows 2000 server, you are prompted to install Microsoft Data Access Components 2.8 instead of the Microsoft Office Access database engine.

After Microsoft Office Access database engine 2007 is installed on your PC, the **Install Shield** window appears.

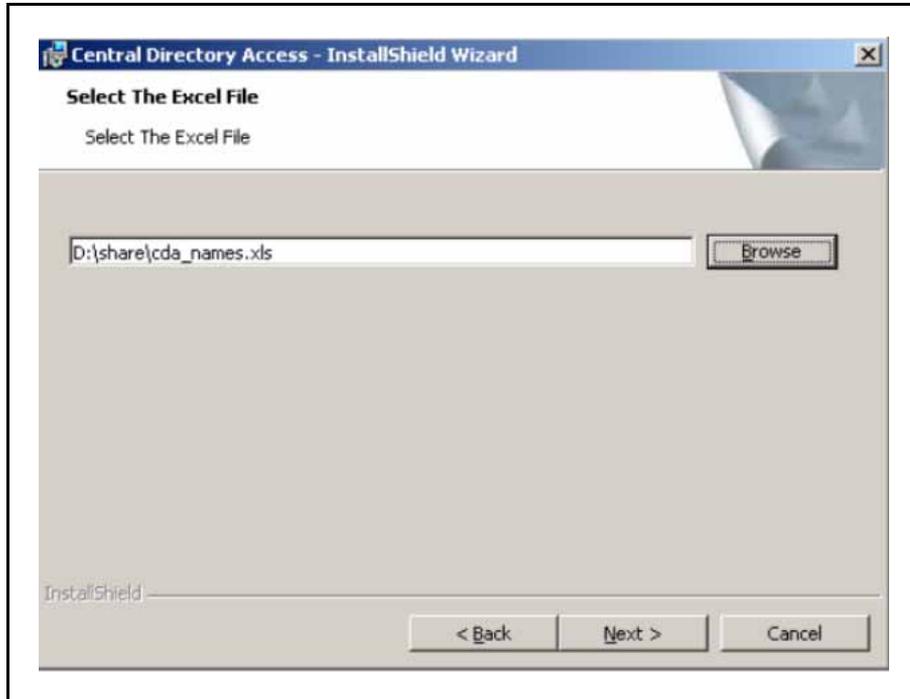
5

Click **Next**.

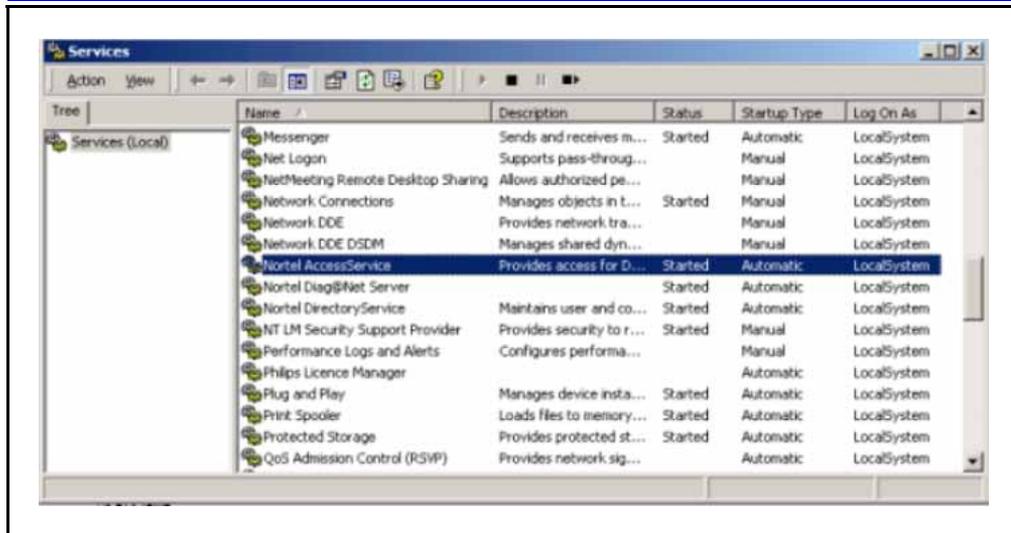
The **Database Type** page appears.



- 6 Select **Excel File** .
- 7 Click **Next**.
The **Select the Excel File** page appears.



- 8 Click **Browse**, and browse to the Excel file that contains the Central Directory data. click **Next**.
The **Ready to Install the Program** page appears.
- 9 Click **Install**.
The system installs the software. Once the installation is complete, the **InstallShield Wizard Completed** appears.
- 10 Click **Finish**.
As result of the installation, two new services are running, as shown in the following figure.
 - Nortel AccessService
 - Nortel DirectoryService



- 11 Ensure that **Nortel AccessService** and **Nortel DirectoryService** are present in the list, and have a Status of Started.

--End--

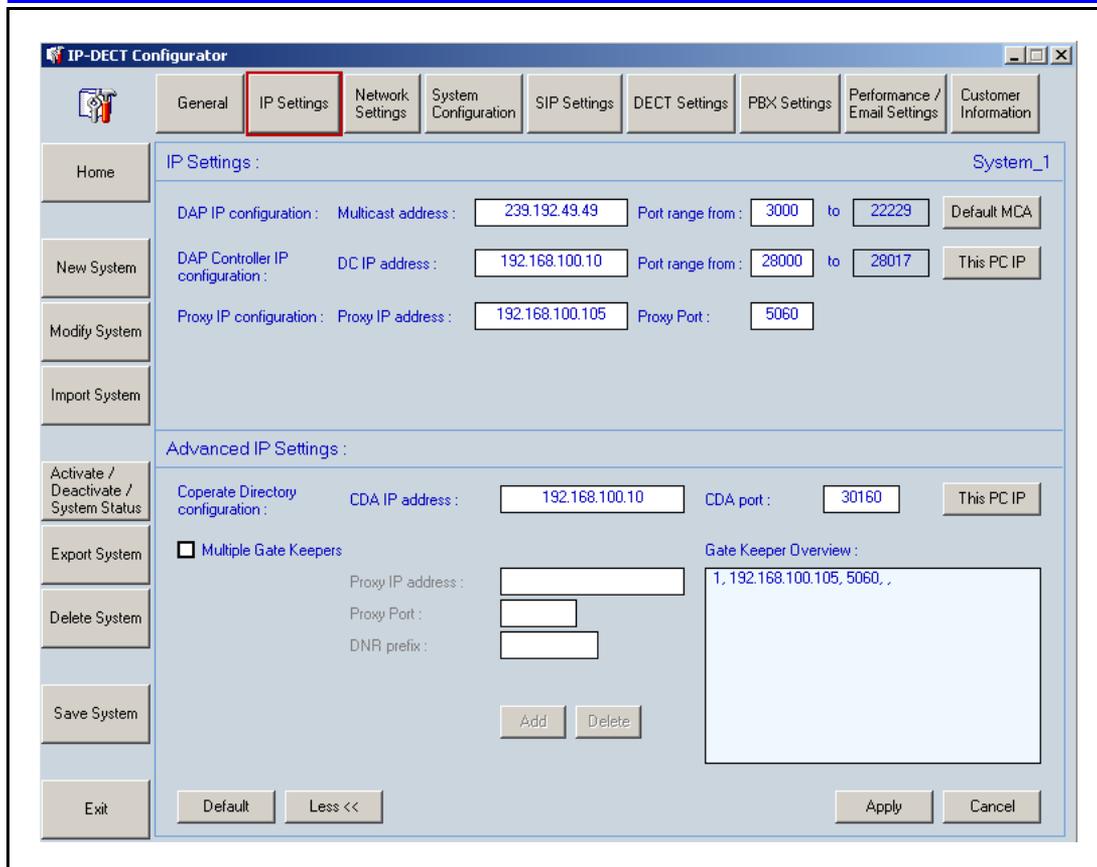
Configure SIP DECT for Central directory access

SIP DECT must be configured to reach the Central directory access services.

Use the steps in the following procedure to configure SIP DECT for using Central directory access.

Procedure 109 Configuring IP DECT

Step	Action
1	Open the DAP Configurator and click Modify .
2	Select the SIP DECT system that you are running. Click IP Settings , and then click More.. The IP Settings page appears.
3	Click More . The Advanced IP Settings pane appears.



4 Enter the **CDA IP Address** and the **CDA port**.

The IP address is the IP address of the computer running the Central directory access tool. The port number is the port that is open for Central directory access on the CDA computer. The default port number is 30160.

5 Click **Apply**.

6 Click **Save System**.

7 Click **Activate / Deactivate / System Status**.

8 Restart the DDS service and reboot all DAPs.

--End--

System maintenance

Navigation

This chapter contains information to help you perform system maintenance, such as replacing DECT Access Points (DAP) and managing DAP synchronization.

- [“DAP LED indications” \(page 215\)](#)
- [“Remove and replace a DAP \(if a new DAP is available\)” \(page 217\)](#)
- [“Remove and replace a DAP \(if a new DAP is not available at the moment\)” \(page 218\)](#)
- [“System synchronization analysis ” \(page 219\)](#)
- [“Export and import SIP DECT system” \(page 228\)](#)
- [“DAP Controller deactivation” \(page 230\)](#)
- [“DAP Controller software deinstallation” \(page 230\)](#)
- [“DAP Controller software update” \(page 231\)](#)
- [“Troubleshooting” \(page 232\)](#)
- [“If you have problems” \(page 236\)](#)

DAP LED indications

The DAP is equipped with one LED. The LED can indicate 6 different statuses of the DAP. The following indications may occur.

- Off No power.
- 0,5 seconds On - 0,5 seconds Off Loading software/firmware.
- Short flash every 0,25 seconds IP Network error (not connected, no DHCP/TFTP server, no DAP Controller)
- Fast blink DAP operational, but trying to synchronize to another DAP.
- Continuous fast blink Hardware error.
- Steady On DAP operational (and synchronized to other DAP or is the synchronization master).

DAP firmware update

Use the information in this section to load updated firmware to the DAPs.



CAUTION

Risk of service loss

You must update the firmware for all DAPs in the system at once. Ensure that all DAPs in the system are running and can be involved in the firmware update process.



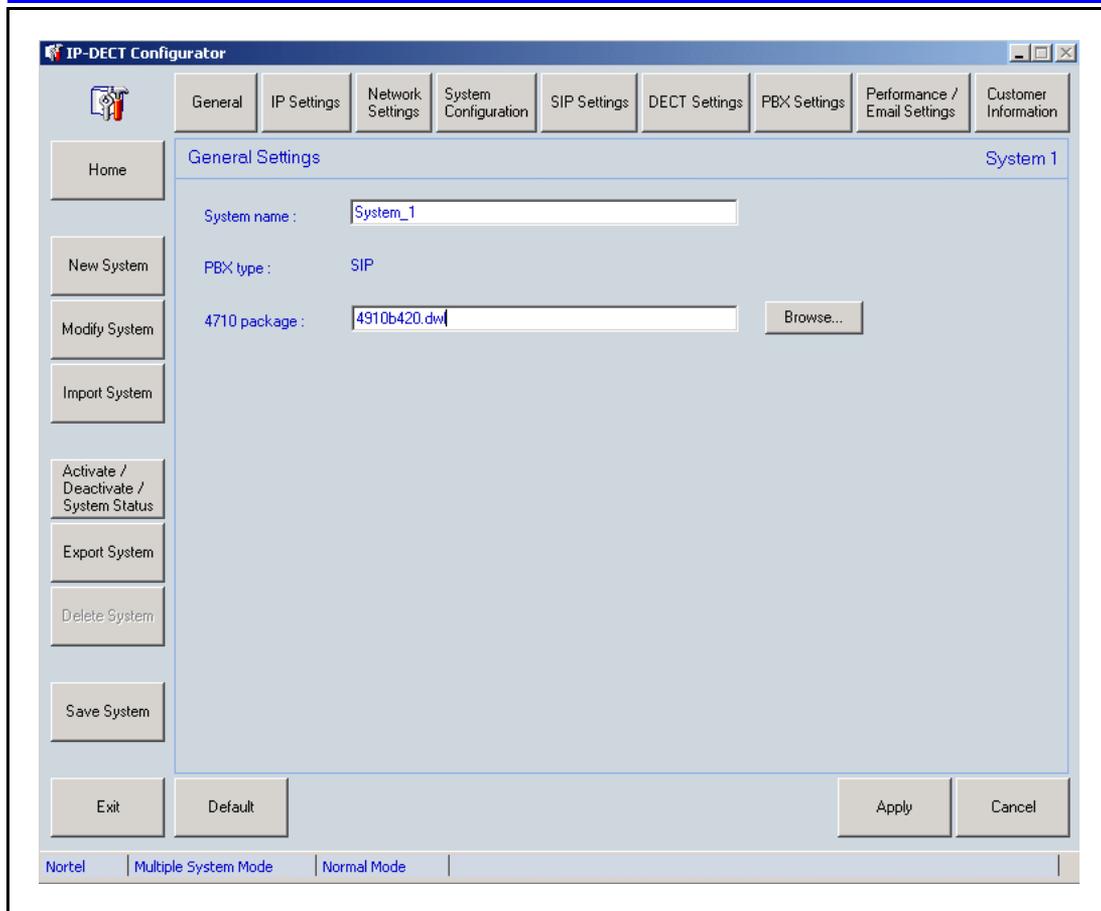
CAUTION

Service loss during restart

During the DAP firmware update, you must restart the DAPs. When you restart the DAPs, any DECT calls that are in progress are dropped, and the SIP DECT system is not available to handle calls until the DAPs finish restarting.

Procedure 110 Updating the DAP firmware

Step	Action
1	Launch IP DECT Configurator
2	In the IP DECT Configurator main window, click General .
3	If you have more than one DECT system configured in IP DECT Configurator, click Modify , and select the system you want to update.
	OR
	If you have only one DECT system configured, proceed to step 4.
4	In the General Settings window click Browse .
5	Browse to the folder where the new firmware (the DAP package file) is stored, select the DAP package file, and click Open . The new firmware information appears in the 4710 Package: field.



- 6 Click **Apply**.
- 7 Click **Save system**.
- 8 Click **Activate/Deactivate/System status**.
- 9 Ensure the DHCP and TFTP servers are running.
- 10 Click **Reboot** to restart the DAPs.
- 11 Enter the following URL in an internet browser:
localhost/cds.
The DAP Manager appears.
- 12 In the **Main** panel, click **Access Points**.
The Access Points page appears.
- 13 On the Access Points page, ensure the new firmware (Package ID) is uploaded successfully.

--End--

Remove and replace a DAP (if a new DAP is available)

To ensure that the newly installed DAP behaves in the same way as the replaced DAP, use the steps in the next procedure to replace a DAP.

Replacing a DAP

Step	Action
1	Ensure that DAP Manager is running before you begin to replace a DAP.
2	Ensure that the DHCP server and the TFTP server are running in the IP network.
3	Open the DECT Manager WEB interface.
4	Click Access Points .
5	Disconnect the DAP that needs to be replaced. Do not continue this procedure until DECT Manager indicates that the DAP is not working.
6	Connect the new DAP. Wait until you see that the new DAP is running (in the DECT Manager interface).
7	Click the Edit button for the new DAP.
8	Change the RPN number of the new DAP to the RPN number of the replaced DAP and click OK . The new DAP reboots. When the DAP is running again, it has the RPN of the replaced DAP. Now the subscriptions that were active in the replaced DAP are automatically installed in the new DAP. This can take a few minutes.
9	Check that the subscriptions of the replaced DAP are on the new DAP. Note: After the subscription records are placed in the new DAP, switch the handsets associated with these records off and on to make them operational again.
10	Check that you can make phone calls using the new DAP.

--End--

Remove and replace a DAP (if a new DAP is not available at the moment)

Use the procedures in this section to replace a DAP that has failed.

**Procedure 111
Replacing a DAP**

Step	Action
1	Open the DECT manager Web interface.
2	Click Access Points .
3	Physically disconnect the DAP that you want to replace.
4	From the DAP list in DECT manager, manually record the Radio Part Number (RPN) of the DAP you are replacing. Wait until the status of the DAP you are replacing changes to not working in the DECT manager Web interface.
5	In the DECT manager Web interface, select the DAP you are removing.
6	Click Delete to delete the DAP from the system. Wait while the system redistributes the subscription records stored on the DAP you are removing. The RPN of the DAP you are removing disappears from the Subscription page in the DAP manager, and is replaced by the RPNs of other DAPs.
7	Turn off each handset that had its subscription record stored on the DAP you are replacing.
8	Turn on each handset that had its subscription record stored on the DAP you are replacing. Each handset is now connected to another DAP.
9	When you get a new DAP, ensure that the DHCP server and the TFTP server are available in the IP network.
10	Connect the new DAP. Wait until the new DAP appears in the DAP list of the DECT manager.
11	In the DECT manager Web interface , click Edit .
12	In the RPN field of the new DAP, enter the RPN value you recorded after you removed the old DAP in step 4.
13	Click OK . The new DAP restarts. After it has restarted, verify that the new DAP has the RPN of the DAP you removed.
--End--	

System synchronization analysis

Use the information in this section to manually synchronize the DECT system, and eliminate possible synchronization problems.

An analysis tool called Synchronization Analyzer is available in the DAP Configurator. You can use the Synchronization Analyzer tool to generate a graphical overview of the synchronization structure in the system, and to calculate the best candidate for the synchronization master. You can also use it to detect potential problems in the synchronization structure.

Synchronization Analyzer provides the following.

- a hierarchical view of the DAP Synchronization using visibility files
- a three dimensional localization of DAPs using location files
- a Traffic Bearer Control file analysis, which you can use to trace what DAPs a handset has used during a call

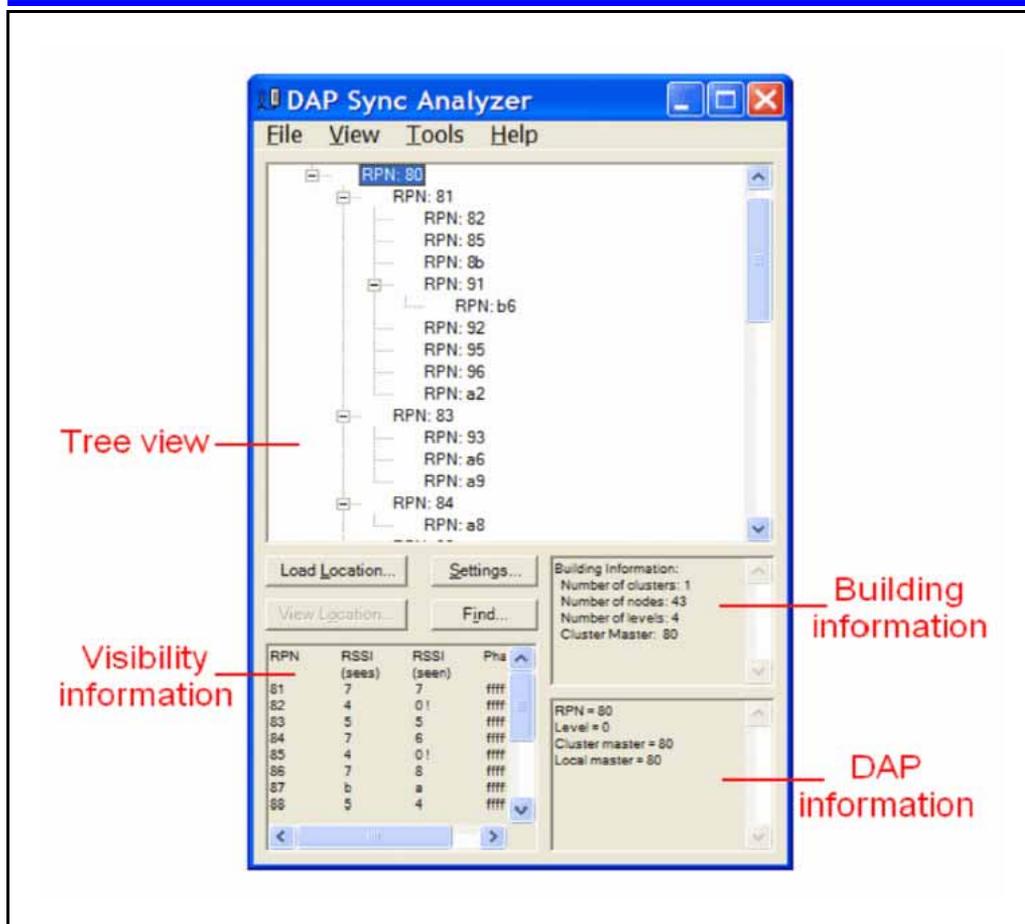
Synchronization Analyzer interface

This section provides an overview of the Synchronization Analyzer interface.

To access the Synchronization Analyzer, click **Start > All programs > DAP controller > DAP Applications > DAP Sync Analyzer**.

Synchronization Analyzer main page

The main page of the Synchronization Analyzer, as shown in the following figure, is composed of four panes.



- **Tree view**
The Tree view pane shows a hierarchical view of the synchronization tree. In the tree view, you can select a DAP.
- **Visibility Information**
The Visibility Information pane shows an overview of the RSSI values.
 - The RSSI (sees) column indicates the signal strength with which the selected DAP sees the other DAPs.
 - The RSSI (seen) column indicates the signal strength with which the other DAPs see the selected DAP.

Although the radio signal connection is reciprocal there can be differences in the seen and sees RSSI value. This difference is caused by the fact that this visibility information is based on a snapshot. The RSSI values are hexadecimal in the range: 0 ... e., , where 0 indicates no signal. The -80 dBm boundary is found at the boundary between approximately 3 and 4. Generally, the Phase difference must be ffffffff with a maximum deviation of 7 (higher or lower).

- Building Information
The Building Information pane shows overall data related to the DECT cluster.
- DAP Information
The DAP Information pane shows data of the selected DAP.

Table 32
Buttons on the Synchronization Analyzer main page

Button	Function
Load Location	Click Load Location to open a specific Location file.
View Location	Click View Location to open the Location page without specifying a Location file. See “Synchronization Analyzer Location page” (page 223).
Settings	Click Settings to open the Settings page, where you can enter the RSSI threshold and the Phase Difference threshold.
Find	Click the Find button to search the RPN number, the MAC address, or Info field of all the DAPs.

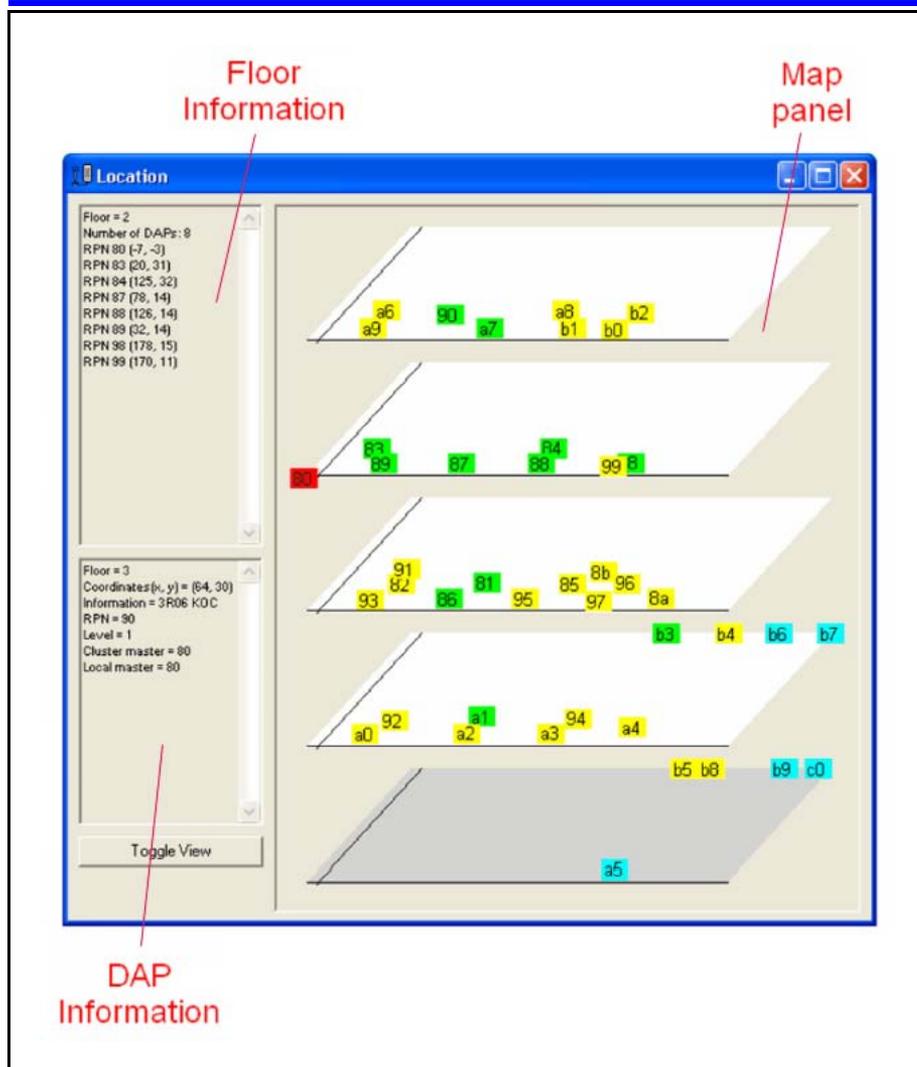
Table 33
Menus on the Synchronization Analyzer main page

Menu	Contains these options										
File	<ul style="list-style-type: none"> • Open Choose Open to open a Visibility File. • Compare Choose Compare to open a Visibility file and compare it with the current tree. One of the following symbols appears next to each DAP in the tree view. <table border="1"> <thead> <tr> <th>Symbol</th> <th>Meaning</th> </tr> </thead> <tbody> <tr> <td>+ Red</td> <td>The current level of an RPN is higher than the one in the compared file.</td> </tr> <tr> <td>- Red</td> <td>The current level of an RPN is lower than the one in file loaded for comparison.</td> </tr> <tr> <td>= Green</td> <td>The current level is the same as the compared level.</td> </tr> <tr> <td>X Red</td> <td>This DAP does not exist in the file that you loaded for comparison.</td> </tr> </tbody> </table> <ul style="list-style-type: none"> • Print Choose Print to send the Tree view to a printer. • Exit Choose Exit to exit from the program. 	Symbol	Meaning	+ Red	The current level of an RPN is higher than the one in the compared file.	- Red	The current level of an RPN is lower than the one in file loaded for comparison.	= Green	The current level is the same as the compared level.	X Red	This DAP does not exist in the file that you loaded for comparison.
Symbol	Meaning										
+ Red	The current level of an RPN is higher than the one in the compared file.										
- Red	The current level of an RPN is lower than the one in file loaded for comparison.										
= Green	The current level is the same as the compared level.										
X Red	This DAP does not exist in the file that you loaded for comparison.										

Menu	Contains these options								
View	<ul style="list-style-type: none"> • Problems Choose Problems to select the problem view, which is the default view. A number of potential problems, such as DAPs that can only synchronize with one other DAP, are defined within the program, and indicated in the tree view by an exclamation mark. • Synchronization Choose Synchronization to select the synchronization view, which shows the synchronization path of the selected DAP. One of the following symbols appears next to each DAP in the tree view. <table border="1" data-bbox="416 573 1383 753"> <thead> <tr> <th data-bbox="416 573 627 615">Symbol</th> <th data-bbox="627 573 1383 615">Meaning</th> </tr> </thead> <tbody> <tr> <td data-bbox="416 615 627 657">+ Blue</td> <td data-bbox="627 615 1383 657">The selected DAP sees this DAP.</td> </tr> <tr> <td data-bbox="416 657 627 699">+ Red</td> <td data-bbox="627 657 1383 699">The selected DAP is synchronized on this DAP.</td> </tr> <tr> <td data-bbox="416 699 627 741">+ Purple</td> <td data-bbox="627 699 1383 741">The selected DAP sees and synchronizes on this DAP.</td> </tr> </tbody> </table> <ul style="list-style-type: none"> • New Master Choose New Master to configure the currently selected DAP as cluster master in the tree view. • Best Master Choose Best Master to calculate what DAP is best suited to be the master. • Expand All Choose Expand All to expand all entries in the tree view. • Collapse All Choose Collapse All to collapse all entries in the tree view. • Location Choose Location to open a specific Location file in the Location page. • Settings Chose Settings to open the Settings page, where you can enter the RSSI threshold and the Phase Difference threshold. 	Symbol	Meaning	+ Blue	The selected DAP sees this DAP.	+ Red	The selected DAP is synchronized on this DAP.	+ Purple	The selected DAP sees and synchronizes on this DAP.
Symbol	Meaning								
+ Blue	The selected DAP sees this DAP.								
+ Red	The selected DAP is synchronized on this DAP.								
+ Purple	The selected DAP sees and synchronizes on this DAP.								
Tools	<ul style="list-style-type: none"> • Track Portable Choose Track Portable to open a traffic bearer file in the Portable Tracking page. 								
Help	<ul style="list-style-type: none"> • Help Choose Help to access Help features. 								

Synchronization Analyzer Location page

Use the Location page to display a visual representation of the locations of the DAPs in the system.



On the Location page, the color used to display each DAP indicates its synchronization level, as follows.

- Red = root level
- Green = first level
- Yellow = second level

After the location information is loaded into the tool from a file a Location file, the DAP positions are shown on each floor. Select a floor, or an individual DAP, and information appears to the left of the selection.

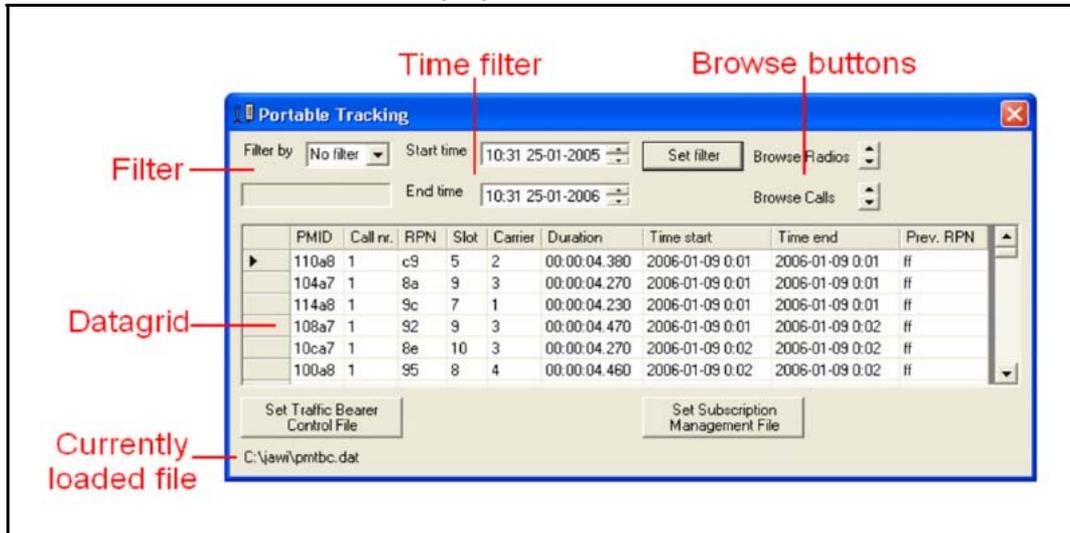
After a DAP is selected, other DAPs that the selected DAP can communicate with change color, and the corresponding node in the tree view is highlighted.

The following controls are available.

- Double-click on the map panel, or click Toggle View, to zoom in on a single floor.
- right-click on the map pane to access a menu of zoom controls.

Synchronization Analyzer Portable Tracking page

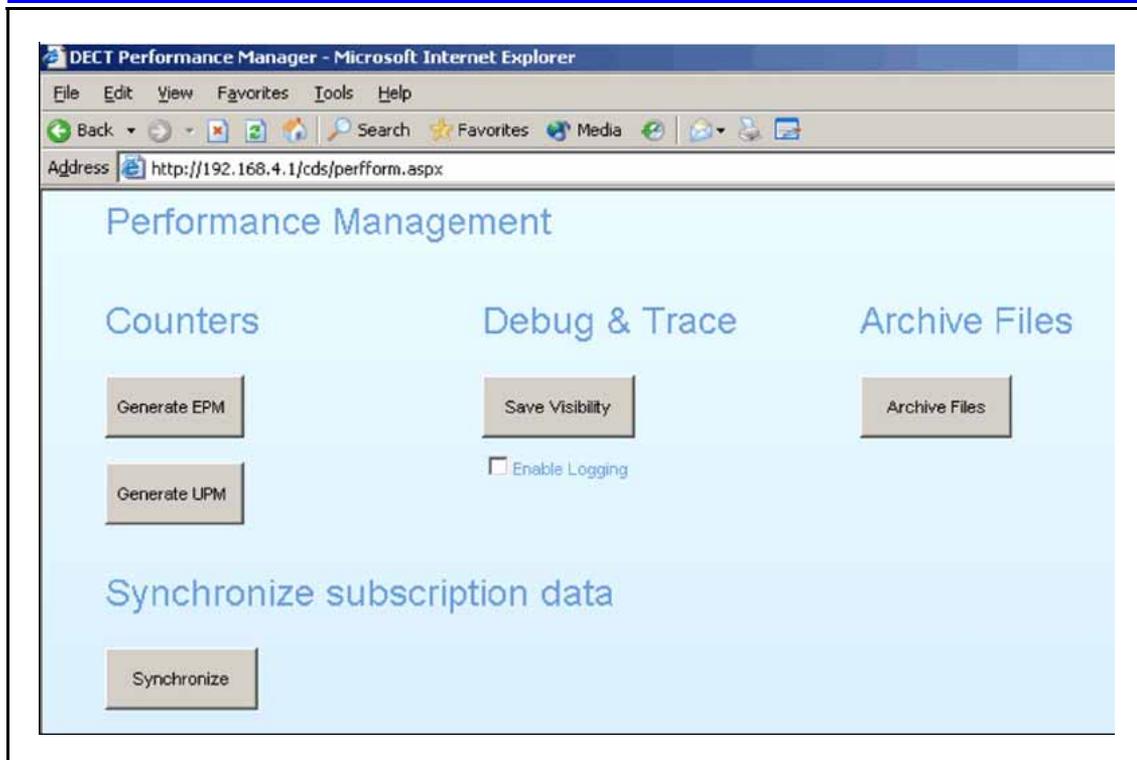
Use the Portable Tracking page to follow the movement of a portable device from DAP to DAP. A portable device can be tracked only if it is in an active call. For an illustration of the parts of the Portable Tracking page see the following figure.



Use the procedures in this section to analyze DAP synchronization and track portable devices in the system.

Procedure 112
Tracking a portable device

Step	Action
1	Click Start > All programs > DAP controller > DAP Applications > IPDECT Performance Manager to open the DAP Performance Management Interface.

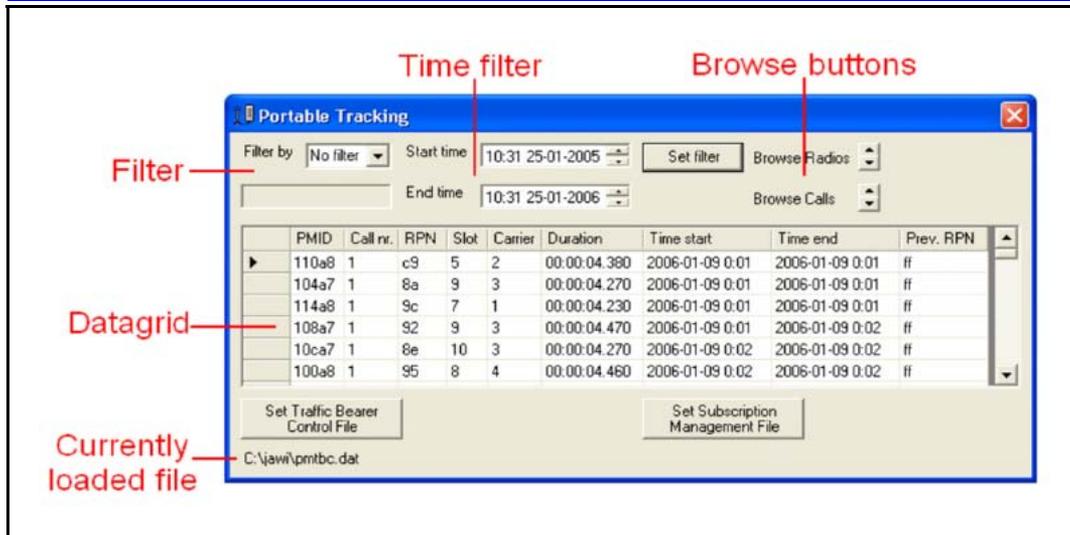


- 2 Select the check box for **Enable Logging**.
The file pmtbc.dat is generated, containing Traffic Bearer Control information.

ATTENTION

You need to disable logging when you finish the activities related to the system synchronization analysis.

- 3 Click **Start > All programs > DAP controller > DAP Applications > DAP Sync Analyzer**.
- 4 Choose **Tools > Track Portable** from the menu.
A file requestor appears.
- 5 Navigate to the directory **C:\..\IPM** on the DAP controller or manager PC, and choose the file **pmtbc.dat**.
The **Portable Tracking** page appears.



- 6 Click **Set Subscription Management File**.
A file requester appears.
- 7 Navigate to the directory **C:\.\IPM** on the DAP controller or manager PC, and choose the file **sm.xml**.
This file contains the relations between the PMIDs to the Extension numbers. After this file is loaded, an extra column appears in the data pane, providing the extension number.
- 8 Use the **Set Filter** and the **Browse** buttons to filter the data that is displayed in the window.

--End--

Table 34
Procedure job aid

Filter buttons	Description
Set filter Filter by Start time End time	Click Set Filter to apply a filter to the information that appears in the data pane.
Browse Radios Browse Calls	Click the Browse buttons to browse between different calls or radios.

Procedure 113
Using DAP Synchronization Analyzer

Step	Action
1	Click Start > All programs > DAP controller > DAP Applications > DAP Sync Analyzer .
2	In the menu, choose File > Open . A file requestor appears.

- 3 Select the file **visadm.txt**, and click **Open**.
- 4 Use the options in the menu **View** to analyze the synchronization structure.
- 5 Optionally, use the menu options under the menu **View** to trouble shoot the structure.
- 6 Optionally, load a location file. The location file contains a site map with buildings and floors in which the DAPs are positioned. Use the site map to quickly determine the position and range of a specific DAP. You can create a Location file using the Location Builder tool. See "[Location builder tool](#)" (page 239).
- 7 Optionally, load a Traffic Bearer Control (pmtbc.dat) data file. This file contains statistics/logging on traffic bearers. To open this file, choose **Tools > Track Portable**. A file requestor appears.
- 8 Navigate to the directory **C:\.\PM** on the DAP controller or manager PC, and choose the file **pmtbc.dat**. The data from the TBC file is presented in a table, and the PMID of each portable appears.
- 9 Navigate to the directory **C:\.\PM** on the DAP controller or manager PC, and choose the file **sm.xml**. An extra column appears in the data pane, providing the extension number.

--End--

Export and import SIP DECT system

You can use the IP DECT Configurator to export your system to another computer or to save the configuration as a backup copy.

After you execute an Export System, all the relevant system settings, including all customer data, are exported to a compressed or zip file. If you want to return to this configuration, you can easily import the compressed file and then your entire system configuration including customer data, such as handset subscriptions, is back again on your DAP controller or manager PC.

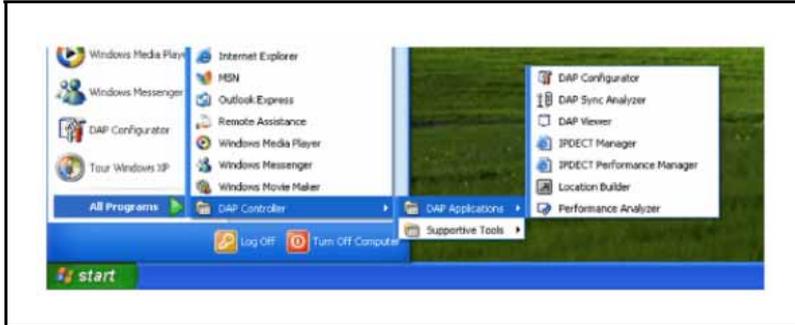
Export a system

Use the steps in the next procedure to export a system configuration.

Procedure 114 Exporting a system configuration

Step	Action
------	--------

- | | |
|---|--|
| 1 | Start the DAP configurator tool. Click Start > All programs > DAP controller > DAP Applications > DAP configurator as shown in the next figure. |
|---|--|



The DAP Configurator tool appears.

- | | |
|---|--|
| 2 | Click the button Modify system and select the system to export. |
| 3 | Click Export system . |

Use the window that appears to store the file on a location of your choice and specify a file name.

--End--

Import a system

Use the steps in the next procedure to import a system configuration.

Procedure 115 Importing a system configuration

Step	Action
------	--------

- | | |
|---|---|
| 1 | Click Start > All programs > DAP controller > DAP Applications > DAP configurator .
The IP DECT configurator window appears. |
| 2 | Click Import System . |
| 3 | Browse to the file that contains the system you want to import. |

--End--

DAP Controller deactivation

You can use the DAP Controller to configure the SIP DECT system. In addition, as long as the DAP Controller is connected and active, it can perform the following functions:

- Process messaging (Low Rate Messaging and interaction with DECT Messenger).
- Move subscriptions from a DAP that is not working to working DAPs. After a DAP is unavailable for 15 minutes, the system considers it to be not working.
- Monitor the SIP DECT system and send archives and alarms by email.

After you have configured the SIP DECT system using the DAP Controller, you can perform either of the following:

- Leave the DAP Controller PC connected and active, so that it performs all the functions listed above, and you can use it at any time to configure the SIP DECT system.
- Deactivate the DAP Controller software. You can then use the DAP Controller PC for other purposes, and if necessary you can disconnect it from the network completely. You can reactivate the DAP Controller software at any time to configure the SIP DECT system.

If you choose to disconnect your DAP controller PC from the network, you must first complete the following procedure to deactivate SIP DECT services.

Procedure 116 Deactivating SIP DECT services

Step	Action
1	Launch DAP Configurator
2	In the IP DECT Configurator main window, click Activate/Deactivate/System Status .
3	Click Deactivate All to stop all enabled services and programs.
4	Once the system is deactivated, click Exit .

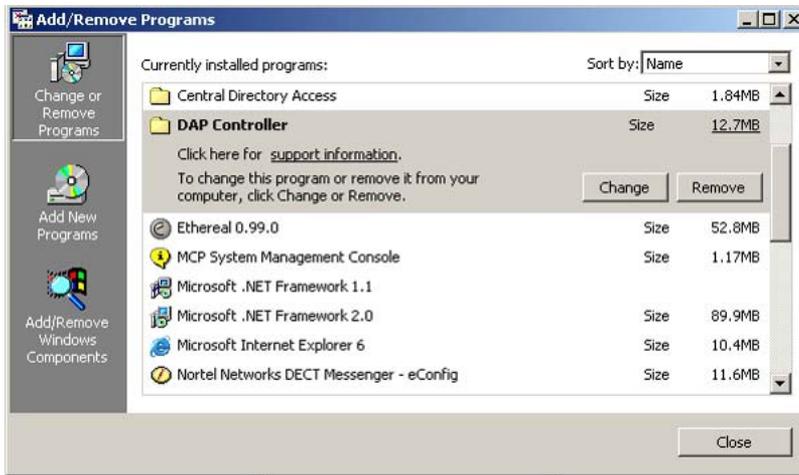
--End--

DAP Controller software deinstallation

If you need to remove the DAP Controller software, use the steps in the following procedure.

**Procedure 117
Uninstalling DAP Controller software**

Step	Action
1	Start the DAP Configurator tool . Click Start > All programs > DAP controller > DAP Applications > DAP configurator .
2	Click Activate/Deactivate/System Status .
3	Click Deactivate all .
4	Close the DAP configurator tool.
5	Click Start > Settings > Control Panel .
6	Double-click Add/Remove Programs .



7	Find DAP Controller in the list of the installed programs in the section Change or Remove programs . See the previous figure.
8	Click Remove .
9	Click Yes to confirm DAP Controller de-installation.

--End--

DAP Controller software update

If you have downloaded a new version of the DAP Controller and you need to update the current version, follow the steps in the next procedure.

Updating the current version of the DAP Controller

Step	Action
1	Export the current system.

- See “Export a system” (page 228).
- 2 Uninstall the DAP Controller.
See “DAP Controller software deinstallation” (page 230).
- 3 Install a new version of the DAP Controller.
See “DAP Controller” (page 130).
- 4 Import the system you exported.
See “Import a system” (page 229).
- OR
- Create a new system if required. See “Configuration of settings using IP DECT Configurator” (page 136).

--End--

Troubleshooting

The Troubleshooting section provides settings you can check to resolve some common configuration problems.

If DAP is not working Prerequisites

1. The signaling server, call server, and DAP Controller are configured and connected to the Ethernet.
2. The SIP DECT system is configured in the IP DECT Configurator.

If DAP is not working, ensure that the DHCP and TFTP servers are configured and running.

If you use the **MS Windows DHCP Server**, ensure:

- the **scope** is created
- the **IP address range** is added
- the **scope options** are configured
- the scope is **activated**
- MS Windows DHCP Server is **running**

If you use the **MS Windows TFTP Server**, ensure:

- the check box next to **Run TFTP Server on this PC** is checked
- **Windows TFTP Server on this PC** is selected

- MS windows TFTP Server (Trivial FTP daemon) is **running**
- **dapcfg.txt** and **DAP firmware package** are presented in the **C:\TFTPDROOT** folder

If you use a **built-in DHCP Server**, ensure:

- the check box next to **Run DHCP Server on this PC** is checked
- the **DAP IP range** is entered
- the **DAP IP Range exclusive for DAPs only** is selected
- the **Subnet Mask** is entered
- the **Default gateway** is entered
- the **TFTP IP address** (of the DAP Controller PC) is entered
- the DHCP Server is **running** (Activate/ Deactivate/ System status button)

If you use **built-in TFTP Server (IP DECT Configurator)**, ensure:

- the check box next to **Run TFTP Server on this PC** is checked
- **3com TFTP Server on this PC** is selected
- TFTP Server is **running** (Activate/ Deactivate/ System status button)

See [“DHCP and TFTP servers” \(page 111\)](#) for details.

If you cannot make calls from a DECT handset to an IP/TDM telephone on the call server

Prerequisites

1. The signaling server, call server, and DECT system are configured and connected to the Ethernet.
2. The DAPs are working.

If you cannot dial an IP/TDM telephone on the call server, verify the following:

- Ensure that a dial tone sounds if a handset goes off-hook
- Ensure that the DECT handset is subscribed. For more information, see [“DAP manager configuration” \(page 150\)](#).
- For DAP Manager:
 - Ensure that DAPs are loaded with correct parameters (see Viewing DAP configuration information).
- For IP DECT Configurator:

- IP Settings window – Ensure that **Proxy IP address** = SIP Gateway Signaling Server node IP address.
See [Procedure 48 “Configuring IP Settings” \(page 139\)](#) for details.
- SIP Settings Window – Ensure that **Predefined SIP server configuration** = Nortel
- SIP Settings Window – Ensure that **SIP domain** is entered
See [Procedure 51 “Configuring SIP Settings” \(page 141\)](#) for details.
- For Call Server:
 - Ensure that **D channel X** is configured and active
See [Procedure 62 “Adding a D-Channel” \(page 156\)](#) for details.
 - Ensure that **Route Y** for **D-CH X** is configured properly
See [Procedure 63 “Adding a route” \(page 156\)](#) for details.
 - Ensure that **Virtual trunks** are added to **Route Y**
See [Procedure 64 “Adding a trunk” \(page 157\)](#) for details.

If you cannot make calls between DECT handsets

Prerequisites

1. The signaling server, call server, and DECT system are configured and connected to the Ethernet.
2. DAPs are working
3. It is possible to make a call from a DECT handset to an IP/TDM telephone on the call server.

If you cannot establish a call between two DECT handsets (see [Figure 53 “Call flow for a call from DECT handset to DECT handset” \(page 236\)](#) for a simplified call flow), ensure the following are properly configured.

Call server

1. **Digit Manipulation Block A** (no digits to delete). See [Procedure 67 “Adding digit manipulation block” \(page 159\)](#) for details.
2. **Route List Block B** is configured for **Route Y** and **DMI A**. See [Procedure 68 “Adding route list block” \(page 159\)](#) for details.
3. UDP - **Location code (RLI B** is entered, **FLEN** is equal to sum of the digits in LOC and DN). See [Procedure 69 “Adding location code \(for UDP\)” \(page 160\)](#) for details.

4. CDP – **Trunk Steering code (RLI B** is entered, **FLEN** is equal to sum of the digits in TSC and DN). See [Procedure 70 “Adding Trunk Steering Code \(CDP\)” \(page 160\)](#) for details.

5. **PCA** is **on** and **UEXT** is configured as follows:

— UXTY SIPN

— KEY 0 SCR <DN>

— KEY 1 HOT P <number of digits> <AC><LOC><DN> (if UDP)

OR

KEY 1 HOT P <number of digits> <TSC><DN> (if CDP)

where DN is the local number of the DECT handset subscribed in the DAP Manager. See [“Call server configuration” \(page 170\)](#) for details.

- SIP GW setting - **Primary Proxy or Redirect (TLAN) IP address** = NRS IP address

See [Procedure 71 “Configuring the signaling server” \(page 161\)](#) for details.

- Signaling Server – the check box for **Enable SIP Proxy / Redirect Server** is checked when SIP Gateway and Redirect Server (NRS) are co-resident Signaling Server – **SIP Domain name** = domain name configured in IP DECT Configurator.

See [Procedure 72 “Configuring SIP properties” \(page 162\)](#) for details.

- **Service domain** name is the same as SIP domain, configured on the signaling server and the IP DECT Configurator.

See [Procedure 75 “Creating service domain” \(page 165\)](#) for details.

- **UDP** and **CDP** domains are configured correctly.

See [Procedure 76 “Adding the UDP domain” \(page 165\)](#) and [Procedure 77 “Adding the CDP domain” \(page 165\)](#) for details.

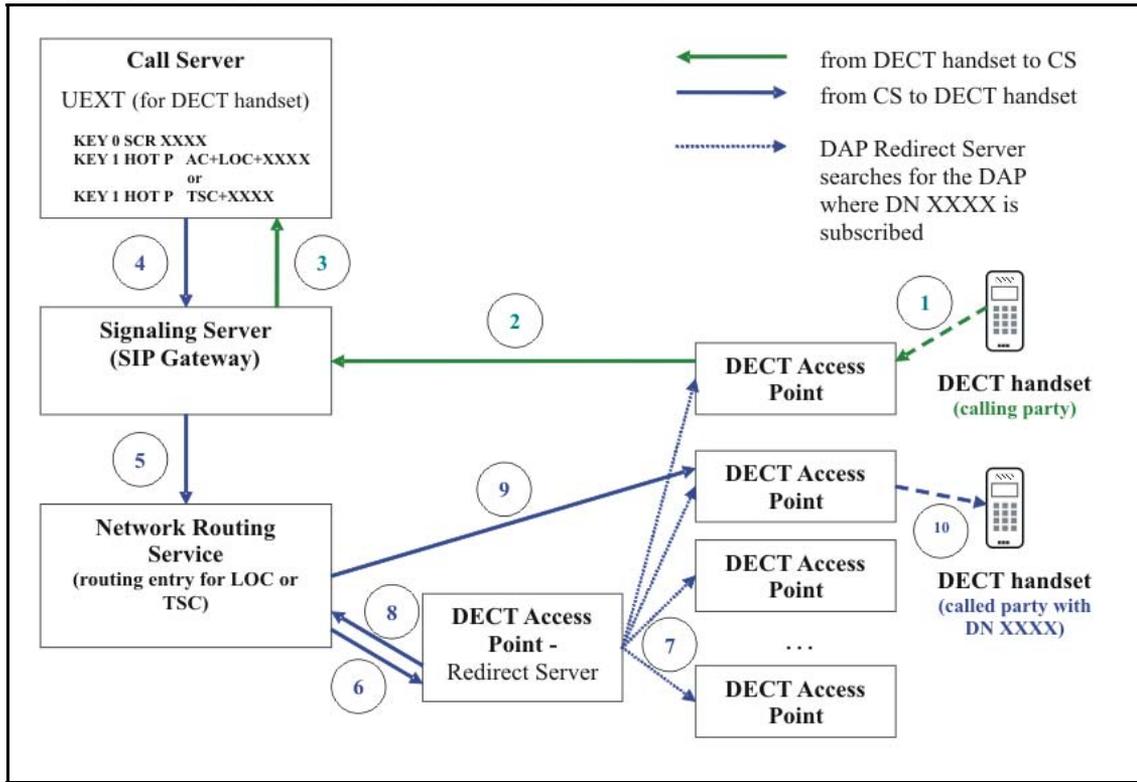
- **Gateway endpoints** for DAP and the signaling server are created.

See [Procedure 78 “Adding Gateway Endpoint for the signaling server” \(page 166\)](#) for details.

- **Routing entries** for UDP or CDP (equal to LOC or TSC) are added for Gateway endpoint for DAP.

See [Procedure 79 “Adding Gateway Endpoint for DAP redirect server” \(page 167\)](#) for details.

Figure 53
Call flow for a call from DECT handset to DECT handset



If you have problems

If you have problems with your SIP DECT system, first review “[Troubleshooting](#)” (page 232). The Troubleshooting section lists and describes the settings you can check to resolve some common configuration problems. If you cannot resolve the issue, collect the necessary information including a system survey, system archive, and network traces. Describe the issue and contact the Nortel helpdesk.

System survey

Complete a system survey for your SIP DECT configuration. Provide the information outlined in the following sections to describe your hardware, IP addresses, software version, configuration, and numbering plan. If you have problems with your SIP DECT system, send your completed system survey with the system archive to the Nortel helpdesk.

Hardware

- Signaling server:
- Call server:
- Number of DAPs:

IP addresses

- Signaling server (Node IP):
- Network routing service:
- DAP redirect server:
- DAP Controller PC:
- DHCP server (if different from DAP controller PC):
- TFTP server (if different from DAP controller PC):

Software version

- Call server release:
- MS Windows (installed on DAP Controller PC):
- DAP controller software:
- DAP firmware package:
- Central Directory access tool (if any):

Configuration

- Single or multiple system (as selected during DAP controller software installation):
- Simple or Routed Head Quarter, or MSMN:
- MS Windows or built-in DHCP server:
- MS Windows or built-in TFTP server:

Numbering plan

- CDP or UDP:
- TSC or LOC used for SIP DECT:
- Number range for SIP DECT handsets:
- Twinned configuration is used or not:
- Call Pilot is used or not:

System archive

The System archive contains important information about your SIP DECT system and must always be sent to the Nortel helpdesk if any problems occur. See [“System archive” \(page 202\)](#) to learn the procedure of creating an archive.

Note: You can be requested by the Nortel helpdesk to temporarily enable logging for your SIP DECT system before testing a specific call scenario. See steps 1 and 2 of [Procedure 112 “Tracking a portable device” \(page 225\)](#) for details. Enabling logging before testing a specific call scenario adds extra information to the system archive.

Network packet capture traces

You can be asked to collect network traces if some call scenario fails on your SIP DECT system. Traces contain SIP messages and RTP packets sent over the Ethernet. Traces can be collected from a computer connected to the network (when hubs are used or if port mirroring is configured on IP switches). In some cases, it is possible to trace SIP messages from Signaling Servers. The Nortel helpdesk can guide you on collecting network traces if you need assistance.

Note: You can be requested by the Nortel helpdesk to temporarily enable logging for your SIP DECT system before capturing traces for a specific call scenario. See steps 1 and 2 of [Procedure 112 “Tracking a portable device” \(page 225\)](#) for details.

Appendix

Location builder tool

The Location Builder tool is used to create a site map within buildings and inside the building floors and, if necessary, lines to indicate contours or anything else that you want to draw.

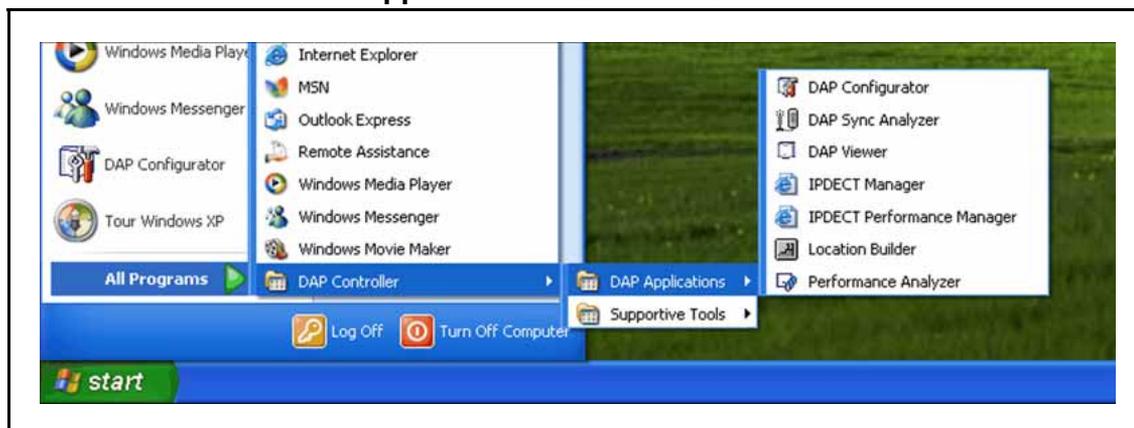
In this map you put the DAPs according to their position in the real site. A map gives you an overview of the DAP structure in a building. You can store this information in a file. Import this file into the DAP Sync Analyzer tool to create an overview of the synchronization structure in a building based on your measurements.

Use the Location builder tool

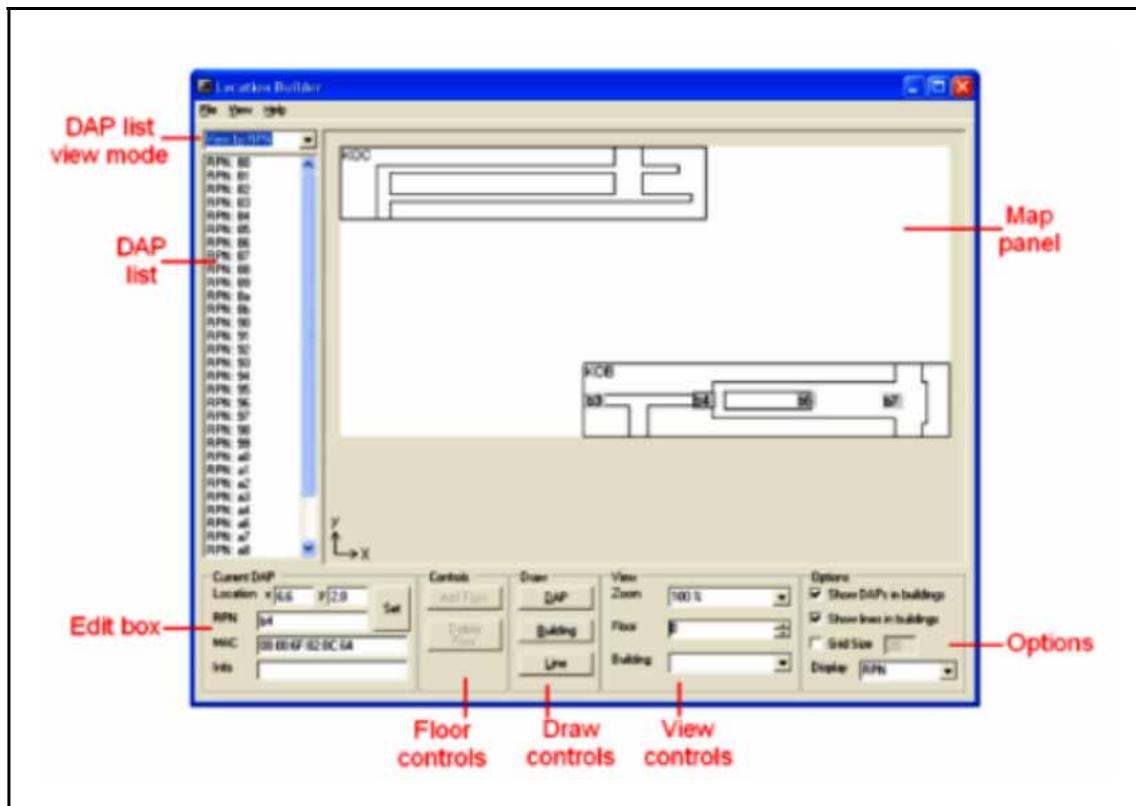
Use the steps in the following procedure to start the Location builder tool.

Procedure 118 Starting the Location builder tool

Step	Action
1	To start the DAP configurator tool through the Start menu, choose Start > All programs > DAP controller > DAP Applications > Location Builder .



The **Location builder** main screen appears.



Note: The main screen does not initially show data. The figure above contains data to better explain the fields in the main screen.

2 The main window contains the Map panel, DAP list view mode pane, Edit box, Floor controls, Draw controls, View controls, and Options panel.

- Use the **Map** pane to view a map of the area. There are two view modes:
 - **Location view** shows one whole floor with multiple buildings visible.
 - **Building view** shows a floor inside a building.
 You can switch between Location view and Building view by double-clicking on a building. You can select either a DAP, a building, or a line. Right-click on the map to access a menu of actions you can perform on the selected item. The Location Builder relies on the usage of coordinates for the localization of DAPs, buildings, and lines. The coordinates of the mouse cursor are indicated if the mouse cursor is hovering over a map. The origin (0,0) of the coordinate system is in the bottom left corner of the map.
- Use the **DAP list view mode** pane to select the view mode for the DAP list . There are three view options:

- RPN numbers
- MAC addresses
- Info field

The DAP list shows a list of DAPs that are not yet on the map. You can drag these DAPs onto map.

Populate the DAP list by adding new DAPs to the **RPNadm.txt file**, using menu item **File > Import**.

- In the **Edit box** area, you can edit properties of the selected location, building, or DAP. After editing the values in the Edit box, click **Set** to save your changes.
- Use the **Floor controls** to add or delete a floor or set the location of a floor.
- Use the **Draw controls** to add a DAP, a building, or a line.
- Use the **View controls** to change the view of the Map pane.
- Use the **Options** controls to customize display options.

--End--

Create a location file

Use the steps in the following procedure to create a location file.

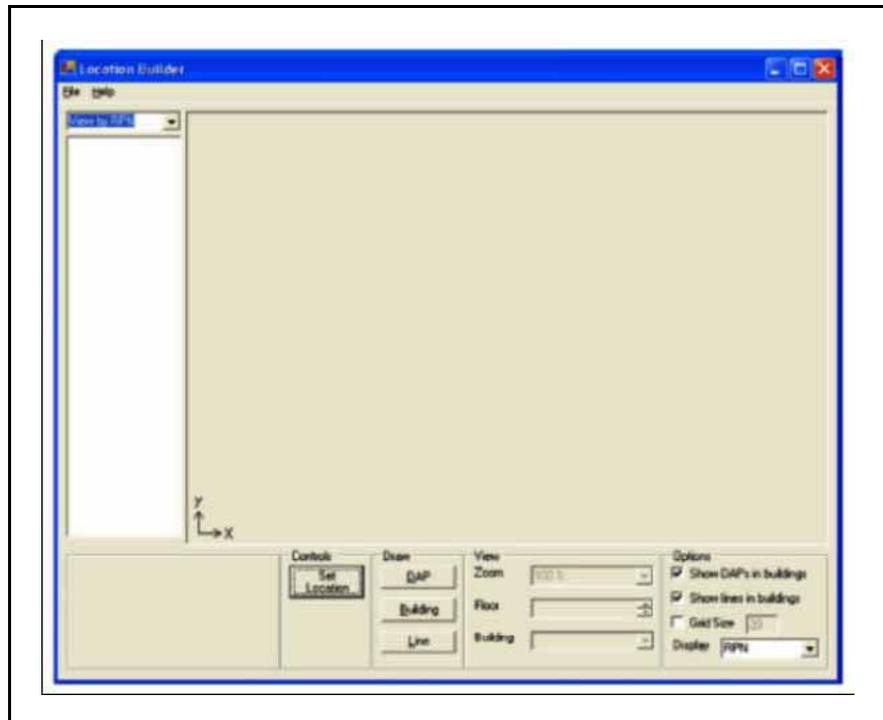
Prerequisites

- Ensure that you have up-to-date maps of the building(s). You can import a map of a building or floor from a bmp, .gif and .jpg file.
- Ensure that you have a clear understanding of the sizes of the area and the buildings. Ensure that the maps use a common scale; if they do not, ensure that you understand how they differ.

Use the steps in the following procedure to create a location file.

Procedure 119 Creating a location file

Step	Action
1	To start the DAP configurator tool through the Start menu, choose Start > All programs > DAP controller > DAP Applications > Location Builder . The Location builder main screen appears.



- 2 Click the **Set Location** button to initialize the Location.
- 3 In the Size fields, enter values large enough to encompass all the buildings in your location.

Note: The size values used in the location builder do not correspond to real-world units, such as meters or feet. However, Nortel recommends that you consistently enter values that equal the measurements in meters, which will make your location map easier to understand.

- 4 Click **Building** to add a building to the Location.
Alternatively, you can also add a building by drawing it in place; click the left mouse button to indicate the lower left corner of the building, and then click the right mouse button to access the menu, and choose **Add Building**.

The **Add Building** window appears.

- 5 Enter values for the location and the size.
 - In the **x** and **y** fields, define the position of the lower left corner of the building.
 - In the **w** field, define the width (x size) of the building. Nortel recommends that you enter the actual width of the building in meters
 - In the **h** field, define the depth (y size) of the building. Nortel recommends that you enter the actual depth of the building in meters

After entering values for the building size and location, you can make changes by selecting the building and editing the values that appear in the **Edit** pane.

Note: There are two view modes. The first is the Location View, which shows one whole floor with multiple buildings visible. The second is the Building view, which shows only a floor inside a building. Double-clicking on a building switches between views.

- 6 To add lines to a building, double-click on the building to which you want to add lines.
The **Building** view is activated.

Note: Lines are used to add contours and shapes to buildings. The lines can provide a reference to items on the maps like stairwells, elevator shafts or oddly shaped (non rectangular) buildings.

- 7 In the **Building** view, add lines using either of the following methods:

- Add lines using the **Add lines** tool:
 - Right click in the Location area.
A menu appears.
 - Choose **Add lines** from the menu.

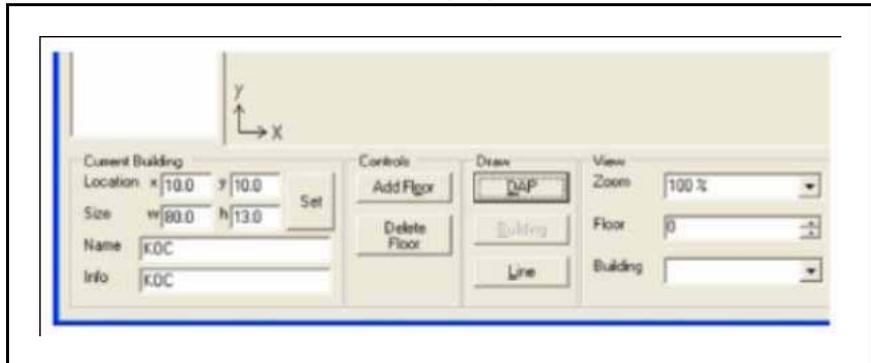
OR

- Add lines in freehand mode:
 - Click **Line** in the draw controls box.
 - With your mouse pointer in the position where you want the line to begin, click and hold down the left mouse button.
 - Move your mouse pointer to the point where you want the line to end, and release the mouse button.
 - Repeat these steps to draw additional lines.

Note: To make it easier to create straight lines in freehand mode, first click **snap to grid**, which will make it easier to draw straight lines. Adjust the **Grid Size** if necessary.

- 8 If your buildings have only one floor, skip this step.
To add a floor, double-click the border line of the building to which you want to add a floor.

A view of the building appears in the map panel. The Control pane in the bottom part of the Location Builder shows the Floor controls, as shown in the following figure.



- 9 Click **Add Floor** .
The **Add Floor** dialog appears.
- 10 Enter the relevant data in the **Add Floor** dialog and click **OK**.
You can also add multiple floors at once, and copy the lines of the current floor to the newly created floors. As well, you can add lines to the new floors or edit existing lines.

Note: At this point the location is filled with buildings, the buildings have floors and the floors have lines. This is all the information you require to provide a reference framework for the position of the DAPs.

- 11 Choose one of the following:
 - If you have not populated a RPNadm.txt file, go to step 17, and add DAPs manually.

If you have populated a PRNadm.txt file, go to step 12. and import the PRNadm.txt file

- 12 In the menu, choose **File > Import**.
The **Import** dialog appears.
- 13 Browse to the **RPNadm.txt** file, and select it. Click **Open**.
A dialogue appears and prompts you to indicate your preferences for the importing the RPNadm.txt file.
- 14 Ensure that **Update DAPs already located** is not checked, and click **OK**.

A list of DAPs appears on the left side of the program window.

Note: You can change the view mode using the view mode select box, located above the DAP list.

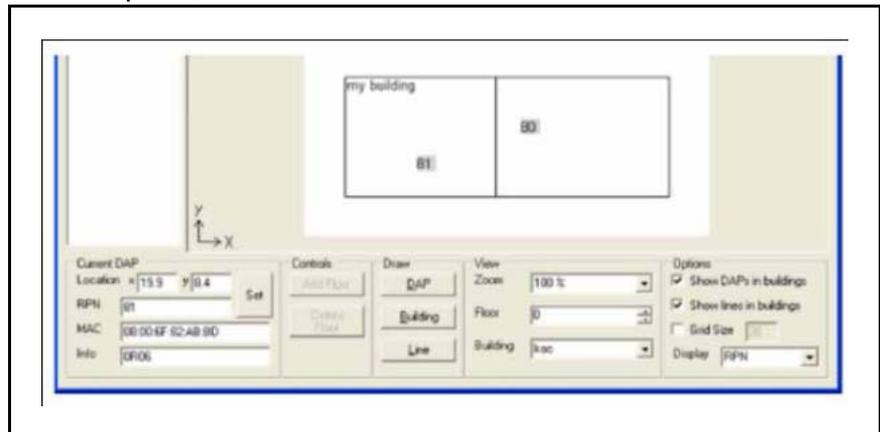
- 15 To move a DAP to the Map, simply drag it onto the Map. If you accidentally release a DAP on the wrong position, you can reposition it.

You can remove a DAP from the map, and put it back in the DAP list. To do so, right-click on the DAP, and choose the menu item **Move To**.

After you place a DAP on the Map, an autonumber function for the Info field is activated. This function only works if the following two items are true.

- The previous DAP added must have an Info field in the form `{current floor number}{string}{number}`, for example 0R05. These are the notations as used in the Site Survey, consult therefore the Site Survey manual for more info on these notations.
- The current DAP must have an empty Info field.

If both these requirements are met, the current DAP gets an Info field assigned in the form `{current floor number}{string}{number + 1}`, for example 0R06. The following figure shows the RPN data and the Info field data in the Edit box pane, titled Current DAP.



- 16 Continue placing the DAPs until the DAP list is empty.
- 17 To add a DAP manually, right-click a point on the Map, and select **Add DAP** from the menu. The Add DAP dialog appears.



The RPN and Info fields are automatically populated. Ensure that the values are correct, and click **OK**.

A DAP is created at the position you specified in the Add DAP dialog.

- 18** After the building of the Location is complete, select one or more of the following options.
- In the menu, choose **File > Save** to save the location file as an .xml file. You can later import this file into the DAP Sync Analyzer tool.
 - Export the location file as a .csv file that can be used in the DAP Sync Analyzer. This file does not contain building information. This .csv file contains DAP information only.
 - Export the Dummy visibility file as a .txt file. This creates a flat synchronization hierarchy. This .txt file can be used only if no realistic visibility file can be obtained.
 - Export the RPNadm file as a .txt file. This file contains the RPN data as you setup in the Location Builder tool. Normally the RPNadm file contains the RPN data provided in the imported RPNadm.txt file.

--End--

Maintenance

You can make changes in the Location configuration after the Location file is created, for example:

- You can make minor configuration changes, excluding RPNadm data. To make minor changes in the configuration, you can import the Location file, and then select the item that has to be updated. You can edit the properties of the selected item using the Edit box.
- You can update the RPNadm.txt data using the update utility that is part of the RPNadm.txt import function. To do so, import an updated RPNadm.txt file, and select the **Update DAPs already located** option. If necessary, select whether the MAC address or RPN is to take precedence. Choosing between RPN and MAC Address is necessary

if, for example, a number of RPNs have changed in the DAP manager, but the radios are still identical, thus having identical MAC addresses.

Index

A

Adding a D-Channel 156
 Adding a DN range 196
 Adding a route 156
 Adding digit manipulation block 159
 Adding Gateway Endpoint for DAP
 redirect server 166
 Adding Gateway Endpoint for signaling
 server 166
 Adding location code (UDP) 160
 Adding number range 151
 Adding route list block 159
 Adding the CDP domain 165
 Adding the UDP domain 165
 Adding trunks 157
 Assembling the deployment tool 57
 Assess floor layout 79
 Assess radio coverage 25

B

Back up and restore subscriptions 197
 Built-in DHCP and TFTP servers 124
 Built-in DHCP server 124
 Built-in TFTP server 126

C

Calculating number of users inside the
 cell within an office 86
 Calculating number of users with office
 outside cell who walk into cell 87
 Calculating the data for all remaining
 cells 89
 Calculating the number of users without
 an office 88
 Call server 99
 Call server configuration 170

Call server configuration to MSNMN 179
 Call server software 103
 CallPilot and message waiting
 indication support 16
 Cell centers marker 40
 Cell reengineering process 83
 Central directory access tool 208
 Change a DAP RPN 194
 Charging the deployment handset
 battery 56
 Charging the deployment tool battery 55
 Charging time of the deployment
 handset battery 56
 Check IIS on PC with Windows 2000 106
 Check IIS on PC with Windows XP 111
 Checking for through-the-floor coverage 79
 Checking IIS on a PC with Windows
 2003 109
 Choice of system configuration 174
 Configuration of settings using IP DECT
 Configurator 136
 Configuration of UEXT, remote system 182
 Configuration on Element manager 154
 Configuration without a DHCP or
 TFTP 126
 Configuring CLID 172
 Configuring network access 158
 Configuring NRS 178
 Configuring Personal Call Assistant 182
 Configuring routing entries for DAP
 Redirect Server 168
 Configuring routing entries for the
 signaling server 169
 Configuring SIP DECT for Central
 directory access 213
 Configuring SIP properties 162
 Configuring the signaling server 161

Configuring UEXT, multi site handset 181
 Configuring Universal Extension 171
 Correcting audio problems 71
 Coverage and signal strength calculation 37
 Coverage terms 51
 Create a location file 241
 Creating a new customer 155
 Creating a table to document telephone types in a cell 90
 Creating an estimate table 85
 Creating an Excel file for the central database 209
 Creating ESN control block 158
 Creating service domain 165
 Critical point marker 40
 Customer review 21

D

DAP AC adaptor part numbers 34
 DAP Controller 130
 DAP controller software 103
 DAP Controller software deinstallation 230
 DAP controller software, internet information services 105
 DAP deployment 67
 DAP deployment rules and requirements 27
 DAP management 194
 DAP manager configuration 150
 DAP manager overview 185
 DAP power configuration 34
 DAP reboot history 202
 DAPs 100
 DECT Access Points 100
 DECT deployment kit 2 64
 DECT handset features 16
 Deleting a number 190
 Deployment illustrations 42
 Deployment review 97
 Deployment review, floor plan completion 97
 Deployment terms 50
 Deployment tool 52
 Deployment tool, how it works 61
 Deployment tool, using 62
 Deployment, cell centers too close 81
 Deployment, cells centers too far apart 81
 Deployment, double cell 75

Deployment, high handset density deployment 95
 Deployment, high rise buildings 81
 Deployment, high traffic areas 83
 Deployment, multi cell 76
 Deployment, multiple floor 78
 Deployment, multiple floor, checking for through-the-floor coverage 79
 Deployment, single and multiple floor 72
 Deployment, single cell 73
 Deployment, single floor 72
 Deployment, too many cell centers 82
 Deployment, traffic volume 83
 Deployment, unusual conditions 81
 Determine cell boundaries 38
 Determining cell reengineering 91
 DHCP and TFTP servers 111
 Disabling a subscription 189
 Double cell deployment 75
 Dynamic IP network addresses 33

E

Editing a subscription RPN 188
 Enabling message waiting indication 172
 Equipment damage 55
 Estimating traffic within a cell 84
 Ethernet requirements 31
 Example cell boundaries 41
 Example of cell labels 41
 Export a SIP DECT system 228
 Export and import SIP DECT system 228
 Export subscriptions 199

F

Fixed IP network addresses 32
 Floor layout, all floors with same layout 79
 Floor layout, all floors without the same layout 80
 Floor plan completion 97
 Floor plan markings 40

G

Gather building information 24
 Gather survey items 22

H

Handset firmware update 204
 Handset status 192

Handset tones interpretation 63
 Hardware installation 99
 High handset density deployment 95

I

Identify critical points and cell boundaries 39
 Identify existing cabling 25
 Identify site contacts 23
 Import a SIP DECT system 229
 Import and export subscriptions 177
 Import subscriptions 201
 Initial critical points on the floor plan to identify 34
 Install and maintain IIS on MS Windows 2000 105
 Install and maintain IIS on MS Windows 2003 106
 Install and maintain IIS on MS Windows XP 109
 Install IIS on PC with Windows 2000 105
 Install IIS on PC with Windows XP 110
 Installation of the Central directory access tool 210
 Installation, call server 99
 Installation, DAPs 100
 Installation, PC (DAP controller) 100
 Installation, signaling server 99
 Installing IIS on a PC with Windows 2003 106
 Internet information services 105
 IP DECT configuration tools 9
 IP network configuration 31

L

Limit the anticipated number of handsets 95

M

Maintenance 246
 Mark the points, centers, and boundaries on the floor plan 40
 MS Windows 2000 and 2003 DHCP and TFTP servers 112
 Multi cell deployment 76
 Multi site mobility network configuration 175
 Multicast addresses 33
 Multiple coverage situations 80

Multiple floor deployment 78
 Multiple floor deployment, checking for through-the-floor coverage 79

N

Network packet capture traces 238
 Normal site survey 21
 NRS configuration 163
 Number of handset users 21

O

Obtain site plans 23
 Outdoor deployment, rules for 63
 Overview of SIP DECT 9

P

PC (DAP controller) 100
 Points, centers, and boundaries on a floor plan 42
 Position and use of available cabling 20
 Prepare the tool for deployment 54
 Product overview 9
 Profile handset use 26

R

Radio coverage 20
 Radio synchronization 27
 Rebooting a DAP 195
 Rebooting all DAPs 195
 Rebooting DECT Access Points 150
 Reengineering cells for high traffic areas 83
 Remove and replace a DAP 218
 Removing a subscription 190
 Restarting IIS on a PC with Windows 2003 108
 Reviewing DAP reboot history 202
 Routed Head Quarter configuration 13, 173
 Rules and guidelines to locate cell centers 35

S

Saving changes 170
 Separating the coverage area and recording the number offices 85
 Setting the database to standby view 164
 Signaling server 99

- Signaling server software 103
- Simple SIP DECT configuration 135
- Single and multiple floor deployment 72
- Single cell deployment 73
- Single floor deployment 72
- SIP DECT capacity limitations 17
- SIP DECT configuration figure 11
- SIP DECT five main components 9
- SIP URI map 162
- Site planning 19
- Site planning example (Able-Studio) 22
- Site planning overview 19
- Site survey example 21
- Site survey process 22
- Software deinstallation 230
- Software requirements 103
- Software requirements, call server software 103
- Software requirements, DAP controller software 103
- Software requirements, signaling server software 103
- Subdivide a cell 95
- Subscribe a multi site DECT handset 176
- Subscribing a DECT handset 152
- Subscribing a handset 187
- Subscription export and import 198
- Subscription management 187
- Supported database types 209
- Synchronization analyzer interface 220
- Synchronization analyzer location page 223
- Synchronization analyzer main page 220
- Synchronization analyzer portable tracking page 225
- Synchronization hierarchy 29
- System administration 185
- System archive 202, 238
- System configuration 135
- System maintenance 215
- System survey 236
- System synchronization analysis 219

T

- Testing the deployment handset 60
- TFTP server 121
- Totalling the estimate for users in a cell 89
- Traffic volume 83

U

- Universal extension support 14
- Using the filter 191
- Using the location builder tool 239

Z

- Zone configuration 155

Nortel Communication Server 1000

SIP DECT Fundamentals

Copyright © 2008-2009 Nortel Networks
All Rights Reserved.

Release: 5.5
Publication: NN43120-123
Document revision: 01.07
Document release date: 6 January 2009

To provide feedback or to report a problem in this document, go to www.nortel.com/documentfeedback.

www.nortel.com
Sourced in Canada

LEGAL NOTICE

While the information in this document is believed to be accurate and reliable, except as otherwise expressly agreed to in writing NORTEL PROVIDES THIS DOCUMENT "AS IS" WITHOUT WARRANTY OR CONDITION OF ANY KIND, EITHER EXPRESS OR IMPLIED. The information and/or products described in this document are subject to change without notice.

Nortel, the Nortel Logo, the Globemark, SL-1, Meridian 1, and Succession are trademarks of Nortel Networks.

All other trademarks are the property of their respective owners.

