DBC 43x and DBC 44x

INSTALLATION INSTRUCTIONS

Mitel®

NOTICE

The information contained in this document is believed to be accurate in all respects but is not warranted by Mitel Networks™ Corporation (MITEL®). Mitel makes no warranty of any kind with regards to this material, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. The information is subject to change without notice and should not be construed in any way as a commitment by Mitel or any of its affiliates or subsidiaries. Mitel and its affiliates and subsidiaries assume no responsibility for any errors or omissions in this document. Revisions of this document or new editions of it may be issued to incorporate such changes.

No part of this document can be reproduced or transmitted in any form or by any means - electronic or mechanical - for any purpose without written permission from Mitel Networks Corporation.

TRADEMARKS

The trademarks, service marks, logos and graphics (collectively "Trademarks") appearing on Mitel's Internet sites or in its publications are registered and unregistered trademarks of Mitel Networks Corporation (MNC) or its subsidiaries (collectively "Mitel") or others. Use of the Trademarks is prohibited without the express consent from Mitel. Please contact our legal department at legal@mitel.com for additional information. For a list of the worldwide Mitel Networks Corporation registered trademarks, please refer to the website: http://www.mitel.com/trademarks.

1 GENERAL

This document is valid for DBC 433 (Mitel 7433ip), DBC 434 (Mitel 7434ip), DBC444 (Mitel 7444ip) and DBC 446 (Mitel 7446ip) phones.

These phones support the H.323 protocol.

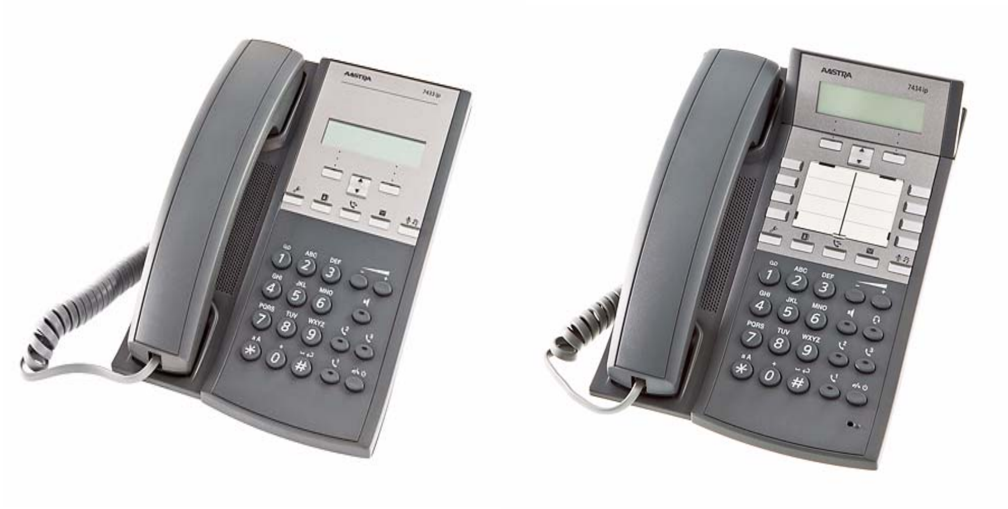


Figure 1: DBC433 and DBC434

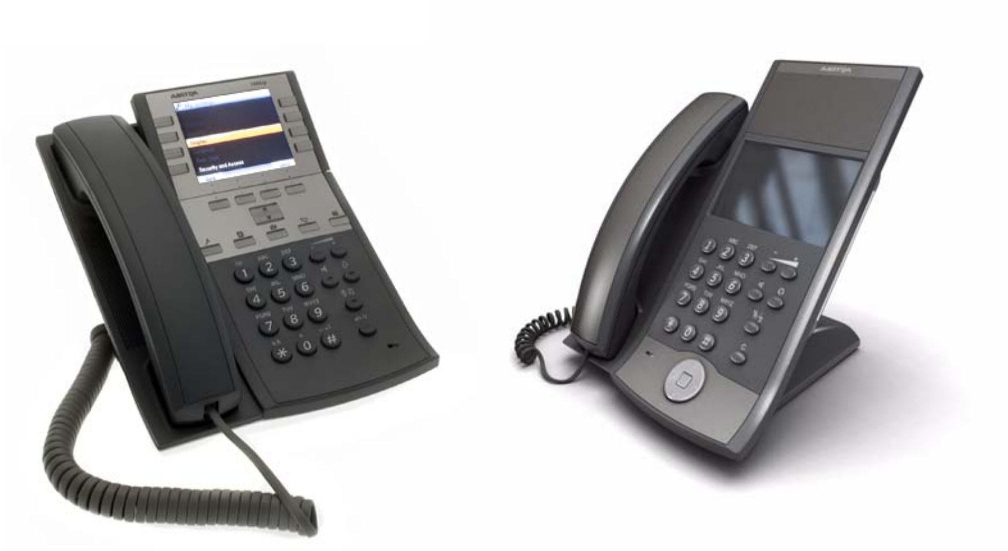


Figure 2: DBC444 and DBC446

1.1 SCOPE

This document describes how to connect DBC 43x or DBC 44x phones to MX-ONE Service Node (SN).

1.2 ACRONYMS

DPU	Display Panel Unit
KPU	Key Panel Unit
OPU	Option Unit
MX-ONE SN	MX-ONE Service Node
XML	Extensible Markup Language

1.3 ENVIRONMENTAL REQUIREMENTS

The products covered in these installation instructions comply with the prerequisites stipulated for placing appliances in office and exchange room environments.

2 PREPARATIONS

Check that an Ethernet cable is available and verify that it is possible to connect to the LAN.

2.1 AIDS

No tools are required for connecting cables to the phone. To fasten the lid covering the connectors on the back of the phone, a crosshead screwdriver is required.

3 DELIVERY METHOD

The phone is delivered in a box together with a foot console, a handset, a handset cord, and a lid for covering the connectors on the back of the phone. Key and display panel units are delivered separately. AC/DC adapter is also delivered separately.

The phone is delivered with the software version that was valid when the phone was produced. The configuration file must be adapted for each site and has to be loaded into the phone. The configuration file is loaded when the phone is started.

4 CABLING

The maximum line length between an IP phone and the LAN is 100 metres (328 feet) according to IEEE 802.3. When using the phone with an GBit option unit, it is recommended that shielded category 6 Ethernet cables are used. When using the phone without a GBit option unit, shielded category 5 Ethernet cables are recommended.

The following Ethernet category 5 cable can be ordered from Mitel:

- TSR 901 0452/3000

The cables shall be connected to the outlets according to the figure.

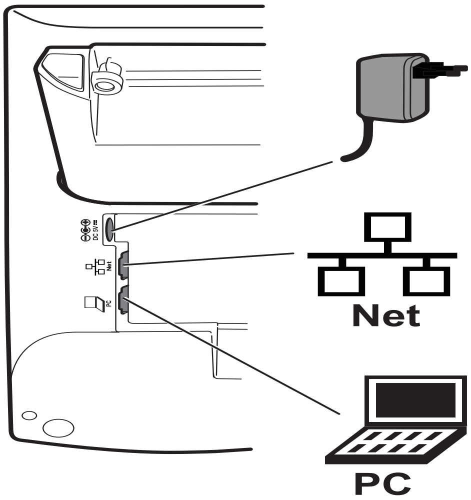


Figure 3: Cabling for DBC43x and DBC444

It is important to fit the cover over the connectors to protect against ESD discharge, see figure below.

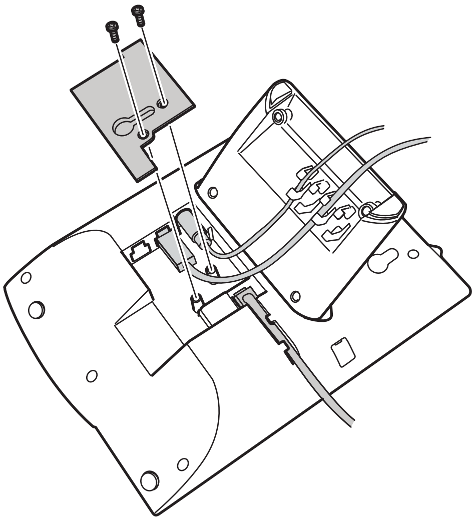


Figure 4: Cover to protect towards ESD discharge

Note: Some types of LAN cables with connectors with sleeve cannot be used, because these connectors can be difficult to fit with the LAN inlet on the DBC433, DBC434 and DBC444 phones.

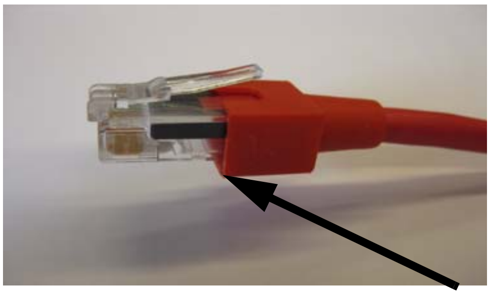


Figure 5: Some types of Ethernet connectors with sleeve do not fit

For more information on how to connect cables, see *the User Guide for each telephone model.*

5 POWER EQUIPMENT

These telephones can be powered from an AC/DC adapter or from Power over Ethernet.

Note: Do not connect these phones to other power adapters than specified below. Using other power adapters (including adapters suiting other Mitel phones) may damage the phone.

DBC 43X and DBC 444

The power adapter (110–240V, 50/60Hz, 5V DC) uses a changeable mains cable fitting most national power feeding systems. The following national variants are available:

- RES 141 319/1 for the EU market except for the UK
- RES 141 319/2 for the US market
- RES 141 319/3 for the UK market.

DBC446

The power adapter (110–240V, 50/60H3, 24V DC) fits most national power feeding systems and the mains cable can be changed. The following national variants are available:

- RES 141 316/1 for the EU market except for the UK
- RES 141 316/2 for the US market
- RES 141 316/3 for the UK market

Power over Ethernet

The alternative is to use Power over Ethernet (PoE). The phone supports the standard IEEE 802.3af. The power consumption for each telephone model is according to the following table.

Device	With AC/DC power adapter*	With PoE*	Power Class	Power Class with OPU
DBC 433	2.0 W	2.6 W	1	2
DBC 434	2.0 W	2.6 W	1	2
DBC 444	2.8 W	3.6 W	2	3
DBC446	2.6 W	3,6W	3 **)	3
KPU	0.1 W	0.1 W	-	-
DPU	0.1 W	0.1 W	-	-
OPU	1.6 W	2.0 W	-	-

*) With a pc connected to the pc port, with an active handset call and with medium backlight.

**) This telephone does not adapt the power class if a GBit Ethernet option unit is connected. The telephone reports power class 3 although it only needs 3.6 W

DBC446 phones equipped with the gigabit Ethernet Option unit (DBY412 01) can be supplied with PoE on a GBbit LAN. However, if a telephone equipped with DBY412 01 is connected to a 10/100 megabit LAN then it can not be powered by a PoE switch. In this case either remove the gigabit unit or use a power adapter.

6 EARTHING AND GROUNDING

No special earthing or grounding is needed.

7 SETTING UP THE SOFTWARE SERVER

The software used by the phone is stored on a software server and downloaded to the phone during power up. In an MX-ONE environment, the host for the MX-ONE Service Node and the IP phone software server can not be the same. Setting up the software server comprises the following steps:

- Installing the software server.
- Creating a directory structure on the server.

When the software server is installed and the directory structure created, the phone software can be stored on the server. For information on how to store phone software on the server, see 9.1 Installing New Phone Software on the Software Server on page 16.

7.1 INSTALLING THE SOFTWARE SERVER

Installation of the software server is done according to the documentation of the HTTP server. Both PC and Unix versions are supported.

The following HTTP servers have been tested with the DBC 43X and DBC 44x phones:

- Microsoft® Windows® 2000 and 2003 Server. When using Windows® Server, the **.dat** and **.hex** file types must be enabled. If certificates shall be loaded the file types **.pem** and **.bin** must also be enabled. Follow the steps below to enable these file types:

  In **IIS Manager**, select **DefaultWEB Site**. Then select **Properties** and edit **HTTP header**. Apply the following settings:

  – **Associated extension: .dat**, **.hex, .pem** and **.bin**.

  – **Content type (MIME): application/octet-stream**.
- Apache 1.3.3 on Microsoft® Windows® or Redhat® Linux 5.2.
- Apache Tomcat. When the IP Phone Configuration File in MX-ONE SN Manager shall be used the Tomcat server is mandatory. For more information, see the description for *Configuration file for DBC 44x and DBC 43x*.

Note: When storing the files on the software server, make sure that the files are transferred in binary mode, otherwise the file can be modified by the transfer tool and the size be changed. In this case the telephone will not load the file.

7.2 CREATING A DIRECTORY STRUCTURE

For DBC 43X and DBC 44x phones to be able to download files from the software server, the appropriate directory structure must be created under the HTTP root directory. If several different configuration files are used (for different groups of phones where each group is a member of a specific domain), the structure with several domain names is used. When using several domains, the configuration files have the same name in each domain, although they have different contents, defining characteristics for the different groups of phones.

The domain name can be either the DNS domain name (DHCP option 15) or the telephony domain name (option 43).

It is only the configuration file, not the application, super boot, KPU and DPU software, that needs to be stored under each domain directory name.

If the phones do not find any configuration file in a domain directory, the configuration file in the **<SW server root>/dbc43x01** directory is used for DBC 43x phones and the **<SW server root>/dbc44x01** directory for DBC 44x phones.

For detailed information on how to store phone software on the software server, see 9.1 Installing New Phone Software on the Software Server on page 16.

The figures below show also the folder **ringtones** where the melodies used as ring signals shall be stored and the folder **certificates** where digital certificates for security with TLS shall be stored.

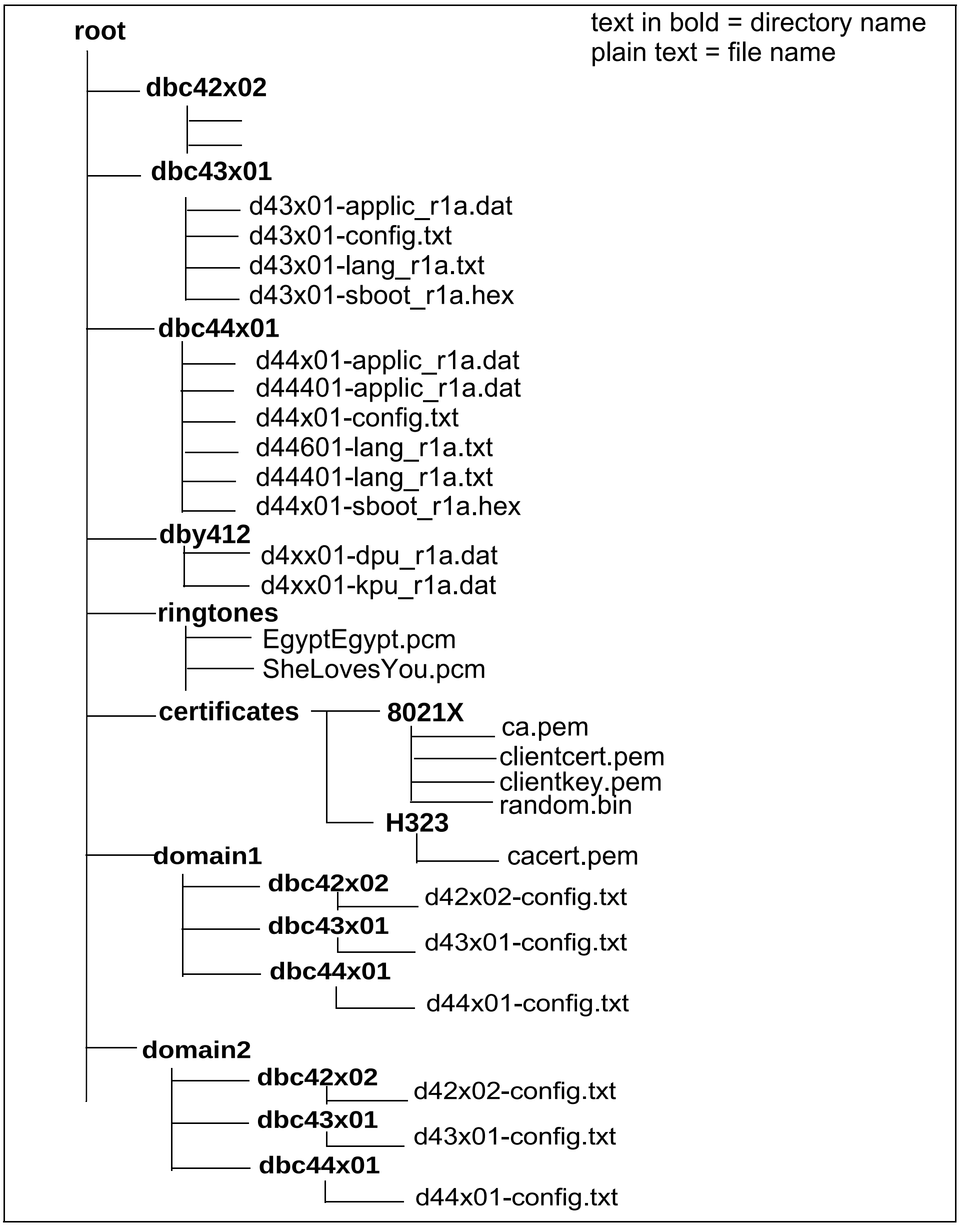


Figure 6: Directory structure using domain names

If the subnet method is used, see 12.25.3 Subnet Method on page 47, the directory structure will be as in the example below. In this example the phones belonging to the first group have the network address 130.100.26.128 with the subnet mask

255.255.255.192. The second group has the network address 130.100.27.0 with the subnet mask 255.255.255.0.

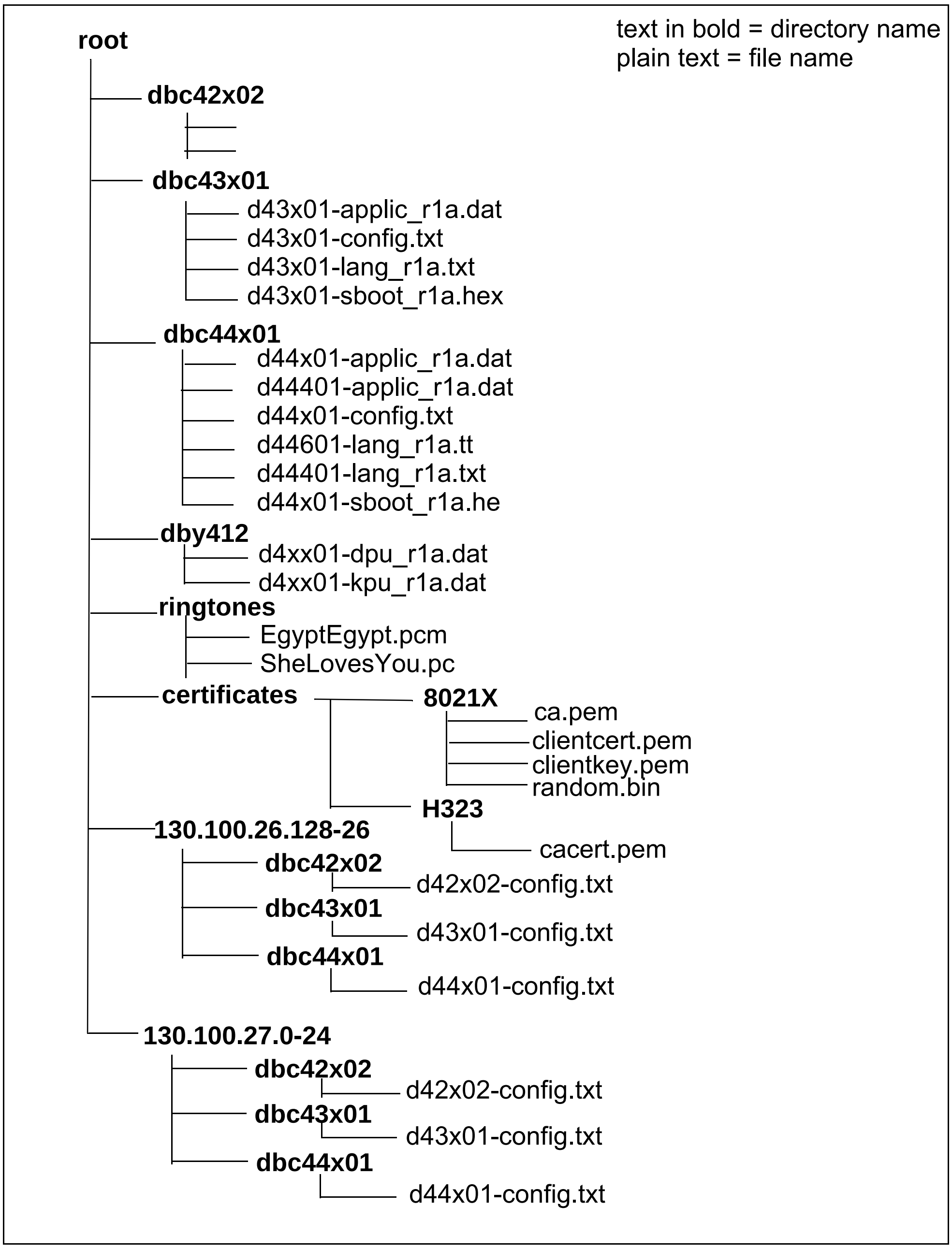


Figure 7: Directory structure using the subnet method

8 HOW TO START A NEW PHONE

The phone is delivered with default settings for an IP network. In most cases, these settings must be adapted to the network to which the phone is connected for the phone to work.

Most settings in the phone can be controlled by the configuration file, available on the software server. When the phone is powered up, the configuration file is downloaded to the phone from the software server.

Starting a new phone comprises two scenarios:

- Connecting the phone to a network using DHCP. This requires that a DHCP server is installed and configured, see section 25 DHCP server on page 89.
- Connecting the phone to network not using DHCP.

8.1 CONNECTING THE PHONE TO A NETWORK USING DHCP

To be able to connect the phone to a network, the following parameters must be configured:

- **The phone's IP address**, **subnet mask**, and **default gateway**. When using DHCP, these parameters are configured automatically.
- **The IP address of the software server**. This address is configured automatically using DHCP or DNS, or manually from the phone. If DHCP is used for providing this parameter, the DHCP server must be configured before the phones can connect to the network. For information on how to configure the DHCP server for providing the phone with the IP address to the software server, see 25.2 Data from DHCP on page 89.

  If DNS is used for providing this parameter, the DNS server must be configured before the phones can connect to the network. For information on how to configure the DNS server for providing the phone with the IP address to the software server, see 12.26 Using DNS SRV Resource Records on page 48.
- **The IP address of the gatekeeper**. This address is configured using the configuration file, manually from the phone, or using the gatekeeper discovery procedure. If the configuration file is used for providing the IP address, the IP address of the gatekeeper must be specified in the configuration file before the phone can connect to the network. For information on how to configure the phone with the IP address of the gatekeeper using the configuration file, see 12.15 Setting the IP Address of the Gatekeeper on page 36.

Follow the steps below to connect the phone to the network:

1. Connect the phone to the network and power supply. For information on how to connect cables, see 4 Cabling on page 7.
2. After approximately 15 seconds, the Mitel logotype is shown in the display and the speaker key LED is lit. After another 10 seconds, the Mitel logo is displayed. The phone is now configured with an IP address, a subnet mask, and a default gateway, provided by the DHCP server.
3. If DHCP or DNS is used for providing an IP address to the software server, proceed to step 5.
4. If DHCP or DNS is not used for configuring the phone with the IP address of the software server, configure this IP address manually. For information on how to

configure the phone with the IP address of the software server manually, see 12.11 Setting the IP Address of the Software Server on page 34.

5. If the message **Software update is available. Update?** is shown in DBC43x or if the corresponding message **A new version of the telephone software is available**. **Update is recommended** is shown in DBC44x, new software for the phone is available on the server. For information on how to install new software, see 9 Installing New Software on page 16.
6. If the IP address to the gatekeeper is specified in the configuration file, proceed to step 7. If not, configure the phone with the IP address of the gatekeeper manually from the phone. For information on how to manually configure the phone with the IP address to the gatekeeper, see 12.15 Setting the IP Address of the Gatekeeper on page 36.
7. Log on to the phone. For instructions on how to log on to the phone, see *the User Guide for each telephone model*.

8.2 CONNECTING THE PHONE TO A NETWORK NOT USING DHCP

When connecting the phone to a network not using DHCP, network parameters in the phone are configured manually after the phone is started.

Follow the steps below to connect the phone to the network:

1. Connect the phone to the network and power supply. For information on how to connect cables, see 4 Cabling on page 7.
2. After approximately 15 seconds, the Mitel logotype is shown in the display and the speaker key LED is lit. After another 10 seconds, the Mitel logo is displayed and the logon page appears.
3. Configure the phone with the IP address to the phone, subnet mask, default gateway and software server. For information on how to configure the IP address to the software server, see 12.11 Setting the IP Address of the Software Server on page 34. When the phone is configured with a valid IP address to the software server, the configuration file is downloaded to the phone from the software server.
4. The phone is now configured according to the downloaded configuration file. For information on how to configure the phone using the configuration file, see *Configuration File for DBC 44X and DBC 43X*.

Note: When connecting to a network not using DHCP, disable DHCP in the phone.

5. If the following message is displayed in DBC43x: **Software update is available. Update?** or if the corresponding message is displayed in DBC44x: **A new version of the telephone software is available. Update is recommended.**

   new software for the phone is available on the server. For information on how to install new software, see 9 Installing New Software on page 16.
6. If the IP address to the gatekeeper is specified in the configuration file, proceed to step 7. If not, configure the phone with the IP address of the gatekeeper manually from the phone. For information on how to manually configure the phone with the IP address to the gatekeeper, see 12.15 Setting the IP Address of the Gatekeeper on page 36.
7. Log on to the phone. For instructions on how to log on to the phone, see the *User Guide for each telephone model*.

9 INSTALLING NEW SOFTWARE

9.1 INSTALLING NEW PHONE SOFTWARE ON THE SOFTWARE SERVER

By updating the software files and corresponding configuration files on the software server, the phones are updated when restarted. The phone software comprises the following files:

d43x01-applic_<version>.dat
(CAA 158 0067) The application software for the DBC 43x phones.

d44x01-applic_<version>.dat
(CAA 158 0057) The application software for the DBC 446 phones.

d44401-applic_<version>.dat
(CAA 158 0070) The application software for the DBC 444 phones.

d43x01-config.txt
(CAA 158 0064) The configuration file for DBC 43x. This file contains information about the version of the software to be used and other configuration data. Normally the configuration file has to be adapted for each installation.

d44x01-config.txt
(CAA 158 0058) The configuration file for DBC 44x phones. This file contains information about the version of the software to be used and other configuration data. Normally the configuration file has to be adapted for each installation

d43x01-lang_<version>.txt
(CAA 158 0063) The language file containing all the languages that are supported for DBC 43x.

d44601-lang_<version>.txt
(CAA 158 0059) The language file containing all the languages that are supported for DBC 446.

d44401-lang_<version>.txt
(CAA 158 0072) The language file containing all the languages that are supported for DBC 444 phones.

d43x01-sboot_<version>.hex
(CAA 158 0068) The super boot software for the DBC 43x phones.

d44x01-sboot_<version>.hex
(CAA 158 0060) The super boot software for the DBC 44x phones.

d4xx01-kpu_<version>.dat
(CAA 158 0065) The software to be loaded into the key panel unit.

d4xx01-dpu_<version>.dat
(CAA 158 0066) The software to be loaded into the display panel unit.

When the phone is powered up, the phone fetches the configuration file from the software server. If the software version defined in the configuration file is different than the software version in the phone, the phone fetches the application file from the software server. The super boot, KPU and DPU software are updated by the application if needed (these cannot be defined in the configuration file). The new software is automatically stored into the flash memory in the phone.

The software of the phone can be upgraded and downgraded.

It is recommended that the application and language files are stored in the **dbc43x01** directory for DBC 43x and under **dbc44x01** directory for DBC 44x. If the correct path is defined in the configuration file, the files can be stored in other directories. For information on the directory structure of the software server, see 7.2 Creating a Directory Structure on page 11.

Note: To update the super boot software, the file with the super boot software must be stored in the **dbc43x01** directory below the root folder for DBC 43x and under the **dbc44x01** directory for DBC 44x phones. To update the KPU and DPU software, the files must be stored under the directory **dby412**.

For information on how to work with multiple configuration files, see 12.25 Using Multiple Configuration Files on page 47.

9.2 INSTALLING NEW SOFTWARE ON THE PHONE

This section describes the procedure of installing new phone software, provided by the software server. The phone will fetch the new version of the software from the software server, when the phone receives a specific command from the gatekeeper or when the phone is restarted. The procedure is:

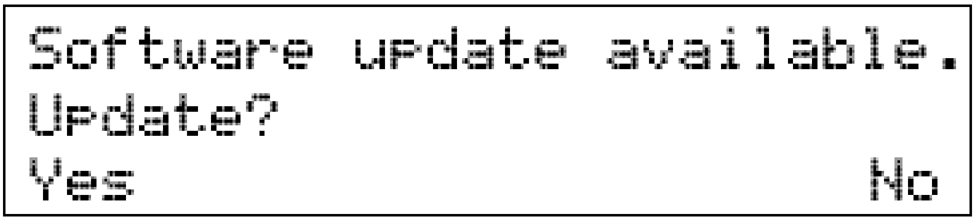
- In the Product Revision Information (PRI) document for the new version of the application, it is defined if there are new parameters in the configuration file. The PRI is accessible from Service Plaza:
  - If there are no new parameters in the configuration file: Update the existing configuration file with the new software versions.
  - If there are new parameters in the configuration file: Adapt the new configuration file with the existing site dependent parameter values.
- Store the configuration file on the software server according to the directory structure described in 7.2 Creating a Directory Structure on page 11.
- Store the new software on the software server according to the directory structure described in 7.2 Creating a Directory Structure on page 11.
- For the phones that are registered in the gatekeeper the following applies:
  - The phones will download the configuration file from the software server every 24th hour to check for new software. This option must be enabled with a parameter in the configuration file, see description of Configuration file for DBC43x and DBC44x.
  - by a command from the gatekeeper the telephone can be ordered to load the new software.
- For the phones that are not registered in the gatekeeper the following applies:
  - The phones will download the configuration file from the software server every 24th hour to check for new software, with the first check initiated 24 hours after the latest log out or restart of the phone.
  - The IP Phone Administrator tool can be used to get a list of unregistered phones. From this tool it is possible to open the Web server interface to the phone, select **Network**, press the key **Apply all settings**. The phone will restart and update the software.
- To start the update process manually from the phone press the ☎ ⏻ key for a couple of seconds and select the restart option (for DBC43x and DBC444). For DBC446 press the keys **C**, **mute** and # simultaneously for a second to restart the phone.

- Alternatively, if the phones are power fed from a power hub, it is possible to update the phone by power off/on the phones centrally.
- Verify that the right version of the software has been loaded by using a print command in the gatekeeper or using the IP Phone Administrator tool.

Note: To be able to download software from the server, the IP address to the software server must be set in the phone (using DHCP, DNS or manually).

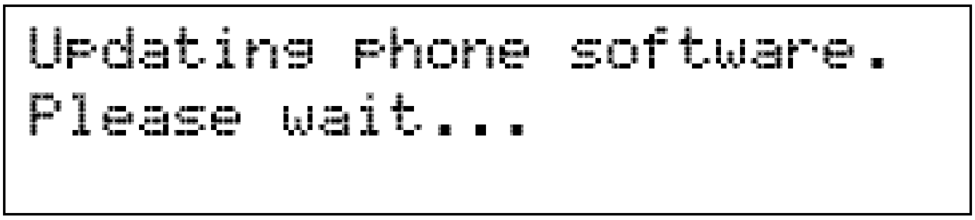
9.2.1 NEW SOFTWARE IN DBC 43X

When there is a new software to install, the following message is displayed:



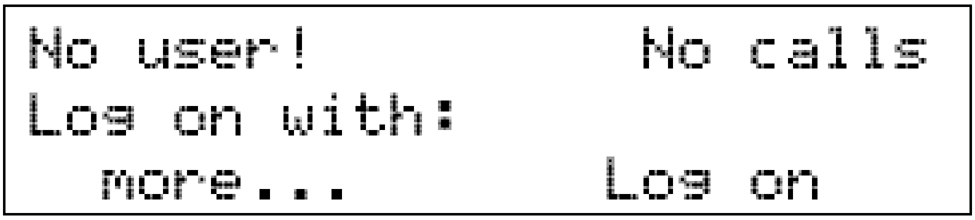
```
Software update available.
Update?
Yes                      No
```

1. To install the new software, select **Yes** or wait for the countdown to finish (takes 60 seconds). The following message is displayed:



```
Updating phone software.
Please wait...
```

2. When the software update is ready, the log on screen is displayed:

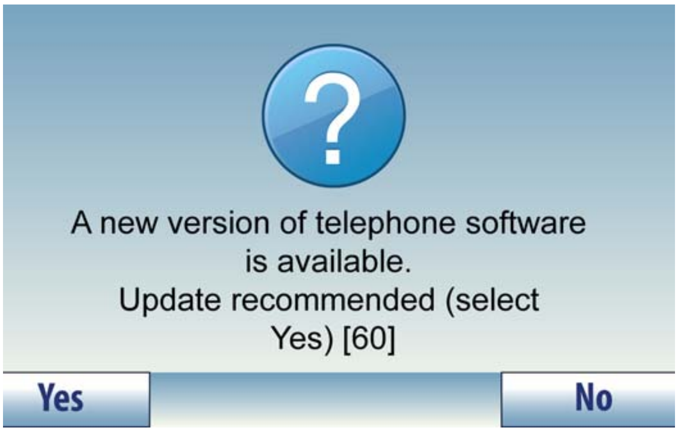


```
No user!          No calls
Log on with:
  more...        Log on
```

If the telephone was logged on before the software was updated, the telephone registers automatically towards the PBX.

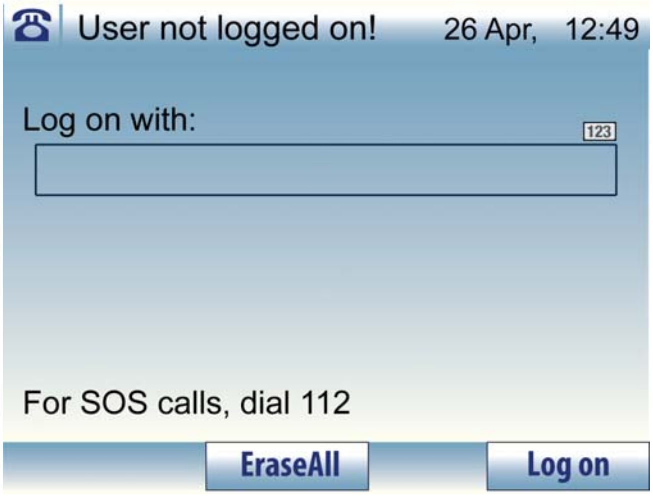
9.2.2 NEW SOFTWARE IN DBC 444

When there is a new software to install, the following message is displayed:



A new version of telephone software is available.
Update recommended (select Yes) [60]

1. To install the new software, select **Yes** or wait for the countdown to finish (takes 60 seconds).
2. When the software update is completed, the log on screen is displayed:



☎ User not logged on! 26 Apr, 12:49

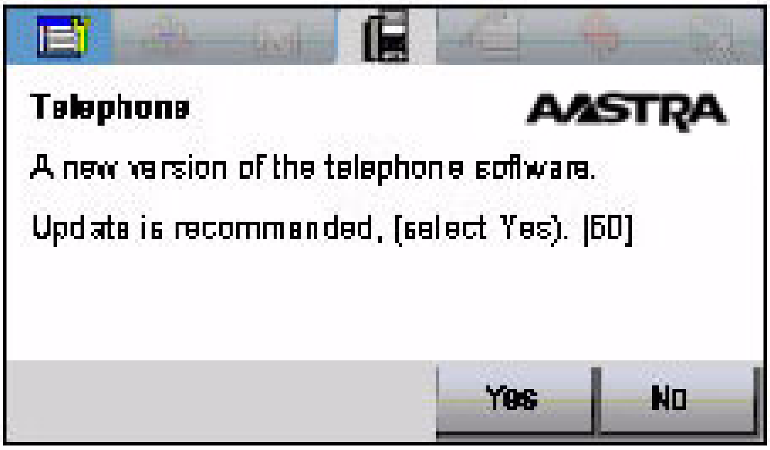
Log on with:

For SOS calls, dial 112

If the telephone was logged on before the software was updated, the telephone registers automatically towards the PBX.

9.2.3 NEW SOFTWARE IN DBC446

When there is a new software to install, the following message is displayed:

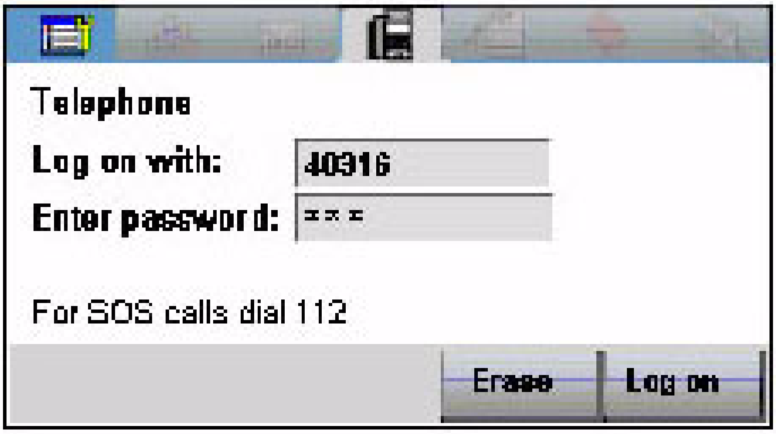


Telephone

A new version of the telephone software.

Update is recommended, (select Yes). [60]

1. To install the new software, select **Yes** or wait for the countdown to finish (takes 60 seconds).
2. When the software update is completed, the log on screen is shown:



Telephone

Log on with: 40316

Enter password: ***

For SOS calls dial 112

If the telephone was logged on before the software was updated, the telephone registers automatically towards the PBX.

9.3 FLOW CHART

The below flow chart describes some of the possible installation scenarios. Please note that installation scenarios may vary a lot, depending on network and configuration file settings.

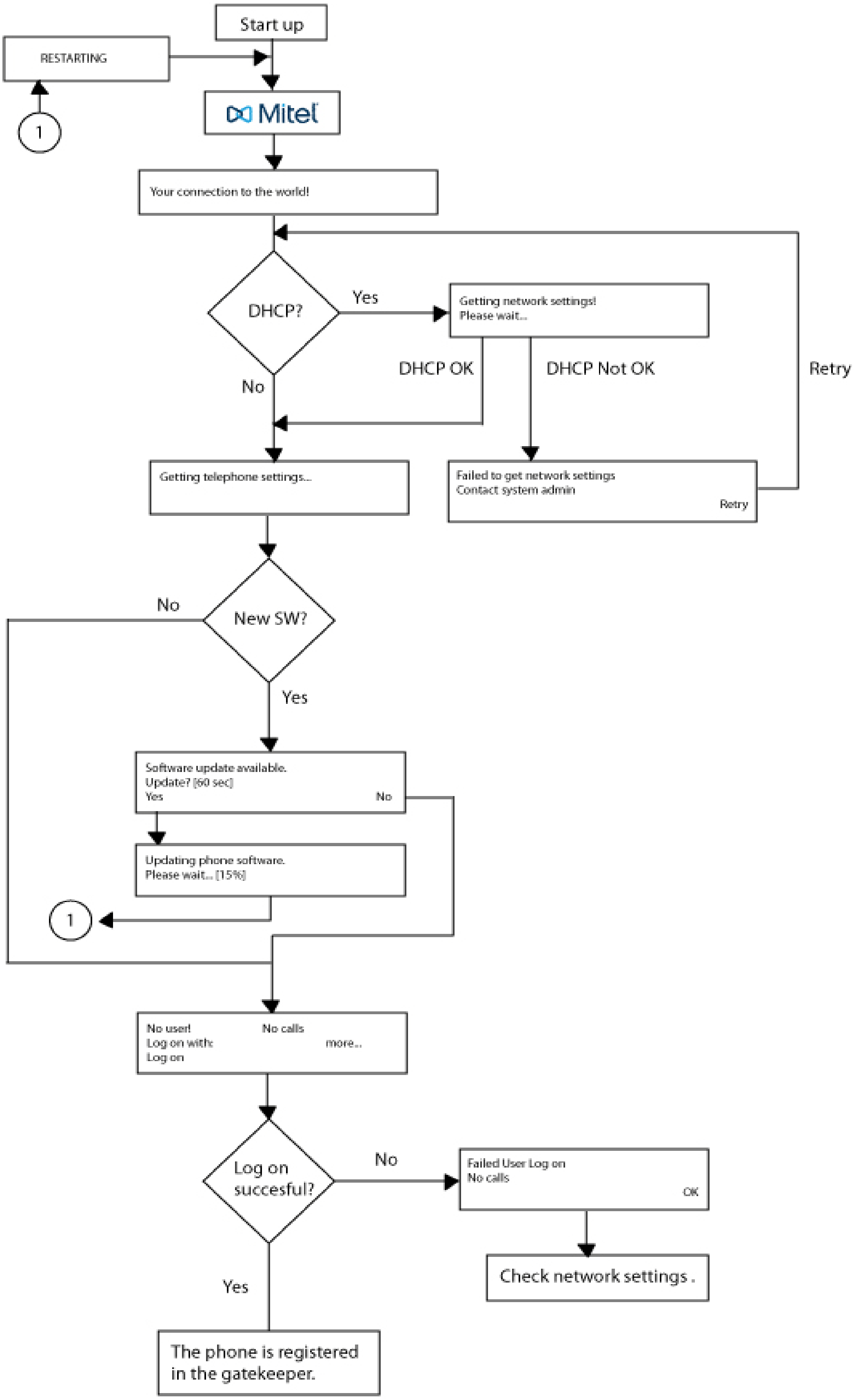


Figure 8: Installation Scenario Flow Chart

9.4 VIEWING SOFTWARE VERSION

It is possible to display versions of the software units (application, superboot, language file, KPU and DPU). Follow these steps:

1. Select Settings and enter administrator mode.
2. Select **Administrator** (**Administrator Settings** in DBC446)
3. Select **Information**.
4. Press navigation key (only DBC 43x) to view the versions of the different units.

An alternative is to initiate a manual self-test of the phone. Follow the steps below to view the currently installed software version of the phone:

1. Simultaneously press ☎⏻, *, and 4. (C, *, 4 in DBC446)
2. Press 1 on the keypad to view the software version (DBC 44x)
3. Close the software version dialog by pressing #.

If there is a fault in the configuration file, an error message is shown in bottom of the software version dialog.

10 RESTARTING THE PHONE

When restarting or powering up the phone, the configuration file is downloaded from the software server.

Software restart of DBC 43x and DBC 444:

The phone can be restarted manually using the following procedure:

1. Press ☎⏻ for a couple of seconds, until the question **Restart the phone?** is shown in the display.
2. Press **Select**.

An alternative way to restart the phone is:

1. Simultaneously press ☎⏻, #, and 🔇.

Software restart of DBC 446:

1. Press *C-key* for a couple of seconds, until the question **Restart the phone?** is shown in the display.
2. Press **Select**.

An alternative way to restart the phone is:

1. Simultaneously press *C-key*, #, and 🔇.

For instructions on how to restore factory defaults, restarting phones or using the phones' Web interface, see *Maintenance Instructions for DBC 43x and DBC 44x*.

All the network settings can be reset via the web interface, see *Maintenance Instructions for DBC 43x and DBC 44x.*

11 ENTERING ADMINISTRATOR MODE

Configuration of certain phone parameters can only be performed from the administrator mode.

When the phone is not registered and entering the administrator mode, the phone will read the configuration file from the software server.

After a period of inactivity, 10 minutes, administrator mode is terminated automatically

Follow the steps below to enter administrator mode:

DBC 43x and DBC 444

1. Simultaneously press ☎⏻, *****, and ***5***.
2. If required, enter the administrator password and press **Log on**. The feature to be forced to enter the administrator password can be enabled/disabled using a parameter in the configuration file.

Follow the steps below to exit administrator mode:

1. From the main dialog, press **more...**.
2. Select **Log off Administrator** and press **Select**.

DBC 446

1. Simultaneously press ***C**-key*, *****, and ***5.***
2. If required, enter the administrator password and press **Log on**. The feature to be forced to enter the administrator password can be enabled/disabled using a parameter in the configuration file.

Follow the steps below to exit administrator mode:

1. From the **Applications and Settings** menu, select **Log off Administrator**.

12 CONFIGURING THE PHONE

This chapter describes how to configure the phone as an administrator. Parameters that can be configured using the configuration file are indicated with a reference to *Configuration File for DBC 44X and DBC 43X*.

Note: For DBC 444 it is only the softkeys, the navigation keys and the function keys that are used at configuration. The shortcut keys to the right and to the left of the display are not used.

12.1 OVERVIEW OF PARAMETERS

This section describes the parameters used when configuring the phone. The parameters can be divided into the following categories:

- Network parameters
- Other parameters (user type mode and OMD).

12.1.1 NETWORK PARAMETERS

The following network parameters can be set in the phone:

- LAN access control (automatic or disabled)
- DHCP (enabled or disabled)
- The phone's IP address
- Subnet mask
- IP address to the default gateway
- Automatic setting of the IP address to the software server (enabled or disabled)
- IP address to the software server
- Proxy server (enabled or disabled)
- IP address to the proxy server
- Proxy port number
- Protocol. Shall always be set to H.323.
- Gatekeeper discovery (automatic setting of the IP address to the gatekeeper). Automatic, enabled, or disabled.
- IP address to the gatekeeper
- VLAN for the phone port
- Phone port VID
- VLAN for the PC port
- PC port VID.

12.1.2 OTHER PARAMETERS

Besides network parameters, the administrator mode is mandatory to set the following parameters:

- User type mode.
- OMD.
- Automatic answer.

12.2 SETTING NETWORK PARAMETERS

Here is the common procedure for setting one of the parameters in **Network**.

DBC 43x and DBC 444

1. Enter administrator mode, see 11 Entering Administrator Mode on page 24.
2. Press 🔧 .
3. Using the navigation keys ▲▼, select **Administrator**. Then press **Select**.
4. Select **Network** and press **Select**.
5. Select the wanted item and press **Select**.
6. Change the parameter value with the navigation keys ▲▼. Then press **Set**.
7. To exit the parameter settings list, press 🔧 .

If an IP address shall be changed:

For **DBC 43x**:

1. Delete the current IP address by pressing the left **Volume** button.
2. Enter an IP address using numeric keys *1* - *9*, then press **Set**. Dots are added automatically or using *.

For **DBC 444**:

1. Delete the current IP address by pressing the **Erase** softkey.
2. Enter an IP address using numeric keys *1* - *9*, then press **Set**. Dots are added automatically or using *.

DBC446

1. Enter administrator mode, see 11 Entering Administrator Mode on page 24.
2. Press ☰ .
3. Select **Administrator Settings**.
4. Select **Network**.
5. Select the wanted item and press **Select**.
6. Change the parameter value. Then press **Set**.
7. To exit the parameter settings list, press the **Back** softkey.

If an IP address shall be changed:

1. Delete the current IP address by pressing the **Erase** softkey.
2. Enter an IP address using numeric keys *1* - *9*, then press **Set**. Dots are added automatically or using *.

12.3 ENABLING AUTOMATIC LAN ACCESS CONTROL

The IEEE802.1x standard is used for port access control authentication. The LAN must support IEEE802.1x signaling and there must be a RADIUS server handling the authentication, according to EAP-MD5 or EAP-TLS. If the authentication is successful, the phone gets access to the LAN and continues with the ordinary start sequence.

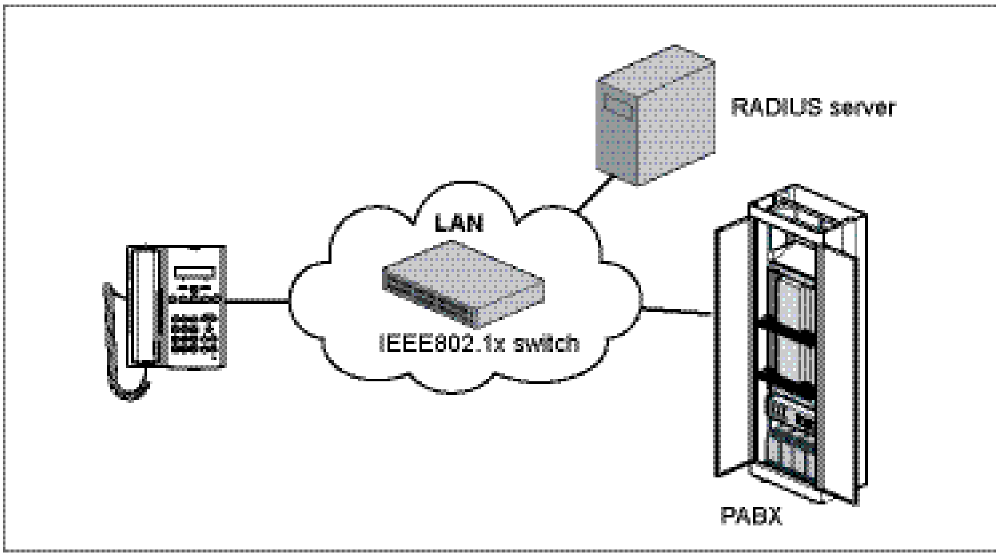


Figure 9: Components in LAN access control

Before the authentication the phone cannot get access to the LAN or even get the IP address from the DHCP server. The authentication is performed periodically (intervals as defined by the LAN switch). If the LAN does not support IEEE802.1x, the phone will start in the ordinary way.

If a PC shall be connected to the PC port in the phone, the phone supports that the PC and the phone are authenticated independent of each other.

Note: The LAN switch must support that two devices are authenticated independent of each other on the same LAN port.

Follow the steps below to enable automatic LAN access control from the phone:

1. Enter the network settings menu, see 12.2 Setting Network Parameters on page 26.
2. Select **LAN access ctrl. (Auto)** for DBC 43x and **LAN access control (Auto)** for DBC 44x.

Note: If parameters regarding automatic LAN access control are configured in the configuration file, the settings made from the phone will be overwritten when the configuration file is reloaded (for example, at restart).

12.3.1 EAP-MD5

The authentication process is initiated during the start up sequence. The phone prompts for a user identity and password. If the authentication is successful the telephone continues with the ordinary start sequence.

At restart of the phone, and when the user identity and password are stored in the phone, the ordinary restart procedure is done which means that the user does not have to do anything.

The following LAN access control parameter settings can be made in the configuration file when using EAP-MD5:

- Storage of LAN access control user identity and password in the phone or not.
- Whether the LAN access control user identity and password is valid for *the phone* or for *the end user*. In the first case the phone do not log off from the LAN when registering with a different extension number towards the PBX. In the second case, the phone shall log off from the LAN when entering a different extension number.
- LAN access control user identity and password, which can be used when all the phones shall have the same user identity and password.

For more information on how to configure LAN access control using the configuration file, see *Configuration File for DBC 44X and DBC 43X*.

12.3.2 EAP-TLS

When using EAP-TLS the authentication is done with a certificate and the telephone does not show any prompt for the user to enter a user identity and password.

The digital certificates must be in X.509 version 3 format with the file extension **.pem**.

The certificates must be downloaded from the software server to the telephone. The file must be stored under the folder ***/certificates/8021X***, see 7.2 Creating a Directory Structure on page 11.

For detailed information how to create and install the certificates, see 12.3.3 Example of How to Create and Install the Certificates on page 28.

If the error message *LAN Access Control EAP-TLS failure* is shown in the display check the following:

- The Radius server is running ok.
- The definition of the root and client certificates are correct in the configuration file.
- The definition of the client key and client key password are correct in the configuration file.
- That the certificate files are stored under the correct path on the software server, see 7.2 Creating a Directory Structure on page 11

Note: It is important to keep track of the expire date for the certificate. If the date expires, the phones cannot access the LAN.

12.3.3 EXAMPLE OF HOW TO CREATE AND INSTALL THE CERTIFICATES

There are a number of ways to generate the certificates but this is not described in this document. Below is a description of how to convert the files to the format that the telephones can use.

First step is to convert from PKCS12 to PEM format by using the *openssl* command in a Linux or a Windows environment:

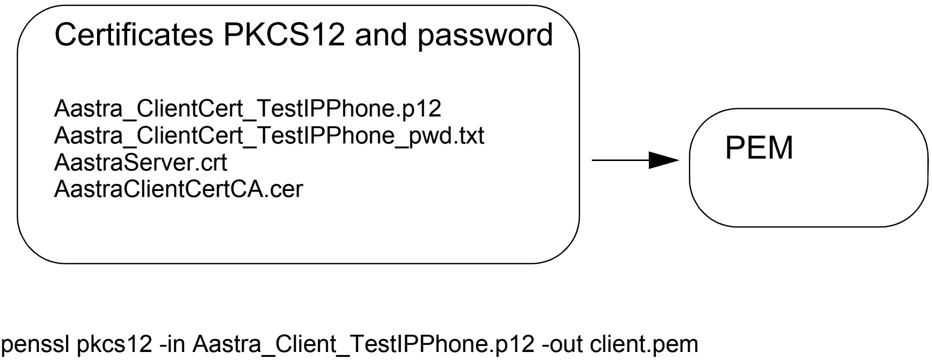

Certificates PKCS12 and password
Aastra_ClientCert_TestIPPhone.p12
Aastra_ClientCert_TestIPPhone_pwd.txt
AastraServer.crt
AastraClientCertCA.cer
PEM
openssl pkcs12 -in Aastra_Client_TestIPPhone.p12 -out client.pem

Figure 10: Convert from PKCS12 to PEM format

The command will ask for a password to decrypt the **.p12** file. It will also ask for a *pass phrase* to encrypt the private key in the **client.pem** file. The file consists of one certificate part and one private key part.

Next step is to create the different certificate files.

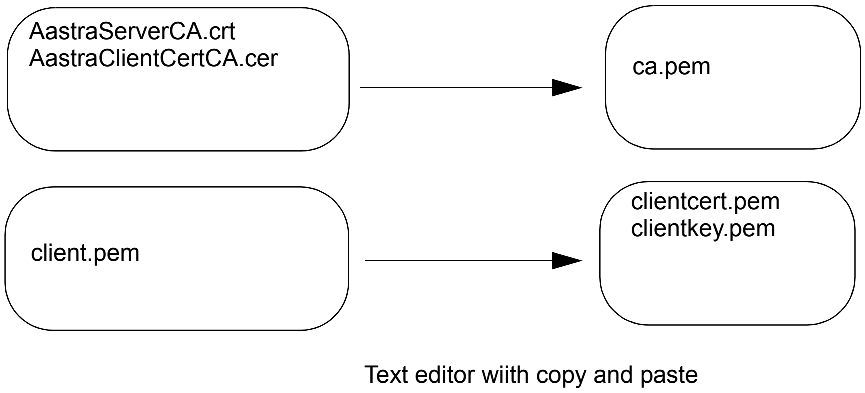


Figure 11: Create the different certificate files

Use a text editor and copy the private key part of *client.pem* to *clientkey.pem* and the certificate part to *clientcert.pem*.

Next step is to remove the encryption of the private key because the phone does not work with encrypted key. This is also done with the openssl command on the *clientkey.pem* file. When this is done check that the heading looks like this:

/* -----BEGIN PRIVATE KEY------ */

It must not have the following text:

/* -----BEGIN ENCRYPTED PRIVATE KEY------ */

Next step is to generate a random binary file by using any random data generator.

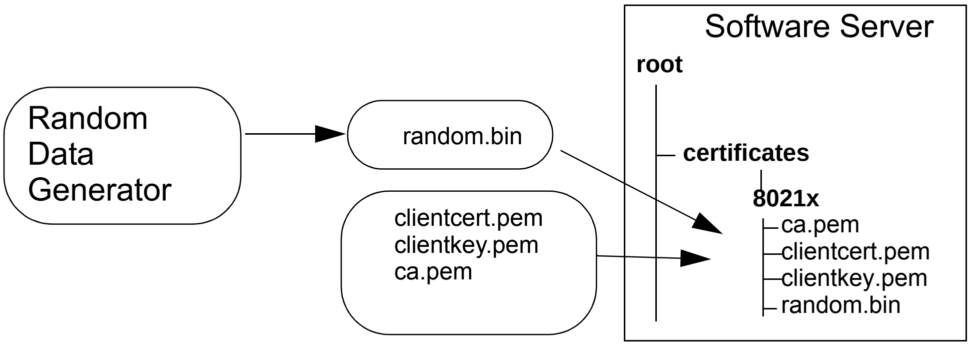


Figure 12: Create the random.bin file and store on SW server

Store the certificate files on the software server.

Note: The *.pem* files must be in unix format.

Edit the configuration file for the telephones. Below is an example:

```
[802.1x]
LANAccessControl=AUTO
StoreUserIdPassword=YES
UserType=PHONE
UserIdentity=Aastra
UserPassword=Aastra
EAP_TLS=ENABLED
RootCert=cacert.pem
ClientCert=clientcert.pem
ClientKey=clientkey.pem
ClientKeyPassw=ZVtTnyE187
RandomFile=random.bin
```

For more information of the parameters, see description of *Configuration File for DBC 44X and DBC 43X*.

Next step is to configure the LAN switch to install the certificates on the telephones. The 802.1x check in the LAN switches shall be disabled. All the phones are restarted to read the configuration file and certificates.

Finally when the certificates are stored in the telephones, the LAN switches shall be enabled for 802.1x again.

12.3.4 CONFIGURING LAN ACCESS CONTROL USING THE CONFIGURATION FILE

The LAN access control parameter values set from the phone are valid until the configuration file is read by the phone. To keep the parameter settings made from the phone during a restart, the corresponding parameter settings in the configuration file must be done.

The following LAN access control parameters are common for both security protocols in the configuration file:

- LAN access control (Auto or No).
- Select if EAP-MD5 or EAP-TLS shall be used.

For more information on how to configure LAN access control using the configuration file, see *Configuration File for DBC 44X and DBC 43X*.

12.3.5 CONFIGURATION EXAMPLES (USING EAP-MD5)

One typical case with basic level of security can be that all phones have the same user identity and password. The configuration of all the phones must be done via a switch where IEEE802.1x is disabled. Using the default values the following configuration will be needed:

- Automatic IEEE802.1x detection (default).
- Define the user identity and the password in the configuration file.
- The user identity and password are stored in the phone (default).
- The user identity is valid for the phone, which means that the end-user can change extension number towards the PBX, without having to enter a new LAN access user identity and password (default value).
- Start the phone via the IEEE802.1x disabled switch. The phone will read and store the user identity and password from the configuration file.
- Set out the phone to the end-user and start it via the IEEE802.1x enabled switch.

Another typical case with a higher level of security is that each phone has individual user identity and password:

- Automatic IEEE802.1 detection (default).
- The user identity and password are stored in the phone (default).
- The system administrator or end-user have to enter the LAN access control user identity and password when starting the phone only the first time.
- The user identity is valid for the phone, which means that the user can change extension number towards the PBX, without having to enter a new LAN access user identity and password (default value).

12.4 DISABLING AUTOMATIC LAN ACCESS CONTROL

Note: If parameters regarding automatic LAN access control are configured in the configuration file, the settings made from the phone will be overwritten when the configuration file is reloaded (at, for example, a restart).

Follow the steps below to disable automatic LAN access control from the phone:

1. Enter the network settings menu, see 12.2 Setting Network Parameters on page 26.
2. Select **LAN access control. (No)**.

12.5 ENABLING LLDP-MED

The Link Layer Discovery Protocol (LLDP) is a vendor-neutral Link Layer protocol used by network devices for advertising their identity, capabilities, and neighbors. The Media Endpoint Discovery is an enhancement of LLDP, known as LLDP-MED. The DBC43x and DBC44x telephones can use this protocol for auto-discovery of the network policy such as VLAN identity and priority.

For information about the priority for the VLAN identity between the different methods, see 12.18 Using Virtual LAN (VLAN) on page 38.

The telephone sends also information in the outgoing LLDP packets for inventory management, allowing network administrators to track their network devices, and determine their characteristics such as:

- Telephone model (DBC433, DBC 434 etc.), hardware revision, firmware revision, serial number
- IP address, MAC address of the phone
- System name and system description = “Aastra IP Phone”
- Power consumption

LLDP-MED is enabled by default. It is possible to disable via a parameter in the configuration file, see description of Configuration file for DBC43x and DBC44x.

The startup sequence is IEEE802.1x -> LLDP-MED -> DHCP. After IEEE802.1x is successfully authenticated, LLDP packets will be sent from the phone to the LAN switch. The phone waits for reply for a short while and then continue with the DHCP signaling.

When the phone receives a changed LAN identity in the LLDP message, the telephone reboots to be able to use the new id.

If LLDP is disabled in the configuration file in a running system and if LLDP shall be enabled, the configuration file with the changed LLDP parameter must be read in from the existing VLAN configuration before the telephone can get the new VLAN information via LLDP.

12.5.1 EXAMPLE WITH CONFIGURATION OF CISCO CATALYST 3560

Below is an example of the configuration of a Cisco Catalyst 3560 and with VLAN identity 51:

Enable LLDP

```
lldp run
```

Port config

```
interface FastEthernet0/9
switchport mode access
switchport voice vlan 51
switchport port-security maximum 2
switchport port-security
switchport port-security aging time 2
switchport port-security violation restrict
switchport port-security aging type inactivity
srr-queue bandwidth share 10 10 60 20
priority-queue out
mls qos trust device cisco-phone
mls qos trust cos
auto qos voip cisco-phone
macro description cisco-phone
spanning-tree portfast
spanning-tree bpduguard enable
service-policy input AutoQoS-Police-CiscoPhone
```

The information that the Cisco switch has received from the telephone can also be showed. Below is an example with a DBC433 terminal:

```
Chassis id: 192.168.51.111
```

```
Port id: 0008.5d70.ea6a
Port Description: esw 0
System Name: Aastra IP Phone
System Description: Aastra IP Phone
H/W revision: R1D
S/W revision: Appl/Boot versions: P2A1t14/P1A4
Manufacturer: Aastra
Model: DBC433
Capabilities: NP, PD, IN
Device type: Endpoint Class III
Network Policy(Voice): VLAN 51, tagged, Layer-2 priority: 6, DSCP: 0
PD device, Power source: Unknown, Power Priority: High, Wattage: 3.8
Location - not advertised
```

12.6 ENABLING DHCP

Follow the steps below to enable DHCP:

1. Enter the network settings menu, see 12.2 Setting Network Parameters on page 26.
2. Select **DHCP (Yes)**.

12.7 DISABLING DHCP

Follow the steps below to disable DHCP:

1. Enter the network settings menu, see 12.2 Setting Network Parameters on page 26.
2. Select **DHCP (No)**.

12.8 SETTING THE PHONE'S IP ADDRESS

If DHCP is used, the phone's IP address is set automatically, using the DHCP server. To be able to set the phone's IP address manually, DHCP must be disabled on the phone.

Follow the steps below to set the phone's IP address manually from the phone:

1. Enter the network settings menu, see 12.2 Setting Network Parameters on page 26.
2. Select **DHCP (No)** and make sure DHCP is disabled.
3. Select **IPadd (<current IP address>)** for DBC 43x and **IP address (<current IP address>)** for DBC 44x.
4. Enter the new IP address.

12.9 SETTING THE SUBNET MASK

If DHCP is used, the subnet mask is set automatically, using the DHCP server. To be able to set the subnet mask manually, DHCP must be disabled on the phone.

Follow the steps below to set the subnet mask manually from the phone:

1. Enter the network settings menu, see 12.2 Setting Network Parameters on page 26.
2. Select **DHCP (No)** and make sure DHCP is disabled.
3. Select **Mask (<current subnet mask>)** for DBC 43x and **Subnet Mask (<current subnet mask>)** for DBC 44x.
4. Enter the new subnet mask.

12.10 SETTING THE IP ADDRESS TO THE DEFAULT GATEWAY

If DHCP is used, the IP address to the default gateway is set automatically, using the DHCP server. To be able to set the IP address to the default gateway manually, DHCP must be disabled on the phone.

Follow the steps below to set the IP address to the default gateway:

1. Enter the network settings menu, see 12.2 Setting Network Parameters on page 26
2. Select **DHCP (No)** and make sure DHCP is disabled. .
3. Select **D GW (<current IP address>)** for DBC 43x and **Default Gateway (<current IP address>)** for DBC 44x
4. Enter the new IP address.

12.11 SETTING THE IP ADDRESS OF THE SOFTWARE SERVER

To download the phone software from the software server, the phone must be configured with the IP address of the software server. This IP address can be set using the following alternatives (priorities as listed):

- Manually from the phone, as described below, or via the administrator web interface.
- Automatically using DHCP, see 25.2 Data from DHCP on page 89.
- Automatically using DNS SRV resource records, see 12.26 Using DNS SRV Resource Records on page 48.

Follow the steps below to configure the phone with the IP address of the software server manually from the phone:

1. Enter the network settings menu, see 12.2 Setting Network Parameters on page 26
2. Select **Auto SW Server (No)** and make sure it is disabled.
3. Select **SWsrv (<current IP address>)** for DBC 43x and **SW server (<current IP address>)** for DBC 44x.
4. Enter the IP address.

12.12 ENABLING AUTOMATIC SETTING OF THE IP ADDRESS OF THE SOFTWARE SERVER

The phone can be configured for automatic setting of the IP address of the software server using DHCP or DNS. For more information, see 12.26 Using DNS SRV Resource Records on page 48.

Note: Automatic setting of the IP address of the software server using DNS requires DHCP.

Follow the steps below to enable automatic setting of the IP address of the software server:

1. Enter the network settings menu, see 12.2 Setting Network Parameters on page 26.
2. Select **DHCP (Yes)** and make sure DHCP is enabled.
3. Select **Auto SW Server (Yes).** The phone will restart to get the IP address to the SW server from DHCP or DNS.

12.13 DISABLING AUTOMATIC SETTING OF THE IP ADDRESS OF THE SOFTWARE SERVER

Follow the steps below to disable automatic setting of the IP address of the software server:

1. Enter the network settings menu, see 12.2 Setting Network Parameters on page 26.
2. Select **Auto SW Server (No)** to disable the automatic SW server address.

12.14 USING A PROXY SERVER

If the software server is outside a firewall, a proxy server must be used. The phone can be configured with an IP address to the proxy server using one of the following methods:

- Using DHCP, see 25.2 Data from DHCP on page 89.
- Manually, as described below.

12.14.1 ENABLING THE USE OF A PROXY SERVER

If the software server is outside a firewall, a proxy server must be used. Follow the steps below to enable the use of a proxy server:

1. Enter the network settings menu, see 12.2 Setting Network Parameters on page 26.
2. Select **Proxy Server (Yes)** and enable the use of proxy server.

12.14.2 DISABLING THE USE OF A PROXY SERVER

Follow the steps below to disable the use of a proxy server:

1. Enter the network settings menu, see 12.2 Setting Network Parameters on page 26.
2. Select **Proxy Server (No)** and disable the use of proxy server.

12.14.3 SETTING THE IP ADDRESS TO THE PROXY SERVER

If the software server is outside a firewall and a proxy server is used, an IP address to the proxy server must be set. Follow the steps below to set the IP address to the proxy server manually from the phone:

1. Enter the network settings menu, see 12.2 Setting Network Parameters on page 26.
2. Select **Proxy Server (Yes)** and make sure it is enabled.
3. Select **Proxy (<current IP address>)**.
4. Enter the IP address.

12.14.4 SETTING THE PROXY PORT

If the software server is outside a firewall and a proxy server is used, a proxy port must be set. Follow the steps below to set the proxy port:

1. Enter the network settings menu, see 12.2 Setting Network Parameters on page 26.
2. Select **Proxy Server (Yes)** and make sure it is enabled.
3. Select **Proxy Port (<current port>)**.
4. Enter the port number.

12.15 SETTING THE IP ADDRESS OF THE GATEKEEPER

The phone is configured with the IP address of the gatekeeper using one of the following methods:

1. Using automatic gatekeeper discovery (with multi-cast signaling), see 12.16 Enabling Automatic Gatekeeper Discovery on page 37.
2. By defining the IP address to a *primary gatekeeper* in the configuration file, see *Configuration File for DBC 44X and DBC 43X*. When configuring the IP address to the gatekeeper using the configuration file, automatic gatekeeper discovery must be disabled.
3. By defining the IP address to a *secondary gatekeeper* in the configuration file, see *Configuration File for DBC 44X and DBC 43X*. The secondary gatekeeper is used when the primary gatekeeper is not available. When configuring the IP address to the gatekeeper using the configuration file, automatic gatekeeper discovery must be disabled.
4. From the phone, as described below. When configuring the IP address to the gatekeeper from the phone, automatic gatekeeper discovery must be disabled.
5. (Branch offices only.) By defining a backup gatekeeper IP address in the configuration file. The backup gatekeeper IP address is used when the connection between a branch office and a main site is lost, to make sure that calls can still be made from the branch office.

The table below shows which method that will be used depending on the settings in the menus in the phone and in the configuration file. 1-5 refer to the methods listed above.

Settings in menus	Backup GK Yes	Backup GK No	Settings in the configuration file
GateKeeper discovery (Yes)	1,5	1	Any value
GateKeeper discovery (No)	4,5	4	Any value
GateKeeper discovery Auto (Yes)	1,5	1	GK discovery = Yes
GateKeeper discovery Auto (No)	2,3,5	2,3	GK discovery = No. Primary and secondary choice available
GateKeeper discovery Auto (No)	4,5	4	GK discovery = No. Primary and secondary choice not available

Follow the steps below to set the IP address to the gatekeeper manually from the phone:

1. Enter the network settings menu, see 12.2 Setting Network Parameters on page 26.
2. Select **GK Discovery (No)** for DBC 43x and **Gatekeeper Discovery (No)** for DBC 44x.
3. Select **GK (<current gatekeeper address>)** for DBC 43x and **Gatekeeper (<current gatekeeper address>)** for DBC 44x.
4. Enter the IP address.

Follow the steps below to set the IP address to the gatekeeper via the configuration file:

1. Enter the network settings menu, see 12.2 Setting Network Parameters on page 26.
2. Select **GK Discovery ()** for DBC 43x and **Gatekeeper Discovery ()** for DBC 44x.
3. Select the parameter value **Auto (No)**

12.16 ENABLING AUTOMATIC GATEKEEPER DISCOVERY

Note: Only certain gatekeepers (PBX systems) have support for automatic gatekeeper discovery.

Automatic gatekeeper discovery is a method to find a gatekeeper (PBX) to register to. When this method is used, the IP phone sends a multi-cast message (Gatekeeper Discovery Request) and waits for a confirmation. Several confirmation messages can be received.

The phone can send the domain name to inform the gatekeeper which domain the phone belongs to. The domain name can be received from DHCP or from the configuration file, see the description for *Configuration File for DBC 44X and DBC 43X*. The domain name provided by DHCP has priority over the domain name defined in the configuration file.

The identity of the gatekeeper to which the phone is to be registered can be defined in the configuration file. See data identifier **GatekeeperID** in the description for *Configuration File for DBC 44X and DBC 43X*.

The use, or not, of automatic gatekeeper discovery can be defined in the configuration file and in the settings menu. By default the phone uses the value defined in the configuration file.

Follow the steps below to enable automatic gatekeeper discovery from the phone:

1. Enter the network settings menu, see 12.2 Setting Network Parameters on page 26.
2. Select **GK Discovery ()**.
3. Select the parameter value **Auto** and make sure that the parameter value in the configuration file is set to YES.
4. Alternatively select the parameter value **Yes** and in this case the parameter value in the configuration file is not considered. This option can be used of one special phone shall use automatic gatekeeper discovery but not the rest of the phones.

12.17 DISABLING AUTOMATIC GATEKEEPER DISCOVERY

Automatic gatekeeper discovery can be disabled from the phone or using the configuration file. When automatic gatekeeper discovery is disabled, the IP address to the gatekeeper must be configured manually from the phone or using the configuration file. For information on how to disable automatic gatekeeper discovery for all phones in a domain using the configuration file, see *Configuration File for DBC 44X and DBC 43X*.

For information on how to set the IP address to the gatekeeper manually from the phone, see 12.15 Setting the IP Address of the Gatekeeper on page 36. By default, the setting in the configuration file is used.

Follow the steps below to disable automatic gatekeeper discovery from the phone:

1. Enter the network settings menu, see 12.2 Setting Network Parameters on page 26
2. Select **GK Discovery ()**.
3. Select the parameter value **No** it the address shall be set manually or **Auto (No)** if the address shall be retrieved from the configuration file.

12.18 USING VIRTUAL LAN (VLAN)

The built-in Ethernet switch can handle virtual LAN identities and priorities for the phone and PC ports.

The following configuration alternatives are available:

- Automatic setting of VLAN (default). With this setting, VLAN configuration is performed using one of the following alternatives:
  - LLDP-MED. This method can be used for configuring the phone port only (not the PC port). See12.5 Enabling LLDP-MED on page 31.
  - DHCP (option 43). This method can be used for configuring the phone port only (not the PC port).
  - The configuration file. This method can be used for configuring the phone and PC ports. Please note that the configuration file contains parameters both for enabling VLAN and for defining VLAN identifiers. For information on how to configure VLAN using the configuration file, see 12.18.1 Config-

uring VLAN Identities Using the Configuration File on page 39 and *Configuration File for DBC 44X and DBC 43X*.

- VLAN disabled. VLAN is disabled from the phone.
- Manually from the phone. This method can be used for configuring the phone and PC ports.

The priority for the VLAN identity between the different methods are:

1. Manual setting of the VLAN identity
2. LLDP-MED
3. DHCP option 43
4. Configuration file

The **VLAN for Phone()** setting in the phone can have the default value **Auto** even when VLAN is not used.

Concerning the priority of the frames

For outgoing frames the following priorities will be set at level 2 for each frame by default, when VLAN is used:

- For frames **originating in the phone** the default value will be 6, meaning voice traffic with less than 10 ms latency.
- For frames **originating in the PC** the default value is 0, meaning best effort.

The priorities can be changed via the configuration file, see the description for *Configuration File for DBC 44X and DBC 43X*.

12.18.1 CONFIGURING VLAN IDENTITIES USING THE CONFIGURATION FILE

For detailed information on how to assign VLAN identities using the configuration file, see *Configuration File for DBC 44X and DBC 43X*.

The configuration file is read from the native LAN

At installation (and power restart) the phone asks for an IP address from DHCP by initiating the DHCP negotiation with untagged messages (native LAN). DHCP provides the IP address but no VLAN identity list. The phone reads the configuration file, but in this case when no VLAN identity list is received from DHCP, a software restart of the phone is performed automatically to get the IP address valid for the tagged VLAN defined in the configuration file.

The configuration file is read from the VLAN

At installation (and power restart), when the configuration file is available in the VLAN but not in the native LAN, the VLAN identity must be set manually from the phone.

12.18.2 ENABLING VIRTUAL LAN (VLAN) FOR THE PHONE PORT

The built-in Ethernet switch can handle virtual LAN identities and priorities for the phone port.

The VLAN parameters can be set automatically using DHCP (option 43) or the configuration file, or manually from the phone.

12.18.2.1 *Enabling Automatic Setting of Phone Port VLAN Parameters*

By enabling automatic setting of the VLAN parameters of the phone port, the VLAN parameters are set automatically using DHCP or the configuration file, where the DHCP setting has the highest priority. For information on how to set VLAN parameters using the configuration file, see *Configuration File for DBC 44X and DBC 43X*.

When using automatic VLAN detection using DHCP, only the phone port is included. A list of three VLAN identities can be handled.

Note: Automatic setting of VLAN parameters using DHCP does not include the PC port.

Prerequisites on the LAN

When the phone is connected to a layer 2 switch, the switch will add the IEEEE 802.1Q header, to untagged frames with the default VLAN identity and forward the frames. The first layer 3 switch must be initiated for DHCP relay and having an ingress port with an IP address on each of the offered VLANs. The address to the DHCP server must be set in the layer 3 switch.

When the layer 3 switch has received a *DHCP discover* message, it will forward this packet to the DHCP server adding the IP address of its ingress port corresponding to the VLAN. It is this address information that informs the DHCP server to which IP subnet that this phone is to be assigned to.

Description of when a VLAN identity list is received from the native LAN

At installation (and power restart) the phone asks for a temporary IP address from DHCP by initiating the DHCP negotiation with untagged messages (native LAN). The relay agent adds the address of its ingress port corresponding to the native LAN. DHCP provides the temporary IP address together with the VLAN identity list. The phone releases the temporary IP address.

Then the phone uses the first VLAN identity in the list and sends a new tagged request to the DHCP server. The relay agent adds the address of the ingress port corresponding to the **selected** VLAN. If there is any available IP address, the DHCP server provides this address to the phone. If there is no available IP address for this VLAN, the phone takes the next VLAN id in the list and asks for an IP address.

If there is no IP address available in any VLAN in the list, the phone will ask for an IP address in the native LAN.

Restart

It is possible to specify in the configuration file whether the phone should retain the previously used VLAN identity after reboot, or whether it should start a new automatic VLAN detection procedure. See description for Configuration file for DBC 44x and DBC 43x.

Enable automatic setting of VLAN parameters

Follow the steps below to enable automatic setting of VLAN parameters for the phone port from the phone:

1. Enter the network settings menu, see 12.2 Setting Network Parameters on page 26
2. Select **VLAN for Phone ()** for DBC 43x and **VLAN for Phone Port ()** for DBC 44x.
3. Select the parameter value **Auto**.

12.18.2.2 *Enabling Manual Setting of Phone Port VLAN Parameters*

Follow the steps below to enable manual setting of VLAN parameters for the phone port manually from the phone:

1. Enter the network settings menu, see 12.2 Setting Network Parameters on page 26
2. Select **VLAN for Phone ()**
3. Select the parameter value **Manual**
4. Select **Phone Port VID ()**. Enter the VLAN identity (1-4094) for the phone port using numeric keys *1 - 9*

Note: If the manual settings of the VLAN parameters shall remain after a software upgrade, all the VLAN settings in the configuration file have to be disabled.

12.18.2.3 *Setting the Phone Port VLAN Identity*

When the VLAN identity for the phone port shall be set manually, see 12.18.2.2 Enabling Manual Setting of Phone Port VLAN Parameters on page 41

12.18.3 DISABLING VIRTUAL LAN (VLAN) FOR THE PHONE PORT

Follow the steps below to disable VLAN manually from the phone:

1. Enter the network settings menu, see 12.2 Setting Network Parameters on page 26
2. Select **VLAN for Phone ()**.
3. Select the parameter value **No**.

12.18.4 ENABLING VIRTUAL LAN (VLAN) FOR THE PC PORT

The built-in Ethernet switch can handle virtual LAN identities and priorities for the PC port.

12.18.4.1 *Enabling Manual Setting of PC Port VLAN Parameters*

Follow the steps below to enable manual setting of VLAN parameters for the PC port manually from the phone:

1. Enter the network settings menu, see 12.2 Setting Network Parameters on page 26.
2. Select **VLAN for PC()** for DBC 43x or **VLAN for PC Port()** for DBC 44x.
3. Select the parameter value **Yes**.
4. Select **PC Port VID ()** and enter the VLAN identity (1-4094) for the PC port using numeric keys *1 - 9*.

12.18.4.2 *Setting the PC Port VLAN Identity*

When the VLAN identity for the PC port shall be set manually, see 12.18.4.1 Enabling Manual Setting of PC Port VLAN Parameters on page 41.

12.18.5 DISABLING VIRTUAL LAN (VLAN) FOR THE PC PORT

Follow the steps below to disable VLAN for the PC port manually from the phone:

1. Enter the network settings menu, see 12.2 Setting Network Parameters on page 26.
2. Select **VLAN for PC ()**.
3. Select the parameter value **No**.

12.18.6 SECURE MAC ADDRESS TABLE

In Cisco LAN switches there is a command (*switchport port-Security maximum n*) to set the maximum number of MAC addresses that are allowed to send traffic into the port. Note that untagged messages from one MAC address and tagged messages from the same MAC address are regarded as two entries in the secure mac address table.

This means that when starting the phone and when the PC is connected, the following is visible in the secure MAC address table:

1. MAC address for the PC in native VLAN (untagged messages from the PC).
2. MAC address for the phone in the native VLAN (untagged messages from the phone).
3. MAC address for the phone in the voice VLAN (tagged messages from the phone).

In this example *switchport port-Security maximum* must be set to 3.

Note: The DBC42x IP phones work different; these phones have a boot and when the boot hands over to the application, layer 2 disappears for a short while which means that the first two entries in the secure mac address table are erased. When the application starts the first and the third entry will occur in the example above. For these phones *switchport port-Security maximum* can be set to 2.

12.19 SETTING USER TYPE MODE

The following user type modes are available on the phone:

- Free user.

  Any user can log on to the phone.

- Permanent user

  The phone is always logged on, using a default user. Only administrators can log on or off. This option can be used for phones in conference rooms, receptions etc. To avoid accidental log off, the default user must have a password or PIN code. If a user is logged on when changing the user type to permanent, the currently logged on user will be set as the default user. If no user is logged on when changing the user type to permanent, the user used for the next log on will be set as the default user (this scenario is only valid when logged on as administrator).

- Temporary user

  Same as for the permanent user mode, with the exception that temporary users can log on and off to the phone. This option can be used in for example, a free seating environment. When users log off, the phone automatically logs on again, using the default user. Temporary users that are not logged off are logged off automatically during night. The phone then logs on using the default user.

Follow the steps below to set the user type from the phone:

DBC43x and DBC444

1. Enter administrator mode, see 11 Entering Administrator Mode on page 24.
2. Press 🔧 .
3. Using the navigation keys ▲▼, select **Administrator**.
4. Select **User**
5. Using the navigation keys ▲▼ and select the wanted user type.

DBC 446

1. Enter administrator mode, see 11 Entering Administrator Mode on page 24.
2. Press 📋 .
3. Select **Administrator Settings**.
4. Select **User**
5. Select the wanted user type.

12.19.1 CONFIGURING USER TYPE USING THE CONFIGURATION FILE

If all the phones in a domain shall have one of the options *permanent user* or *temporary user,* it is possible to set the parameter *LogOffRestriction* in the configuration file. In this case the phones will get the directory number that is currently logged on as the default number.

If the option *free user* is used, and if the phones shall be forced to log off at a certain time, it is possible to enable the parameter *LogOffTime* in the configuration file and set the time.

When the parameter *LogOffRestriction* is used in the configuration file, it is not possible to change the user type mode locally in each phone. These options are grey in the menu and the **Save** key is missing.

If the phone is not automatically logged on after the configuration file is read, the default user and password or PIN code can be configured using one of the following methods:

- By entering administrator mode. When the **Log on with** menu appears, log on with the default user and password or PIN code.
- Using the administrator web interface.

12.20 SETTING TIME AND DATE

Time and date can be set using the following alternatives:

- WAP messages. For PBX's supporting WAP, the time in the IP phone is updated automatically as soon as the phone is registered towards the PBX.
- SNTP (Simple Network Time Protocol). The time in the phone can be set via SNTP, as described below. This method must also be used if security is enabled (with validation of the server certificate) in the phones and in the system.

If the SNTP server is enabled and defined in the configuration file, the phone will take the time from the SNTP server.

12.20.1 SIMPLE NETWORK TIME PROTOCOL

When SNTP is available in the LAN, the time and date in the phone are updated automatically when the phone is started and is verified periodically. If SNTP is used, the IP address and the Time zone will be set in the configuration file, see *Configuration File for DBC 44X and DBC 43X*.

If the LAN does not have SNTP or NTP available, a server with SNTP software has to be initiated.

12.21 CONFIGURING LANGUAGE SETTINGS

The language file contains the text strings used by the phone. The file is stored on the software server and loaded to the phone during power up. For information on how to change text strings in the language file, see *LANGUAGE FILE FOR DBC 43X*.

For information on how to change a user's language settings from the phone, see *Mitel User Guide for each telephone model.*

12.22 USING SHORTCUT KEYS

The shortcut keys can be assigned to:

- Functions (for example, call back or follow me)
- Phone numbers or procedures with * and #. (TNS keys)
- Monitored extensions (MNS keys).

There are no shortcut keys on DBC 433.

Note: When using Provisioning Manager (PM) it is possible to fetch the current programming of the shortcut keys. The first step is to set the terminal administrator password in MP:

System > **Subsystem** > create or change > **Terminal Password**

After this it is possible for MP to fetch the key data.

With a parameter in the configuration file it is possible to not show the **Reject** softkey and to disable the reject function of the **Clear** key.

Display panel units (DPU) and Key panel units (KPU) can be connected to DBC434 and to DBC444.

12.22.1 SHORTCUT KEYS IN DBC 434

In this phone, there are 8 shortcut key positions available.

12.22.2 SHORTCUT KEYS IN DBC 444

In this phone, there are 80 shortcut key positions available. There are virtual pages with shortcuts and there are soft keys to browse to next or previous page.

There is a pop up option for monitor (MNS) keys, which means that the page containing the monitor key is displayed when e.g. a call to the monitored extension is received. This feature is enabled via the configuration file.

By attaching a DPU it is possible to see the first page on the phone and the next 24 shortcuts on the DPU. The remaining 48 shortcuts are available as virtual pages on the phone.

By attaching two DPUs it is possible to see 8+24+24=56 shortcuts. The remaining 24 shortcuts are available as virtual shortcut pages.

12.22.3 SHORTCUT KEYS IN DBC 446

In this phone, there are 80 shortcut key positions available. There are virtual pages with shortcuts and there are soft keys to browse to next or previous page.

There is a pop up option for monitor (MNS) keys, which means that the page containing the monitor key is displayed when e.g. a call to the monitored extension is received. This feature is enabled via the configuration file.

It is not possible to attach any DPU or KPU to this model.

12.22.4 ASSIGNING FUNCTIONS TO SHORTCUT KEYS

Using the configuration file, the shortcut keys can be assigned to call functions such as callback, conference calls, or follow me. For instructions on how to assign a function to a shortcut key, see *Configuration File for DBC 44X and DBC 43X*. Assignment of functions to shortcut keys can only be performed by administrators via the configuration file or via commands in the PBX.

12.22.5 ASSIGNING PHONE NUMBERS TO SHORTCUT KEYS (TNS KEYS)

Shortcut keys that are not assigned to functions or monitored extensions can be assigned to phone numbers, here called TNS keys. By pressing a TNS key, a call to the phone number is initiated.

Assignment of phone numbers to shortcut keys is made by the user from the phone or the phone's web interface. It is also possible to initiate the TNS number from the PBX.

When initiating a TNS key, the data is stored locally in the phone, in the PBX, or in a file on an FTP server (for information on storing user specific data using an FTP server, see 12.28 Configuring Central Storage of User Specific Data on page 50).

If the TNS key data is stored in the PBX or on a FTP server, a user's shortcut key configuration is available to any phone within the system to which the user logs on. To enable storing of TNS key data in the PBX, the **EnablePBXStoring** parameter must be set in the configuration file. For information on how to configure phones for storing TNS keys in the PBX, see *Configuration File for DBC 44X and DBC 43X*.

For information on how to assign phone numbers to shortcut keys, see the *User Guide for each telephone model.*

Some PBX platforms (e.g. MX-ONE Service Node) support that the label of the TNS key can be set from the PBX.

12.22.6 ASSIGNING MONITORED EXTENSIONS TO SHORTCUT KEYS (MNS KEYS)

The shortcut keys can be configured as monitoring keys (that is, assigned to monitored extensions). Using monitoring keys, the LED of the shortcut key is used for indicating the status of the monitored extension. By pressing the shortcut keys, calls to monitored extensions can be answered. Monitoring keys can be used for, for example, boss-secretary functions.

Monitoring keys are configured from the PBX, except the time interval from when a call is received on the monitored extension until it is indicated on the monitoring key, and MNS ring signal level when the phone is busy, are configured using the configuration file, see *Configuration File for DBC 44X and DBC 43X*.

Some PBX platforms (e.g. MX-ONE Service Node) support that the label of the key can be set from the PBX.

12.23 CONFIGURING AUTOMATIC ANSWER

With this feature the call is answered automatically in handset, handsfree or headset mode.

This feature is set by the system administrator. The following options are available:

- With delay, which means that one ring signal is heard before the call is answered
- No delay, the call is answered immediately

To set the auto answer feature:

1. Enter administrator mode, see 11 Entering Administrator Mode on page 24.
2. Press 🔧 .
3. Using the navigation keys ▲▼, select **Administrator**.
4. Select **Auto Answer**
5. Select the wanted parameter value.

DBC 446

1. Enter administrator mode, see 11 Entering Administrator Mode on page 24.
2. Press ☰ .
3. Select **Administrator Settings**.
4. Select **Auto Answer**
5. Select the wanted user type.

12.24 CONFIGURING PRESENCE SERVICES

The phone has menu support for activation and deactivation of:

- Absence reason (message diversion)

When the user selects an presence service the phone sends the procedure (*n#) to the PBX.

The presence services are defined in the configuration file, see *Configuration File for DBC 43X and DBC 44X*. If a presence service is not defined in the configuration file, the corresponding selection is unavailable in the phone menu.

The absence reasons must be synchronized with the absence reasons defined in the PBX and in CMG (if used).

When the user sets the absence reason, the telephone proposes a default return time. It is possible to change the default time with a parameter in the configuration file. It can be necessary to adapt this time to the default return time in the interception service system.

12.25 USING MULTIPLE CONFIGURATION FILES

A certain group of IP phones can often have different characteristics compared to the other groups of extensions concerning which codec to use, domain names, emergency number data etc. The following methods exist to get different configuration files for the groups of phones:

- Using the DNS (Domain Name Service) domain name received from DHCP.
- Using the telephony domain name received in the vendor specific field in the DHCP messages.
- Using the subnet method.
- Setting the IP address of the software server manually from the phone. In this case there must be one software server per configuration file.

For all the methods, the corresponding directory names have to be created in the software server and the corresponding configuration files have to be stored under these directories.

12.25.1 DNS DOMAIN NAME

The DNS domain name provided in option 15 in DHCP, is used to create the URI (universal resource identifier) to fetch the configuration file from the software server. Example: /dns_domain_name/d43x01-config.txt.

12.25.2 TELEPHONY DOMAIN NAME

If the DNS domain name cannot be used, it is possible to create telephony domain names and these are sent as a tag in option 43 in DHCP. If the IP phone finds this tag, it will create the URI containing this domain name and fetch the configuration file from the software server. Example: /telephony_domain_name/dbc43x01/config.txt.

12.25.3 SUBNET METHOD

The URI consists of the network address together with the subnet mask length. The network address consists of the phone's IP address with a logical AND operation of the subnet mask.

Example: The phone has the IP address 130.100.26.144 and the subnet mask is 255.255.255.192. The AND operation gives the URI /130.100.26.128-26/dbc43x01/config.txt. The component -26 is the length of the subnet mask (number of ones in the binary value of the subnet mask).

12.25.4 PRIORITY BETWEEN THE DIFFERENT METHODS

The following priority is valid when the phone uses a domain name to fetch the configuration file:

- The telephony domain tag in option 43.
- The DNS domain in option 15.
- Subnet method.
- The default configuration file is fetched. This file is stored under /dbc43X01/d43X01-config.txt for DBC 43X and under /dbc44X01/d44X01-config.txt for DBC 44x.

12.26 USING DNS SRV RESOURCE RECORDS

To get necessary IP addresses into the phone, one option is to use the DNS (Domain Name Server) SRV (service) resource records. The following data can be retrieved in this way:

- The IP address to the software server. To get this option, set the data in following way: In **Network** settings, chose **Automatic SW server = YES** but do not initiate this data in option 43 in DHCP. In this case the phone will get the SW server IP address from DNS SRV.
- The IP address to the IP Phone Administrator server.

The DNS SRV handling does only work when DHCP is used and when the DHCP server points out the DNS server. This service is described in the RFC 2782.

With this method the phone sends a request to the DNS server to get a particular service.

In the answer from the DNS server the phone can get a list with hosts.

12.26.1 ENTERING DATA IN DNS SRV RESOURCE RECORDS

The IP address to the software server

In the DNS SRV resource records, the following data has to be set to find the IP address to the SW-server:

Service

_aasdbc_cfg._tcp

_aas544x_cfg._tcp (For DBC 446 up to and including application R2J)

Protocol

_tcp

Prio

The priority of the target host. The phone will try to contact the target host with the lowest-numbered priority. Target hosts with the same priority should be tried in pseudo random order. The range is 0-65535.

Weight

A load balancing mechanism. When selecting a target host among those that have the same priority, the chance of trying this one first is proportional to its weight. The range is 1-65535. Domain administrators shall use Weight = 0 when there is not any load balancing to do.

Port
80 (fixed value)

Host
The DNS name of the Software server

The IP Address to the IP Phone Administrator Server

In the DNS SRV resource records, the following data has to be set to find the IP address to the IP Phone Administrator server:

Service
_aasdbc_smgt._tcp

_aas544x_smgt._tcp (For DBC 446 up to and including application R2J)

Protocol
_tcp

Prio
The priority of the target host. The phone will try to contact the target host with the lowest-numbered priority. Target hosts with the same priority should be tried in pseudo random order. The range is 0-65535.

Weight
A load balancing mechanism. When selecting a target host among those that have the same priority, the chance of trying this one first is proportional to its weight. The range is 1-65535. Domain administrators shall use Weight = 0 when there is not any load balancing to do.

Port
8080

Host
The DNS name of the IP Phone Administrator server

12.26.2 VERIFICATION OF ENTERED DATA

The data entered into a DNS SRV resource record can be verified in a PC by:

- Open a DOS prompt window
- Enter the command **nslookup.** The response will show the current DNS server
- Enter **set type=srv**
- Enter the wanted service. Example: **_aasdbc_cfg._tcp.** domain name where the domain name is the one the phone receives from DHCP.
- The response will contain the DNS SRV resource record data, including the host name to the requested service

12.27 USING THE PHONE AS AN OPERATOR MEDIA DEVICE (OMD)

The phone can be used in a PBX operator solution based on IP. In this solution, an Operator Work Station (OWS) in a PC is used for the call handling and the phone (OMD) is used for the speech. OMD can only be used with MX-ONE Service Node. The interface between the OMD and the gatekeeper is not based on H.323, it uses a proprietary signaling. Depending on that the gatekeeper is not using H.323, it is called the telephony server.

The IP address and port number to the telephony server are defined in the configuration file, see the description for *Configuration File for DBC 44X and DBC 43X*.

To register the OMD to the telephony server, the directory number and password must be entered from the phone. The directory number and password must first be defined in the telephony server.

The phone can play call progress tones but these are generated in the PBX.

The ring signal has two options:

- The PBX sends low ring signal level. The phone generates a low ring signal where the volume cannot be changed.
- The PBX sends high ring signal level: The PBX operator can change the volume of the ring signal with the volume keys.

Follow the steps below to configure the phone as an OMD:

1. Enter the network settings menu, see 12.2 Setting Network Parameters on page 26.
2. Select **OMD** and select **Yes**.

It is also possible to set this data from the administrator web interface.

12.28 CONFIGURING CENTRAL STORAGE OF USER SPECIFIC DATA

To enable users to access their user specific data from different phones, this data can be stored on an FTP server, instead of in the phone. Secure FTP (SFTP) can also be used, see section12.28.4 Secure FTP (SFTP) on page 53.

Central storage of user specific data is enabled using the configuration file. The following user specific data can be stored:

- Contacts
- Call list
- Shortcut keys
- My mobile phone number
- My voice mail phone number
- Number to fetch message waiting
- Free on busy status
- Ring signal settings; ring type and ring volume
- Alerting setting (different ring signals for first call and if busy)
- Language
- Handset and handsfree level
- Melody list
- Time and date format
- Missed call status

The FTP server can be located on the same server as the software server or on another server that is specified in the configuration file for the telephone.

At registration, the file with user specific data is downloaded to the phone and the user data in the phone is replaced by the corresponding data in the file. If this data is changed from the phone or using the phone's web interface, the corresponding data on the FTP server is updated when exit from changing data in settings, call list, contacts or messages. It is also updated when the phone is logged off.

Central storage of user specific data is mandatory when using the My Dialog Contacts feature.

User specific data is stored as **.xml** files. There is one **.xml** file per extension, with a file name based on the extension number. Example:

- 67609.xml

In a site with DBC 42x phones in combination with DBC 43x and DBC44x phones, a text file (example 67609.txt) can also be stored on the FTP server for compatibility reasons. This file contains only Contacts data. The use of **.txt** files is enabled in the configuration file.

The **.xml** file support in DBC 446 was introduced in the application R3A. In applications earlier than R3A the DBC 446 phone created a **.txt** file to store the contacts. At upgrading from an application earlier than R3A, set the parameter **CompatibleWithD4=YES** in the configuration file to get the contacts from the old to the upgraded system.

My Dialog 4000 Contacts can only use the text file, which means that the parameter **CompatibleWithD4** must be set to **YES**. See 23 Installing the My Dialog Contacts Application on a Web Server on page 86.

A user identity (user account) has to be created on the FTP server. This user identity and the password are defined in the configuration file for the phone. The default user identity is *Telephone* and the default password is also *Telephone*.

Note: Make sure that the user identity has access rights to read and write the Phone Contacts files on the FTP server.

12.28.1 WINDOWS® IIS

Follow the steps below to create a user on the FTP server:

1. In Windows® IIS, right-click **My Computer**, select **Manage** and **Computer Management**.
2. Expand **Local Users and Groups**.
3. Right-click **Users** and add a new user. Enter the same user identity and password as defined in the phone configuration file.
4. Disable **User must change password at next log on** and enable **Password never expires**.
5. Click **Create** and then close.

Follow the steps below to create directories on the FTP server:

1. Expand **Services and Applications**.
2. Expand **Internet Information Services**.
3. Create a directory where to store the files for user specific data. This directory must be the home directory for the user created above.
4. Select **Default FTP site**.
5. Right-click and select **New**.
6. Select **Virtual Directory**. Name the virtual directory according to the to physical directory created above. Enable read and write as access permission.

12.28.2 FASTREAM (FOR WINDOWS)

Fastream NETFile FTP/Web server can be downloaded from www.fastream.com. When Faststream is used, the web server part in Fastream NETFile must be switched off.

Follow the steps below to configure the FTP server:

- The account and the password must be created. Use the same values as defined in the configuration file for the phone.
- Select the **Path** tab and create or add a home directory for the account. Select the option **Home Folder**.
- For this home directory, select **File Rights** options **Download**, **Upload** and **Delete**, select **Folder Rights** option **Change**.
- Under the tab **Cache**, disable both **Folder Cache** and **File cache**.

12.28.3 LINUX

The recommended FTP servers to use on Linux are **pure-ftpd** or **vsftpd**, which are usually bundled with the used Linux installation distribution. If not they can be downloaded from the following web sites: www.pureftpd.org, www.vsftpd.beasts.org

A user account has to be created on the Linux machine where the FTP server will be hosted. The account must be according to the user ID and password defined in the configuration file for the phone (the default user identity is *Telephone* with password *Telephone*).

To perform the operations described below, root access is needed.

To create the user account and password it is possible to use any of the GUI tools included in most of the Linux distributions. It is also possible to use the **useradd** and **passwd** commands. Example with the default account and password *Telephone*:

ftp-server: # useradd -g users -m -s /bin/false Telephone ftp-server: # passwd Telephone

Note: The parameter -s /bin/false prevents anyone from using the account to log on to the FTP server using Telnet or SSH (Secure Shell).

To install the FTP server it is possible to use the GUI tools or to use commands. Depending on that the different GUI tools require different actions, they will not be described here. Please refer to the documentation for the used Linux distribution.

There are two ways that the FTP server can be used either as a stand alone server or as a part of a super server. To keep this section brief there is only a description of how to set up the FTP server as a part of the **xinetd** super server.

12.28.3.1 *Pure-ftpd*

This FTP server is set up by use the command line option. Open the file /etc/xinetd.conf in an editor and add the following:

service ftp {socket_type = stream protocol = tcp wait = no user = root server = /usr/sbin/pure-ftpd server-args = -A -E -H -i -u 500 -c 1000}

The explanation of the arguments can be found in the documentation for the FTP server.

As an alternative this can be set in the file /etc/xinetd.d/pure-ftpd instead.

Restart the super server with the command:

ftp-server: # killall -USR2 xinetd

12.28.3.2 *vsftpd*

This FTP server is set up by using a configuration file. The options listed below are a subset of all available options.

Open the file /etc/vsftpd.conf and edit the following options:

write_enable=YES ls_recurse_enable=YES local_enable=YES chroot_local_user=YES anonymous_enable=NO connect_from_port_20=YES pam_service_name=vsftpd

All the remaining settings can be disabled by creating a comment (# character).

Then open the file /etc/xinetd.conf in an editor and add:

service ftp {socket_type = stream protocol = tcp wait = no user = root server = /usr/sbin/vsftpd log_on_failure += USERID}

As an alternative this can be put in the file /etc/xinetd.d/vsftpd instead.

Restart the super server with the command:

ftp-server: # killall -USR2 xinetd

12.28.4 SECURE FTP (SFTP)

The user name and password to log on to the SFTP (or FTP) server is set in the configuration file of the telephone. The default user name is Telephone.

In a SFTP server running on Linux the following must be considered:

The **.xml** files with user specific data and the **.txt** files with contacts are stored under the folder: **/home/Telephone**, when using the default user name. These folders must be enabled for read and write access.

In the Linux environment the following parameters have to be set in the file: /etc/ssh/sshd_config

PasswordAuthentication yes
AllowUsers Telephone

If the user name and password to the SFTP server shall be something else than default, the configuration file of the phone and /etc/ssh/sshd_config must be updated.

12.29 CONFIGURING THE DIFFSERV PARAMETER

Diffserv is a model for handling of priority, based on the type of service (TOS) field in the IP packet heading. For information on how to configure Diffserv, see *Configuration File for DBC 44X and DBC 43X*.

12.30 DOMAIN NAME

The domain name is used in the following contexts:

- In the function automatic gatekeeper discovery, to find a PBX to register to.
- In the registration request message when using MX-ONE as gatekeeper.
- When several configuration files are used, see 12.25 Using Multiple Configuration Files on page 47. The domain name defined in the parameter **Domain** in the configuration file cannot be used.

The priority between the domain names when they are used in gatekeeper discovery:

1. Domain name received in DHCP option 43.
2. Domain name received as DNS domain name in DHCP option 15.
3. Domain name from the configuration file. This domain name is only working if no domain name is received from DHCP, neither option 15 nor option 43.

12.31 HLR REDUNDANCY

HLR redundancy is a function in the MX-ONE system. If the server, where the data for the extension (Home Location Register) is stored, becomes unreachable, a temporary HLR will be created in another server and the IP extension can register towards this server.

12.31.1 HLR REDUNDANCY IN H.323 MODE

12.31.1.1 Prerequisites

The HLR redundancy feature will only work when:

- The gatekeeper address is **not** set manually
- Backup gatekeeper is **not** used (in branch office scenarios)

In the configuration file of the phone, both primary and secondary gatekeeper (GK) address must be defined.

12.31.1.2 *Change-over to Temporary HLR*

The phone will use the primary GK address towards the entry GK in MX-ONE, and receive a list of the GKs to be used. Alternatively the entry GK could accept the registration directly. If a list is received, the phone will try to register according to the list.

When the server with the ordinary HLR becomes inaccessible, there are two different cases:

- The phone was registered in the server of the ordinary HLR. The terminal will not receive any reply to the keep-alive check and will then try re-registration to the secondary GK, according to the configuration file. A temporary HLR will be created in the server where the registration can be accepted.
- The phone was registered in another server than in the ordinary HLR server. This will happen if load distribution was used when trying to register to the primary GK. A temporary HLR will be created in that other server (where the phone was registered).

12.31.1.3 *Change-back to Ordinary HLR*

If the server of the ordinary HLR becomes available again, the periodic keep-alive check request will be rejected by the GK (in the server of the temporary HLR). The terminal will request a registration to the primary GK, that is, in the server of the ordinary HLR.

The phone will then re-register according to the configuration file, that is, to primary and secondary GK, in that order.

12.32 SELECTION OF TRANSPORT ADDRESSES (PORT NUMBERS)

The tables shows the port numbers used for signaling and media in the phone. It is the receiving port numbers in the phone that are shown.

Table 1 UDP ports used by the phone

Type of signaling	Minimum	Maximum	Comment
DHCP client	68	68	
SNMP	161	161	
RAS/GRQ	1718	1718	Multicast
RAS	1719	1719	
WAP (Push)	2948	2948	Receive from internal WAP server (PBX)
URQ in secure mode	3727	3727	
OMD	5000	5001	For speech
VoIP Recording	7300	7300	
RTP	16986	17012	
RTCP	16987	17013	RTP port + 1

Type of signaling	Minimum	Maximum	Comment
WAP (Reply)	49152	49152	Receive from internal WAP server (PBX)
WAP (Reply)	49153	49153	Receive from external WAP server

Table 2 TCP ports used by the phone

Type of signaling	Minimum	Maximum	Comment
SSH	22	23	Secure Shell
Web Server Port	80	80	Web server in the phone
H.225 secure port	1300	1300	Incoming call to the phone, default value. Can be 1722 if the phone receives this value in RCF.
H.245	1390	1396	
H.225	1720	1720	Incoming call to the phone
H.225 unsecure port	1722	1722	Incoming call to the phone is 1722 if the phone receives this value in RCF. The default number is 1300.
RAS over TCP	3727	3727	TLS signaling.
Web Browser Port	8080	8080	When using the WAP browser in the phone to access external web pages

Port number for Operator Media Device (OMD): the port number is set in MX-ONE (OPSAI command). The same port number shall be set in the configuration file for the telephone and in the configuration of the Integrated Attendant Workstation, NOW (if applicable).

12.33 CONFIGURING A BACKUP GATEKEEPER FOR BRANCH OFFICES

In a branch office scenario where the IP phones in the branch office are connected to the PBX in the main office, it must be possible to make calls even if the connection to the main office is lost. The solution for this is to use a backup gatekeeper locally in the branch office. When the connection to the main office is lost the IP phones in the branch office automatically register to the backup gatekeeper. When the connection to the main office works again, the IP phones un-register from the backup gatekeeper and register to the PBX in the main office.

It is possible to have encryption of the calls also when the phone registers to the backup gatekeeper.

The procedure to get this working in the IP phones is:

- Define in the configuration file, used by the phones in the branch office, the type and the IP address of the backup gatekeeper, see *Configuration File for DBC 44X and DBC 43X*.
- The frequency of the keep alive check from the phone towards the gatekeeper must be considered. The recommended value is one minute, which means that

maximum one minute and 9 seconds (the check is performed 3 times with 3 seconds pause) after the connection to the main office is lost, the phones in the branch office will try to register towards the backup gatekeeper. The drawback of setting the time too short is that the network will be loaded with such messages. See parameter **RRQTtl** in *Configuration File for DBC 44X and DBC 43X*.

- The frequency of the routine for discovering when the main office connection is working again is also defined by the parameter **RRQTtl**, see *Configuration File for DBC 44X and DBC 43X*. When the main office connection is working, the phone will be registered to the main office gatekeeper.

12.34 POLYPHONIC RING SIGNALS (MELODIES)

It is possible to have melodies instead of the ordinary ring signals from the tone ringer. The melody files must be stored by the system administrator on the software server, under the directory **ringtones**, see 7.2 Creating a Directory Structure on page 11.

12.34.1 FILE FORMAT

The only supported file format is: *8-bits G.711 μ-law mono raw at 8 kHz*. The bit rate is 64 kbit/s and the file size is 80 kilobytes per 10 seconds melody. The file extension type is **.pcm**.

To get the right file format a polyphonic tone ringer converter is needed. There are a number of options:

- Adobe Audition
- Absolute Audio Converter
- Arial Audio Converter
- Etc.

There are some limitations for the melody files on the sw server:

- Max 100 melody files on the software server
- Max 160 kilobytes (20 seconds) per melody file
- Rules for the file name:
  - < 25 characters including the extension **.pcm**
  - letters in the English alphabet, underscore, hyphen
  - digits 0-9
  - must not contain any space

12.34.2 FUNCTION

The assignment of melodies is only shown in the menus in the phone when the header for the default melodies is enabled in the configuration file.

It is possible to assign 10 melodies in the phone in addition to the 10 ring signals from the tone ringer.

The assignment of melodies to the melody positions can either be done by the end-user or by the system administrator as default melodies in the configuration file.

The names and size of the files of the melodies assigned as default melodies or by the end-user, are copied to the user specific data file (.xml file).

12.34.2.1 System administrator

When the system administrator defines a default melody list in the configuration file, see *Configuration File for DBC 44X and DBC 43X*.

The system administrator can choose how many melodies, maximum 10, that shall be defined as the default list. The rest of the positions in the list can be used by the end-user to assign individual melodies from the software server.

A sequence number in the configuration file shall be increased every time the system administrator wants to force the phones to load the updated list with default melodies.

The downloading of new melodies takes place when the phone registers to the PBX, if a new configuration file has been loaded and the sequence number is increased. The melody names that are not changed will be kept in the phone.

If an end-user has defined a melody in a position that is defined in the configuration file, it will be overwritten when the configuration file is loaded into the phone and if the MelodyListIndex is increased compared to the previous time

12.34.2.2 End user

The phone user can browse and listen to the melodies stored on the software server by pressing: **Settings - Sounds - Ring Signals - Default Ring Signal - Melody n - Add**.

If the user listen to one melody, the file is downloaded from the software server to the phone and if the user selects one of the melodies, the melody will be stored in the flash memory in the phone. When exit **Settings** the melody name and size of the file is copied to the user specific data file (.xml file).

For more information how to use the menus in the phone to handle the melodies, see the user guide for each telephone model.

12.35 CORPORATE DIRECTORY

From the phone it is possible to search in the CMG directory or in the D.N.A directory. It is also possible to search in a directory outside CMG by using a subset of the XML interface for the Mitel SIP Phones.

To be able to access the corporate directory from the phone, some parameters in the configuration file of the phone have to be set, see *Configuration File for DBC 44X and DBC 43X*.

The phone sends a http request with the search criteria to the directory server and receives a list with the search result. The answer can be in XML format.

The user can select the phone number in the search result and initiate a call towards the gatekeeper.

There are two XML options for all the models:

- XML interface made for DBC43x and DBC44x in CMG.
- a subset of the XML interface for Mitel SIP Phones.

The support of the corporate directory has been introduced in the way described below.

For DBC 43x phones

- uses the XML interface from application R2A.
- no corporate directory support in applications earlier than R2A

For DBC 444 phones:

- uses the XML interface from application R1A.

For DBC 446 phones:

- uses the XML interface from application R3A.
- in applications earlier than R3A, the built in web browser was used to access the directory. It is still possible to use the option by enabling a parameter in the configuration file but shall only be used for backward compatibility reasons.

12.35.1 ACCESS THE CORPORATE DIRECTORY

There are two ways to access the corporate directory in DBC 444:

- Press 👤 and then 🏢
- Softkey number three to access the corporate directory directly from the idle menu

To access corporate directory in DBC43x and DBC 446: Select **Contact** and then **Corporate Directory.**

The corporate directory access is only visible if the URL to the corporate directory server is enabled in the configuration file of the phone.

12.35.2 CMG DIRECTORY

See *Corporate Directory for IP Phone - Installation and Configuration Guide* in the CMG documentation.

12.35.3 OTHER CORPORATE DIRECTORY SERVERS

When a directory server outside CMG shall be used, the telephone can use the same XML interface as the Mitel SIP phones are using. This interface is described in the Development Guide XML API for Mitel SIP phones.

The DBC43x and DBC 44x telephones support only a limited part of the interface and below is a description of what is supported.

The TextMenu, InputScreen and TextScreen objects are supported.

The table below describes the document objects that are supported in the DBC 43x and DBC44x phones.

Table 3 Supported document objects

TextMenu	InputScreen	TextScreen
Title	SoftKey	Title
SoftKey	URL	Softkey
defaultIndex	Parameter	Text
MenuItem	Promt	
promt	Default	

TextMenu	InputScreen	TextScreen
URI	type= string / number	
Dial		

12.36 TELEPHONE WEB BROWSER

DBC 446 has a built in web browser that can access Internet web pages.

To be able to access web pages some parameters in the configuration file of the phone have to be set, see *Configuration File for DBC 44X and DBC 43X*.

The web browser supports WML, HTML, XHTML basic and XHTML mobile profile. It has some limitations in the support of Flash graphics.

12.37 POWER SAVING

The telephones have the following options for power saving:

- Switch off the terminals at certain times via the configuration file. Only DBC 43401 and DBC44401. The user has to switch on the telephone before using it again.

  If the extension number has an associated PIN code, the user has to enter his PIN code. If the extension does not have a PIN code, the phone registers automatically.

- Switch off the backlight at a certain time. Only DBC 44401 and DBC44601. These are the only phones with slight backlight on, all the time.

For information how to set the parameters, see description of *Configuration File for DBC 44X and DBC 43X*.

Upgrading of the firmware in the telephones that are switched off, will take place when the end-user switches on the power to the phone.

12.38 CALL PARK POOL

For a detailed description of the Call Park Pool feature in an MX-ONE environment, see operational directions for Call Park Pool.

No configuration in the phone is needed for this feature.

12.39 INTERCOM

Intercom means that a shortcut key is defined as an MNS key and when there is an incoming call to this number, the phone will answer this call automatically but with the microphone muted. The user has to press the mute key to connect the microphone.

If the telephone is busy with an ongoing call when a call to the intercom key is received, the user must park the ongoing call and manually answer the intercom call by pressing Intercom (MNS) key.

It is only possible to have intercom between two telephones, it is not possible to have one A-party and several B-parties.

12.39.1 CONFIGURATION

The Intercom key on the phone is initiated as an MNS key in the PBX. The MNS number can be a virtual extension, application link DTS or an analogue extension without a telephone, see below.

To avoid that somebody else than the Intercom extensions, by mistake, dials the MNS number, this number shall not be possible to dial from other users. This can be implemented with the traffic matrix.

To program the intercom feature in the telephone:

Settings > **Shortcuts** > Select the wanted MNS key > **more...** > **Auto answer** and enter admin mode to set auto answer.

In the **more...** menu, the type of alert (ring) signal can also be set.

To check if the MNS key is of type intercom:

Settings > **Shortcuts** > Select the wanted MNS key > **more...** > **Auto answer**, if auto answer is enabled, the key is used for intercom.

It is also possible to program the intercom feature via the web interface.

Note: Automatic answer on a MNS key shall only be used for Intercom but never for ordinary monitoring.

12.39.2 USING A VIRTUAL EXTENSION

For MX-ONE Service Node, see operation directions for Intercom.

12.39.3 USING AN APPLICATION LINK DTS

A digital extension board must exists, but no telephone is needed.

12.39.4 USING AN ANALOGUE EXTENSION

An analogue extension board must exists, but no telephone is needed.

12.40 MESSAGES

The message menu is accessed by pressing the ✉ key. There are two options:

- **My VoiceMail**
- **My Messages**, for example messages from the PBX operator or manual message waiting.

It is possible to disable, with a parameter in the configuration file, the option **My Messages.** In this case the voice mail is reached directly. A default Voice Mail Box Number can be defined via configured file (Only in DBC 43x and in DBC 444).

12.41 MISSED CALL

One of the options in the call list is Missed calls. In the case when a user has several telephones using a feature like parallel ringing or multiple terminals service, a call is marked as a missed call although the call is answered on another telephone.

It is possible to set a timer, meaning the time in seconds in ringing state before an incoming call is regarded as a missed call. The timer is set in the configuration file.

It is also possible to disable the missed call feature via the telephone user interface: **Call List** > **more...** > **Do Not Log Missed Call**.

12.42 DOOR PHONE (ONLY DBC 444)

This phone model can be used as a door phone, which means:

- The second page with shortcuts is shown in idle mode. It is not possible to navigate to alternative display pages. The advantage to show page two is that bigger labels are shown in the display compared to the ordinary idle page.

  Note: Follow-me should be disabled in the PBX for this extension otherwise it is possible to activate follow-me without showing any warning text in the display.
- All five individual menu keys (Settings, Contacts, Shortcuts, Call List and Messages) are disabled.
- The user cannot change any data.
- Restart key is disabled.

The extension number for the door phone shall have an associated PIN code to avoid that anybody else log in with the same number.

The door phone functionality is enabled in the following way: enter administrator mode, press 🔧 and scroll down to Door Phone.

When the phone is in door phone mode, the administrator mode must be entered before it is possible to access settings 🔧 .

12.43 CORPORATE LOGON (ONLY DBC 444)

This phone model can use the Corporate Logon function, which makes it possible to log on to a home exchange from a networked system. E.g.even if you are temporary visiting your office in Paris you should be able to logon to your normal office in Stockholm.

Log off

Do as follows:

1. Press the **More** key, select **Corporate Logon**, a list of the configured names of the Corporate Servers will be displayed.
2. When a server is selected, the **Corporate Logon** prompt page appears.

Log on

Do as follows:

1. Press the **More** key, select **Log On Temporary User**.
2. Press **More**, select **Corporate Logon**, a list of the configured names of the **Corporate Servers** will be displayed.
3. When a server is selected, the **Corporate Logon** prompt page appears.

The corporate logon function is defined in the configuration file, see Configuration File for DBC 43X and DBC 44X. If it is not defined in the configuration file, the corresponding selection is unavailable in the phone menu.

Note: When the [Security] parameters Security and SignalingEncrypted are enabled, the parameter SecurityFallback should also be enabled (because a Corporate logon server may have a different certificate than the one specified by the RootCert parameter).

13 PASSWORDS AND PIN CODES

The following passwords or PIN codes are used when working with these phones:

- User passwords or PIN codes for registering phones to the gatekeeper (PBX). For information on how to change PIN codes, see the user guide for each telephone model.

  It is recommended to use a password or PIN to avoid that an end-user can log on with another end-user’s directory number.
- Administrator password for accessing the phone using SSH or the phones' web interface.
- Password for LAN access control authentication.
- Password for logging on to the phone using the phone's web interface

13.1 CHANGING THE ADMINISTRATOR PASSWORD

The administrator password is used for logging on to phones using SSH or the phones' web interface. The default password is **Telephone**.

Follow the steps below to change the administrator password:

1. Log on to a phone through SSH using the following data:
   - **Login:** <Administrator used ID> (as defined in the configuration file.)
   - **Password:** <Administrator password> (as defined in the configuration file.)
2. Enter the command **encryptPasswd “<new password>”** (including quotation marks). The password must be at least eight characters. An encrypted password is created.
3. In the [SYSTEM] header in the configuration file, specify the encrypted password generated in the previous step using the **AdminPassword** data identifier.
4. Store the updated configuration file on the software server.
5. To configure the phones with the new password, restart the phones.

13.2 WEB INTERFACE PASSWORDS FOR END USERS

End users can use a Web browser to access the phone's Web interface. This interface can be used when working with contacts, call lists, and other user specific data.

The Web interface is accessed using one of the following methods:

- Using the same password or PIN code as used when registering the phone to the PBX. The password or PIN code must be less than eight characters.
- Using the default password **Welcome**. (Provided that no password or PIN code has been defined and that the usage of the default password is enabled in the configuration file.)

14 ACCESSING THE PHONE FROM A PC

Users can access a phone using the phone's Web interface. Administrators can access the phone using the following alternatives:

- Using the phone's web interface (recommended).
- Using SSH (Secure Shell). This interface can be used by experts.

  In the maintenance PC, a SSH client must be used. There are several freeware clients, such as PuTTY for PCs using Windows®.

  The default encryption keys cannot be changed.

For detailed instructions on how to log on to the phone as an administrator, see *Maintenance Instructions for DBC 43X and DBC44x*.

15 THE IP PHONE ADMINISTRATOR TOOL

The tool *IP Phone Administrator* is used to monitor the IP phones in the network. This is useful in the following cases:

- To find the IP address to the IP phones and especially to the phones without a display.
- To get an overview of all registered and not registered phones.
- To see the hardware and software versions in both registered and not registered IP phones.

An alternative to *IP Phone Administrator* is to use the SNMP client in the telephone, see section 15.2 SNMP agent on page 70.

The *IP Phone Administrator* is used in either of two ways depending on the telephony system.

MX-ONE SN	Use the IP Phone Administrator task, which is part of MX-ONE Service Node Manager. (No separate installation is needed.)

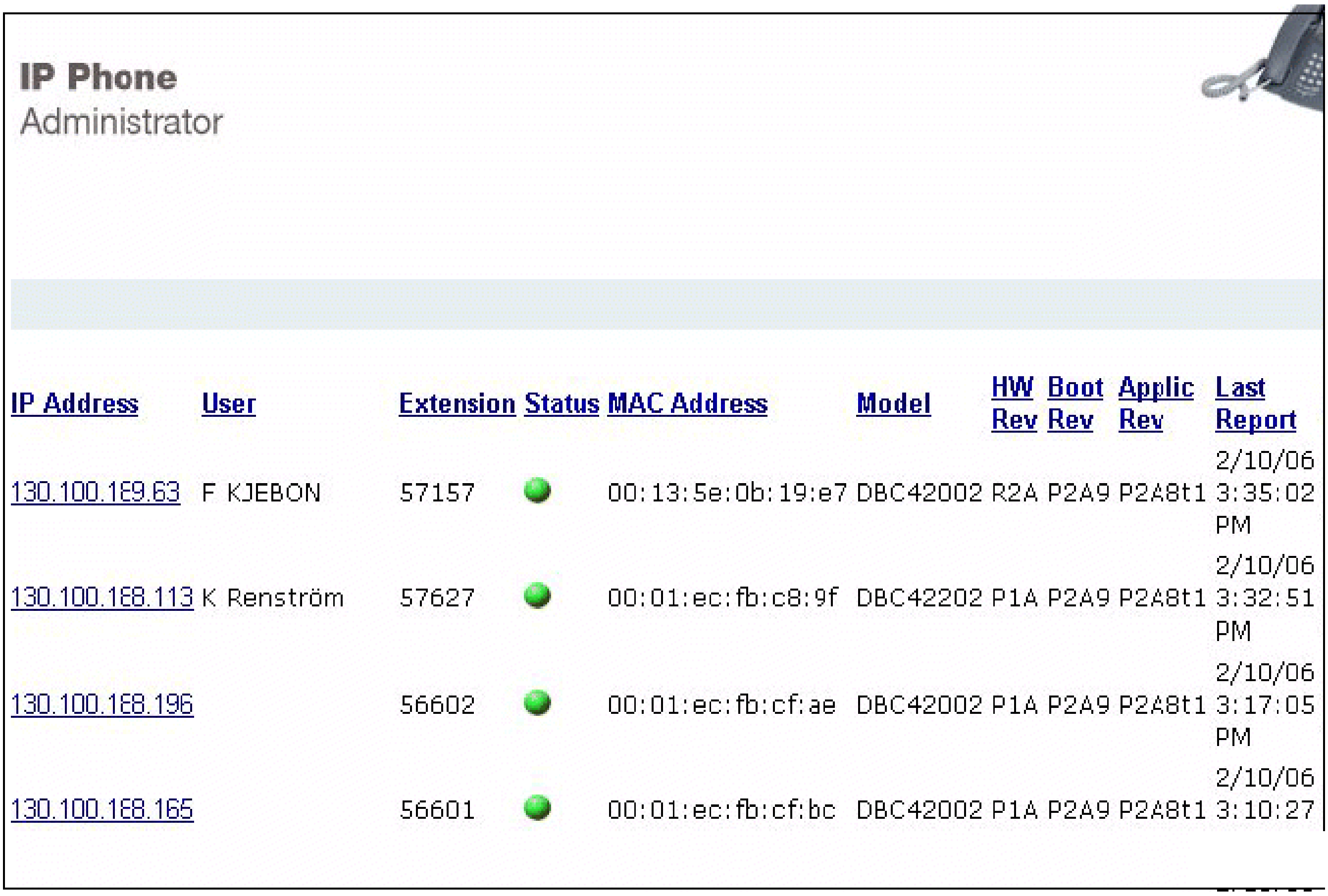
Each phone is sending http messages to the IP Phone Administrator server with data and events. The sent data are e.g. the MAC address, the IP address, the hardware and firmware version and the extension number. The events that can be sent are: the phone has started, the phone is registered or not registered toward the PBX.

The *IP Phone Administrator* tool collects all the http messages from the phones and has a Web GUI to present the data for the system administrator

It is possible to enable and disable the sending of these http messages from the phone with a parameter in the configuration file, see *Configuration File for DBC 44X and DBC 43X*.

The phones gets the IP address to the IP Phone Administrator server by DNS SRV resource records or via the configuration file, see the description for *Configuration File for DBC 44X and DBC 43X*.

User interface of the stand-alone IP Phone Administrator



IP Phone
Administrator

IP Address	User	Extension	Status	MAC Address	Model	HW Rev	Boot Rev	Applic Rev	Last Report
130.100.189.63	F KJEBON	57157	●	00:13:5e:0b:19:e7	DBC42002	R2A	P2A9	P2A8t1	2/10/06 3:35:02 PM
130.100.188.113	K Renström	57627	●	00:01:ec:fb:c8:9f	DBC42202	P1A	P2A9	P2A8t1	2/10/06 3:32:51 PM
130.100.188.196		56602	●	00:01:ec:fb:cf:ae	DBC42002	P1A	P2A9	P2A8t1	2/10/06 3:17:05 PM
130.100.188.165		56601	●	00:01:ec:fb:cf:bc	DBC42002	P1A	P2A9	P2A8t1	2/10/06 3:10:27

Figure 13: IP Phone Administrator

A log in window will pop up when starting the tool. The user name and the password is set by the system administrator at installation of IP Phone Administrator.

The following columns exist in the GUI:

IP Address

Clicking on the IP address means that the web interface in the phone is opened.

User

The name of the user that is registered or was registered before the phone was logged off. This name is normally received in the phone from the PBX, but can also be the name in the Contacts for the actual extension number.

Extension

Extension number for the user that is registered towards the PBX, or that was registered before the phone was logged off.

Status

An icon in different colors is shown:

- Red icon: the phone is not registered towards the PBX.
- Green icon: the phone is registered.
- Grey icon means: no log on attempt towards the PBX has been done
- Yellow icon with an exclamation mark: the phone has tried to register but has got reject back from the gatekeeper.

- Yellow icon: the phone has not reported anything to the IP Phone Administrator since 48 hours.

MAC Address
The MAC address can also be found on the label under the phone.

Model
Type of phone.

HW rev
Hardware revision of the phone.

Boot rev
Revision of the super boot software in the phone.

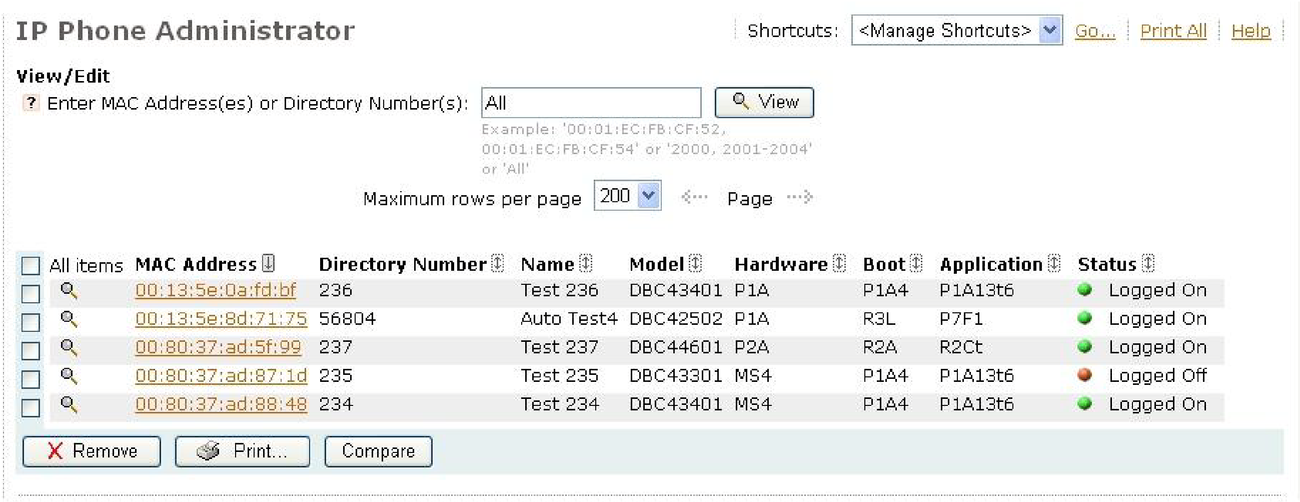
Applic rev
Revision of the application software in the phone.

Last report
The time stamp when the phone sent a http message to the IP Phone Administrator. Even if the status in the phone is not changed, the phone sends an update once every 6:th hours.

Uptime
The time since last restart of the phone. The abbreviation **d** means days.

Remove old entries
Removes entries for phones that has not sent any report during the last 48 hours.

User interface of IP Phone Administrator in MX-ONE Service Node Manager



IP Phone Administrator

Shortcuts: <Manage Shortcuts> | Go... | Print All | Help

View/Edit

? Enter MAC Address(es) or Directory Number(s): All [View]

Example: '00:01:EC:FB:CF:52, 00:01:EC:FB:CF:54' or '2000, 2001-2004' or 'All'

Maximum rows per page 200 Page

□ All items	MAC Address	Directory Number	Name	Model	Hardware	Boot	Application	Status
□	00:13:5e:0a:fd:bf	236	Test 236	DBC43401	P1A	P1A4	P1A13t6	🟢 Logged On
□	00:13:5e:8d:71:75	56804	Auto Test4	DBC42502	P1A	R3L	P7F1	🟢 Logged On
□	00:80:37:ad:5f:99	237	Test 237	DBC44601	P2A	R2A	R2Ct	🟢 Logged On
□	00:80:37:ad:87:1d	235	Test 235	DBC43301	MS4	P1A4	P1A13t6	🔴 Logged Off
□	00:80:37:ad:88:48	234	Test 234	DBC43401	MS4	P1A4	P1A13t6	🟢 Logged On

Figure 14: IP Phone Administrator in MX-ONE Service Node Manager

A log in window will pop up when starting the tool. The user name and the password is set by the system administrator at installation of IP Phone Administrator.

The following columns exist in the GUI:

MAC Address

The MAC address can also be found on the label under the phone.

Directory number

Directory number for the user that is registered towards the PBX, or that was registered before the phone was logged off.

Name

The name of the user that is registered or was registered before the phone was logged off. This name is normally received in the phone from the PBX, but can also be the name in the Contacts for the actual directory number.

Model

Type of phone.

Hardware

Hardware revision of the phone

Boot

Revision of the super boot software in the phone.

Application

Revision of the application software in the phone.

Status

An icon in different colors is shown:

- Red icon: the phone is not registered towards the PBX.
- Green icon: the phone is registered.
- Grey icon means: no log on attempt towards the PBX has been done
- Yellow icon with an exclamation mark: the phone has tried to register but has got reject back from the gatekeeper.
- Yellow icon: the phone has not reported anything to the IP Phone Administrator since 48 hours.

15.1 INSTALLING THE IP PHONE ADMINISTRATOR SERVER

The stand alone tool (product number CXC 109 0050) can be downloaded from the Service Support Plaza web site. The files are stored on a Apache Tomcat server. The installation is described in the read me file for the IP Phone Administrator tool.

15.2 SNMP AGENT

There is a built in SNMP (Simple Network Management Protocol) agent in the telephone. When using a port scanning program, the SNMP agent returns the phone model, MAC-address and the hardware and firmware revisions.

The SNMP agent is by default disabled, but can be enabled via the configuration file. In this case it is mandatory to set the *community* string in the configuration file, see description of configuration file for DBC43x and DBC44x.

The MIB (Management Information Base) OID (Object IDentifier) must be 1.3.6.1.2.1.1.1.0.

For a more detailed description of the SNMP agent, see installation instructions for DBC420.

16 BUILT-IN ETHERNET SWITCH

DBC 43X and DBC 44x have a built-in Ethernet switch with two available ports. One port is used to connect the LAN and the other can be used by a PC.

The phone has support for the IEEE standards 802.1D (except spanning tree) and for 802.1p&Q.

The frames sent from and to the phone (voice and signaling) are handled with higher priority within the switch compared to the frames sent from and to the PC.

Note: Concerning spanning tree: The phone's PC port is intended to be connected to a PC but not to another switch. As such, spanning tree protocol (STP) support is not required as the phone/PC will be an end branch of the tree.

Note: To move the PC from the phone PC port to another port in the VLAN can fail in some cases. If the LAN switch is enabled with security meaning that it will not allow the same MAC address access from two different LAN ports, the following can be configured in the LAN switch (in the case of Cisco):

authentication mac-move permit

17 HEADSET

Wireless headsets according to the DHSG protocol as well as headsets with cable can be used with DBC 434 and DBC 444.

The DHSG interface uses a 8 pole connector. When a headset with a 4 pole RJ45 connector shall be used, an adapter is needed to convert from 4 pole to 8 pole RJ45. The product number of the adapter is TSR 217 001.

DBC446 has only support headsets with a 4 pole connector but no DHSG support.

18 KEY PANEL UNITS AND DISPLAY PANEL UNITS

DBC 434 and DBC 444 can be equipped with up to three Key Panel Units (DBY 412 11) or up to two Display Panel Units (DBY 412 21). Each key panel offers 24 additional keys for storing of the user's most frequently used phone numbers and features.

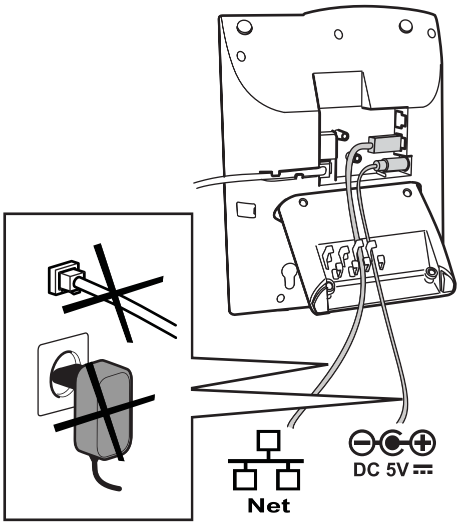
Display Panel Units are self signing, meaning that the name, number or function that is programmed to a certain key will be shown in the display next to the key.

For KPUs, designation cards need to be printed and placed under the plastic designation cover. Design Card Manager (DCM) is used to make and print key panel designation cards. DCM is included on the Enterprise Telephone Toolbox CD. It can also be downloaded from: *http://www.mitel.com*. For more information, please contact your Mitel Enterprise certified sales partner.

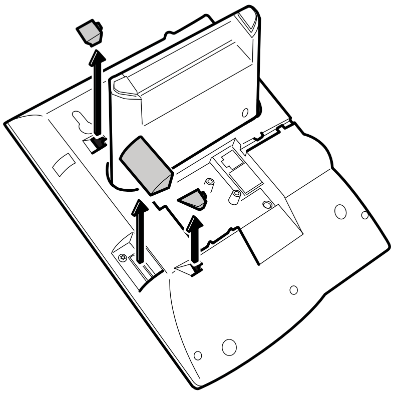
Note: It is not possible to mix KPUs and DPUs on the same phone.

18.1 INSTALLING KEY PANEL UNITS AND DISPLAY PANEL UNITS

1. Disconnect the power from the phone, otherwise the key panel can be damaged.

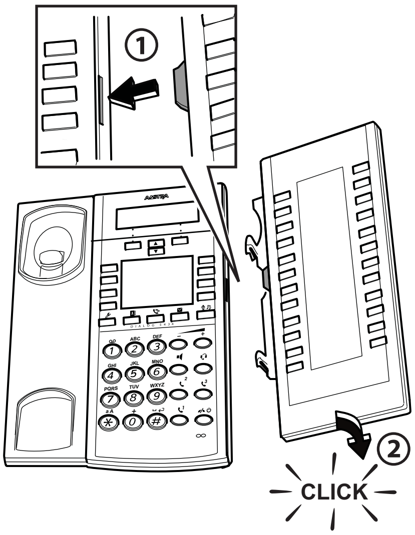


2. Remove the rubber pieces from the back of the phone.

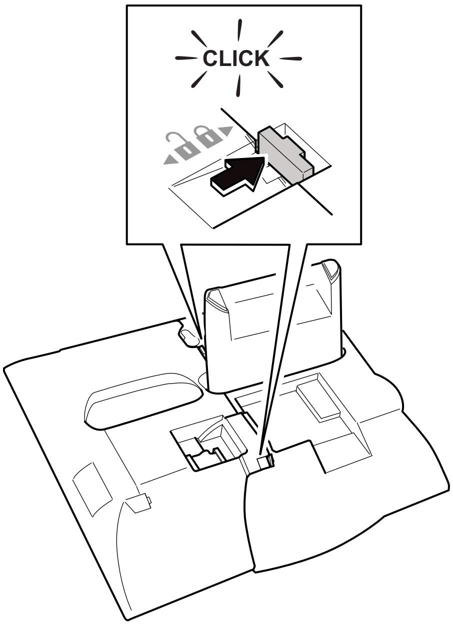


3. Attach the KPU or DPU to the phone as seen in illustration below (1).

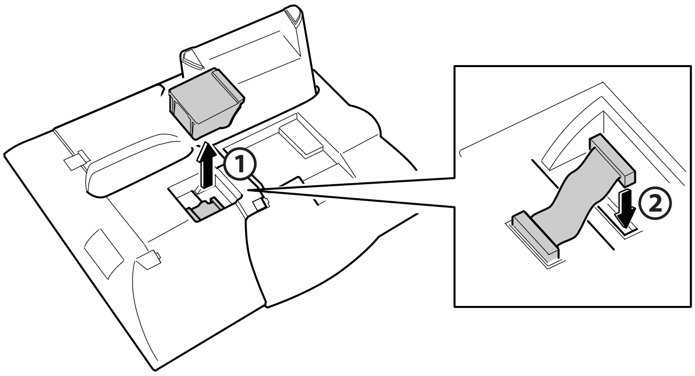
4. Press down the KPU or DPU until you hear a click sound (2).



5. Lock the unit.



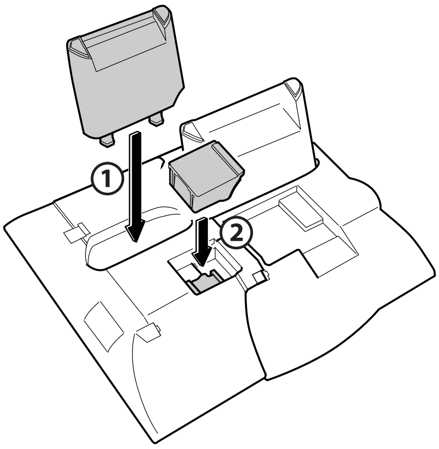
6. Remove the rubber piece from the back of the phone, see illustration below (1).
7. Connect the ribbon cable to the phone. Make sure it fits correctly before pressing it down (2).



8. Connect the foot console on the KPU or DPU (the console is enclosed in the box), see illustration below (1).

   This is done in the same way as connecting the phone's foot console to the phone.

9. Replace the rubber piece, see illustration below (2).



18.1.1 POST INSTALLATION MEASURES AFTER MOUNTING OF PANEL UNITS

After installing key panel units or display panel units, follow the steps below to verify that the panel units work correctly:

1. Connect the power to the phone and connect the phone to the LAN.
2. Program one function key per panel unit.
3. Establish a call using the key on each panel unit.

18.2 REMOVING KEY PANEL UNITS AND DISPLAY PANEL UNITS

To remove a KPU or DPU, follow the steps below:

1. Disconnect the power from the phone.
2. Disconnect the ribbon cable from the phone.
3. Unlock the KPU or DPU.
4. Press the unit in the opposite direction to when you installed it.

19 OPTION UNIT (DBY412 02)

This option unit can be used with DBC433, DBC 434 and DBC 444.

The option unit can provide the following features:

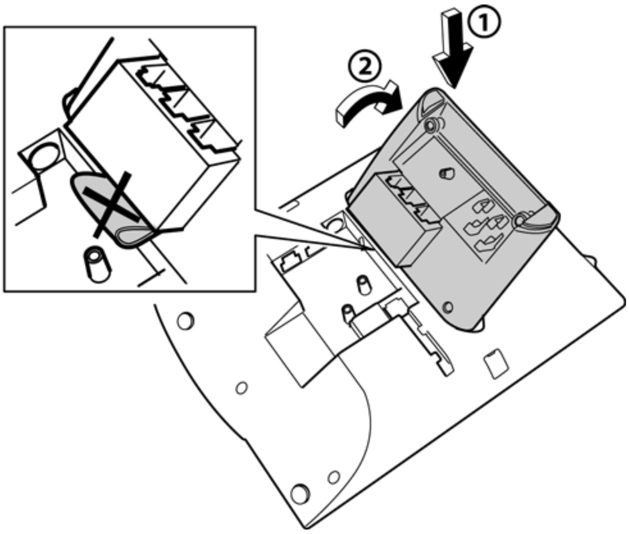
- The Gigabit Ethernet works as an interface to the PC that is connected to the LAN via the phone.
- Extra bell. An extra bell (or lamp) can be activated in parallel with the ring signal.
- Busy signal. The busy signal is activated in off-hook mode.

The option unit is built into the foot console.

19.1 INSTALL THE OPTION UNIT

To install the option unit, do the following:

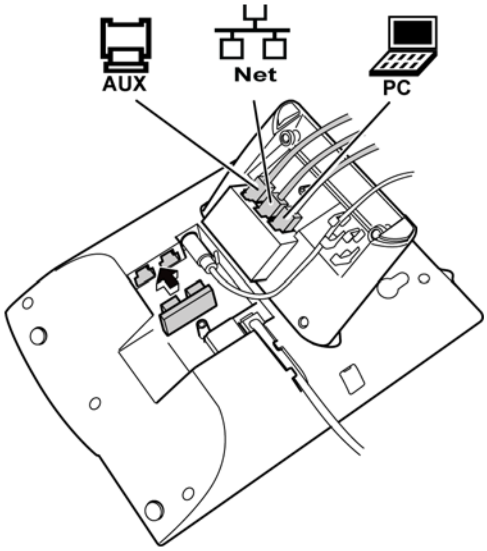
1. Log off the phone and disconnect all cables, including the power, from the phone.
2. Connect the ribbon cable to the phone, making sure the cable does not get stuck.
3. Attach the option unit at the arrows on the back of the phone. Press until you hear a click sound.



Note: Avoid touching the contacts when you connect the ribbon cable.

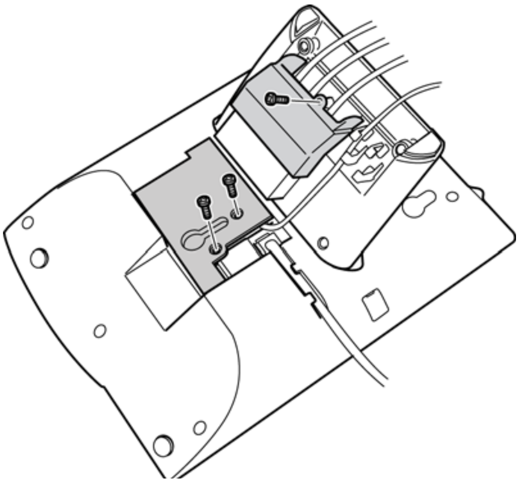
4. Connect the cables to the option unit and attach the rubber piece as showed in the figure below.

   Apart from the pc and LAN cables, you need to connect the auxiliary cable for an extra bell or busy lamp, otherwise the extra bell and busy lamp feature will not work.



Note: Unless the LAN cable is connected to the port marked **Net** on the option unit, the phone will not work.

5. Attach the ESD covers on the back of the phone to protect the connectors from ESD. For this you need a screwdriver.



19.1.1 CHECKING THE OPTION UNIT INSTALLATION

After mounting the option unit, follow the steps below to make sure the option unit was installed correctly.

1. Connect the power to the phone and log on to the gatekeeper.
2. Check that a call can be established.
3. Check that the installed equipment works.

19.1.2 REMOVING AN OPTION UNIT

To remove the option unit, do the following:

1. Log off the phone and disconnect all cables attached to the option unit.

2. Press the unit in the opposite direction to when you installed it.
3. Disconnect the ribbon cable.

19.2 GIGABIT ETHERNET

The option unit contains a gigabit Ethernet interface. The purpose of this unit is to pass on gigabit traffic to the PC that is connected to LAN via the IP phone. The phone itself does not require the gigabit speed.

The switch parameters in the Gigabit Ethernet module, for example VLAN identity, can be changed from the phone.

In the configuration file and in the menus, the same parameters are used for changing the settings in the phone switch as for changing the settings in the Gigabit Ethernet switch. For information about the parameter settings in the configuration file, see the description in the *Configuration File for DBC 44X and DBC 43X*.

To change the switch settings from the menus, do the following:

1. Press🔧 to enter the administrator mode.
2. Select **Administrator**, then **Network**.

For information about the power consumption using the option unit, see 5 Power Equipment on page 9.

19.3 EXTRA BELL AND BUSY SIGNAL

Apart from the Ethernet interface, the option unit also has a port for external functions such as an extra bell and busy signal. It is possible to activate either or both of these two functions, see below.

- **Extra bell.** The extra bell (or lamp) is activated in parallel with the ring signal. It is possible to define via the configuration file if the bell or lamp shall be activated when a call is received on a MNS key.
- **Busy signal**. The busy signal is activated in off-hook mode. The function can be used to control a Do-not-disturb lamp at the door.
- **Combined extra bell and busy signal**. The two functions are activated in parallel with the ring signals and steady active in off-hook mode. This indication can be used for lamp indication in environments such as office landscapes.

Note: A Free on second call does not activate the extra bell function.

When the function is active, the circuit is closed via an opto relay, which is used to separate the external device electrically from the phone. Maximum load on the external device is: 1 A resistive or 0.3 A capacity or 0.3 A inductive load, at maximum 24 V AC or 48 V DC. An external over-voltage protection is recommended.

Cables to external equipment are connected to the pin outlets of the option unit according to the picture below.

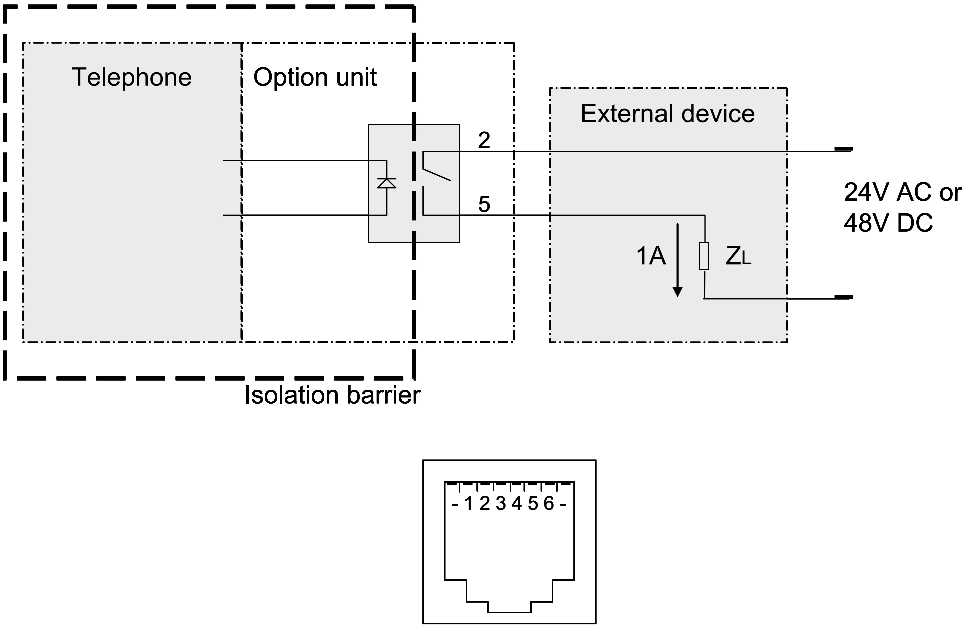


Figure 15: Cable connections for external equipment

20 OPTION UNIT (DBY 412 01)

This option unit can be used with DBC 446.

Follow the steps below to install an option unit:

1. Log off the phone and disconnect all cables, including the power cable, from the phone.
2. Mount the separate pin connector to the option unit. If possible, avoid to touch the contacts.

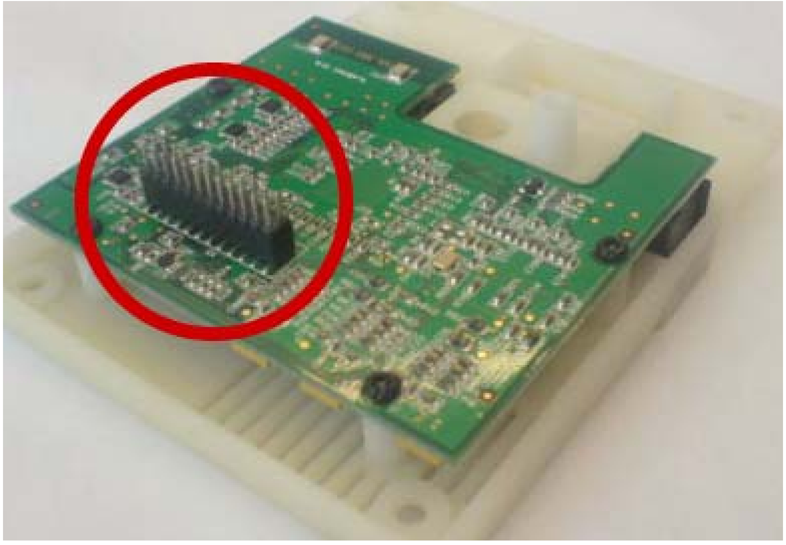


Figure 16: Mounting the pin connector

3. Remove the four screws holding the cover on the bottom side of the phone and remove the cover.
4. Attach the option unit to the phone. Make sure that the pin-connector on the option unit is aligned with the corresponding contact on the phone.

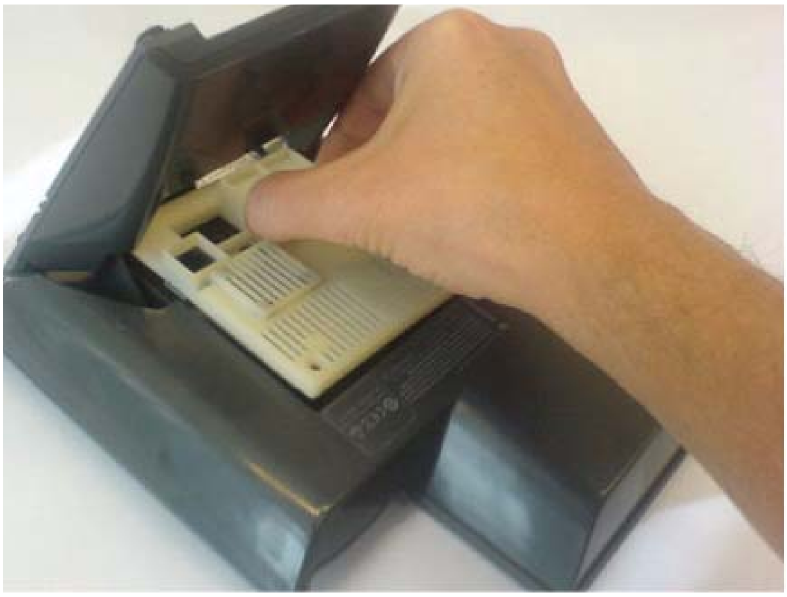


Figure 17: Attaching the option unit

5. Firmly press the option unit to make sure it is properly attached to the phone.

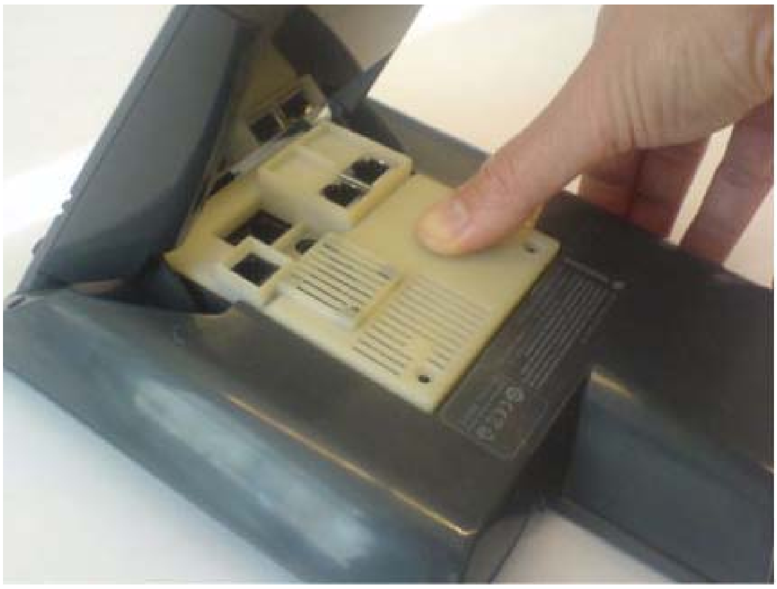


Figure 18: Attaching the option unit

6. Mount the option unit using the four screws.

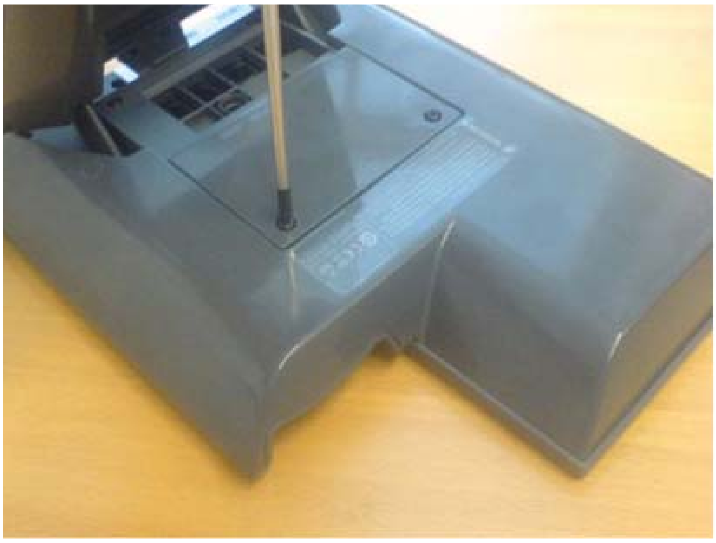


Figure 19: Mounting the option unit screws.

7. Connect the cables to the option unit. Insert the cables from under the foot console and connect the cables according to the markings on the plastic cover of the option unit (from left to right):

   - PC (if applicable)
   - LAN
   - Power (if an adapter is used)
   - External functions (if applicable)
   - Headset (if applicable)
   - Handset.

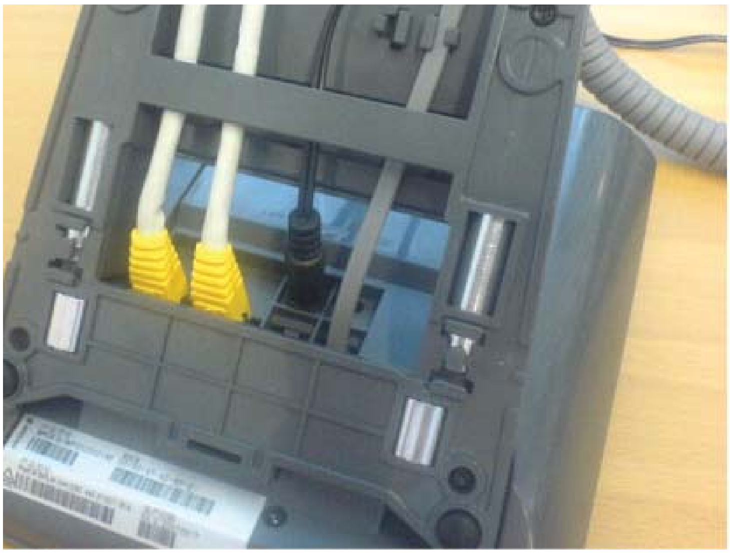


Figure 20: Mounting cables

After connecting the power adapter to an electric socket the phone can be started using the standard startup and log-on procedure.

20.1 GIGABIT ETHERNET

The option unit contains a gigabit Ethernet interface. The purpose of this unit is to pass on gigabit traffic to the PC that is connected to the IP terminal. The IP-phone itself does not require the gigabit speed. For information about power consumption, see 5 Power Equipment on page 9.

This Gigabit Ethernet option unit has support for VLAN tagging of the telephone port but not for the PC port. This means that the telephone works in an environment where the voice LAN is tagged and the data LAN has no VLAN tagging.

If a telephone equipped with the gigabit Ethernet Option unit (DBY412 01) is connected to a 10/100 megabit LAN, the telephone must be powered by a power adapter. The alternative is to remove the gigabit Ethernet unit.

20.2 EXTRA BELL/BUSY SIGNAL

See 19.3 Extra Bell And Busy Signal on page 79.

20.3 POST INSTALLATION MEASURES AFTER MOUNTING THE OPTION UNIT

Connect the power to the phone and when the phone has started, log on to the gatekeeper. Check that a call can be established and check that the installed extra equipment works.

21 EMERGENCY CALLS

There are two cases of emergency calls:

- initiated from an IP phone which is not logged on.
- initiated from an IP phone which is logged on.

21.1 LOGGED ON TELEPHONE

The call is handled as an ordinary call using the IP extension interface. The sent A-number is the extension number of the logged on user.

For DBC 444 it is possible to define three emergency text rows which are shown in the display when the telephone is logged on. This text is shown in the same text box as the follow me information. The text rows are defined in the configuration file, see *Configuration File for DBC 44X and DBC 43X*.

21.2 NOT LOGGED ON TELEPHONE

The emergency number as well as the IP address and other data for the server which will be used for the call are defined in the configuration file, see *Configuration File for DBC 44X and DBC 43X*.

In the configuration file it is also possible to define the A-number to be sent. This should be the A-number associated with the geographical area where the phone is located.

A group of phones that will send different geographical A-numbers compared to another group of phones, must use different configuration files, see 12.25 Using Multiple Configuration Files on page 47.

When the emergency call function is enabled in the configuration file, the emergency number is shown in the log on menu. When the user lifts the handset the dial tone is heard although the phone is not logged on. When the user dials the emergency number, the phone uses the IP trunk interface to establish the call. The Setup is sent directly without any admission check.

The A-number sent to the public exchange must be within the direct-in-dialing number series, otherwise the public exchange will replace this number.

After the emergency call is terminated the phone returns to the not logged on state. The emergency centre can call back to the terminal although it is logged off.

It is possible to define a first and a second choice for the emergency call server in case of that the first choice fails.

Note: As soon as the emergency number is defined in the configuration file, the log on menu in the phones indicates that it is possible to dial the emergency number. But it is very important that the emergency number is set up in the PBX and tested before it is enabled in the IP phones.

Note: Verify that it is possible for the alarm centre to call back to the number that is sent as the A-number. One possibility is that the number is answered by the PBX operator.

For DBC 444 it is possible to define three different emergency numbers and three emergency texts which are shown in the display when the telephone is logged off.

22 IP VOICE RECORDING

It is possible to record voice calls to a central recording equipment. The phones that shall have recording are monitored via the CSTA interface and this means that an Application Link or an Open Application Server (OAS) must be used to provide the CTI interface to the recording system. The call events and the IP address to the phones to be monitored are sent over the CSTA interface

For more information about the recording solution for MX-ONE Service Node see *Description for Voice Recording* and the *Interface Description for VoIP Recording Interface.*

The signaling between the recording system and the IP phones is based on SIP, although the phone is using the H.323 mode. The recording system sends an INVITE message to the phone to inform about the IP address to where the voice packets shall be sent. A SIP ACK message orders the phone to start forwarding the received and transmitted RTP streams to the logger.

There are the following options

1. Total recording: all calls to the monitored extensions are recorded
2. Record on demand: the user can start and stop the recording by pressing the recording key.

Note: It is only possible to record IP phones. No other types of phones shall be monitored.

The voice stream is sent un-encrypted to the recording equipment, if the original call is without encryption. If the call is encrypted, the telephone forwards an encrypted voice stream to the recorder. In this case the encryption keys are sent via the CSTA interface to the recording equipment.

There are a number of parameters in the configuration file for voice recording, see *Configuration File for DBC 44X and DBC 43X*.

The shortcut key for recording on the phone is initiated from the PBX.

Total recording

The recording key is lit as soon as the telephone forwards the RTP stream to the recording system.

The icon for recording in DBC444, is shown when the telephone forwards the RTP stream to the recording system.

Record on demand

The LED on the recording key on the phone is lit when the end-user has ordered the call to be recorded by pressing the key and the phone has got a confirmation from the recording system.

The icon for recording in DBC444, is shown when the telephone forwards the RTP stream to the recording system.

The URL that the telephone sends to the recording system, when the user presses the recording key, can be defined in the configuration file.

23 INSTALLING THE MY DIALOG CONTACTS APPLICATION ON A WEB SERVER

My Dialog Contacts is an application that makes it possible for the end-user to merge the contents in Microsoft® Outlook Contacts to the existing Phone Contacts in the IP phone. This application updates the Phone Contacts on the FTP server, and after that the phone is updated with the new Contacts in a file from the FTP server. This means that the Phone Contacts must be stored centrally on the FTP server, see 12.28 Configuring Central Storage of User Specific Data on page 50.

It is important how the end-user stores the external phone numbers in Microsoft® Outlook Contacts. If the external destination code starts with 0 and the area code also starts with 0, the phone cannot distinguish those numbers. If an external number in Outlook is stored with the external access code, it will **not** work. The recommendation is to store the complete external numbers in Outlook i.e. +country code, area code, phone number. Example: 46 is the country code, 08 is the area code and 7190000 is the phone number, store +4687190000.

My Dialog Contacts program shall be stored on a web server and the end-user shall get a link to a web page from which this application can be downloaded to his/her PC. Java run time library 5.0 or higher is needed on the end-used PC (can be downloaded from the Sun® home page).

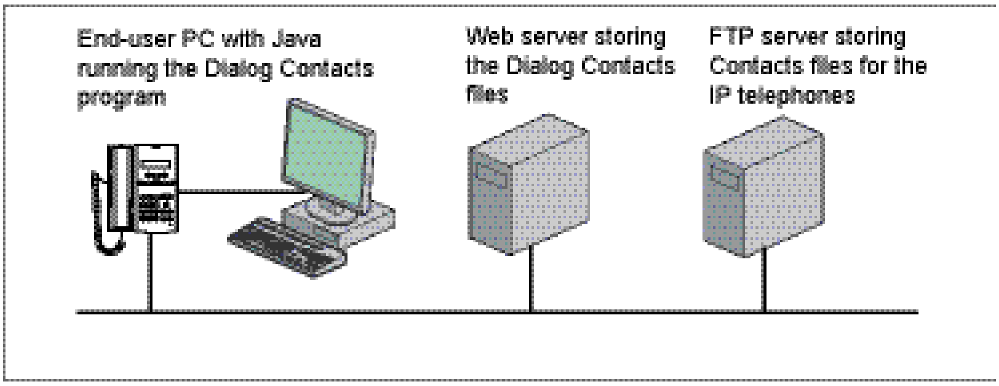

End-user PC with Java running the Dialog Contacts program
Web server storing the Dialog Contacts files
FTP server storing Contacts files for the IP telephones

Figure 21: Components in My Dialog Contacts

For instructions on how to use the **My Dialog Contacts** application, see the *User Guide for each telephone model.*

23.1 INSTALLING MY DIALOG CONTACTS

Deliverable

This application is delivered as a zip-file containing:

- A folder **My Dialog Contacts** containing the program files to install and a read me file.
- A sample web page, **dialogwebstart.htm**, containing the code to include on a company web page for the user to download the application.
- An example of a company web page **index.html**

Installation of the program files:

- Unzip the zip file to a temporary location
- Copy the folder **My Dialog Contacts** to a location on a web server that the end-users can access.

The end-user starts the downloading of My Dialog Contacts from a web page (this file is called **index.htm**). This web page has a link to **dialogwebstart.htm** and shall also contain information and instructions to the end-user. The included web page is an example, which can be changed to a layout according to the customer’s need.

The **dialogwebstart.htm** file contains sample code to enable download of the **dialog4000.jnlp** file. In **dialogwebstart.htm** the reference to the appropriate URL where the application is stored, has to be set.

When using an IIS server as the web server, the file types **.properties** and **.jnlp** must be enabled in a similar way as described above, see 7.1 Installing the Software Server on page 11.

For more details bout the installation, see the read me file included in the zip file.

Configuration

The file **dialog.jnlp** contains the configuration parameters. The file can be updated with any text editor. The parameters are described in the read me file.

24 QUALITY OF SERVICE (QOS)

As an administrator, it is possible to view the quality of service statistics of the connection for the last 10 calls using the phone's Web interface. The statistics shows for example the delay, jitter and number of lost packets. For more information on QoS, see *Maintenance Instructions for DBC 43X and DBC 44x*.

25 DHCP SERVER

25.1 INSTALLATION

Installation of the DHCP (Dynamic Host Configuration Protocol) server should be done according to the documentation of the manufacturer. Both PC and Unix versions are supported.

The following DHCP servers have been tested with the IP phone:

- Microsoft® Windows® NT4.
- Microsoft® Windows® 2000 and 2003 server.
- Redhat® Linux.

25.2 DATA FROM DHCP

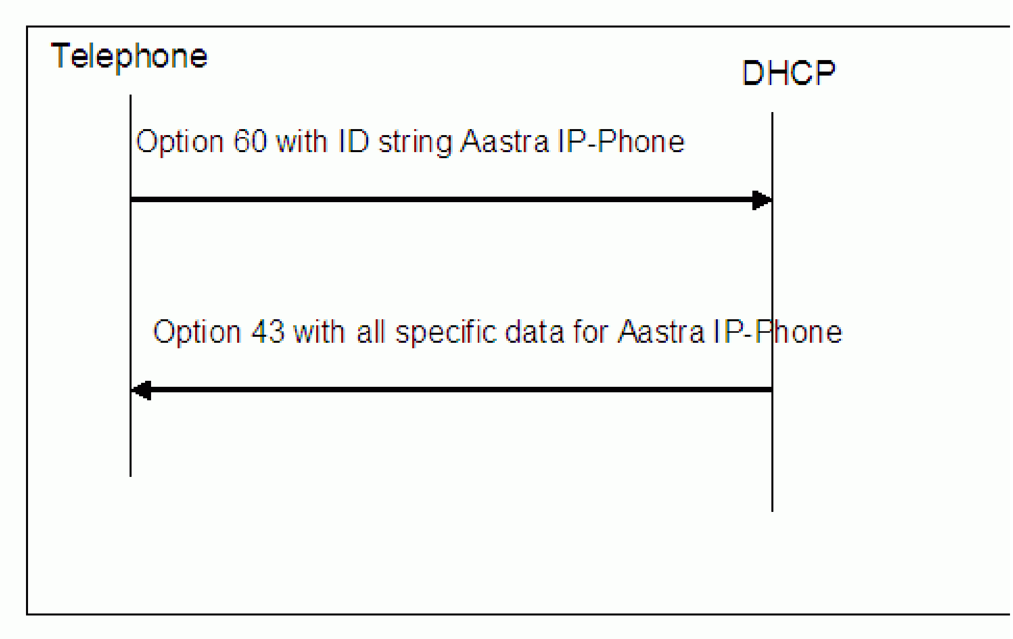
The phone has support for DHCP by which the following IP configuration data can be provided:

- Own IP address, subnet mask and default gateway, received in the DHCP standard fields (1 and 3).
- The domain name for the LAN segment (DNS domain name) in code 15. The domain name is used in the automatic gatekeeper discovery routine, see section 12.16 Enabling Automatic Gatekeeper Discovery on page 37. It can also be used when several configuration files are used, see section 12.25 Using Multiple Configuration Files on page 47.
- The vendor specific field 43 can be used to get the following data:
  - IP address of the software server, see section 7 Setting Up the Software Server on page 11.
  - IP address and port number of the http proxy server. If the software is to be loaded from a SW server outside the firewall the proxy settings are needed.
  - The telephony domain name. This can be used in the automatic gatekeeper discovery routine, see section 12.16 Enabling Automatic Gatekeeper Discovery on page 37. It can also be used when several configuration files are used, see section 12.25 Using Multiple Configuration Files on page 47.
  - A list with VLAN identities. These are used when the phone will automatically be assigned to a VLAN, see 12.18 Using Virtual LAN (VLAN) on page 38.
- DNS identity (web address) for the phone.

For the complete usage of the domain name, see section 12.30 Domain Name on page 54.

25.3 DHCP SETTINGS FOR OPTION 43 AND 60

DHCP option 60 (vendor class identifier) and option 43 (vendor specific information field) are used by the phone to get the specific configuration data from the DHCP server. The flow is as follows:


Telephone
DHCP
Option 60 with ID string Aastra IP-Phone
Option 43 with all specific data for Aastra IP-Phone

The procedure to initiate the data for option 43 and 60 in the DHCP server is as follows:

1) define vendor class (option 60)

2) set predefines options (option 43)

3) set scope options (option 43)

25.3.1 VENDOR CLASS IDENTIFIER

Vendor class identifier (option 60) option is used to secure that option 43 data for the specific vendor is sent from the DHCP server to the client. The phone sends the vendor class identifier to the DHCP server, which returns vendor specific information for the requested vendor class in option 43 to the phone.

When vendor class identifier shall be used to get the option 43 data for the Mitel IP-Phone, it is necessary to initiate the vendor class *Mitel IP-Phone* in the DHCP server and in some cases also the vendor class *Ericsson IP-Phone*, see section 25.3.2 Vendor Specific Information Field on page 90.

25.3.2 VENDOR SPECIFIC INFORMATION FIELD

The vendor specific information field (option 43) is coded as shown in the figure below.

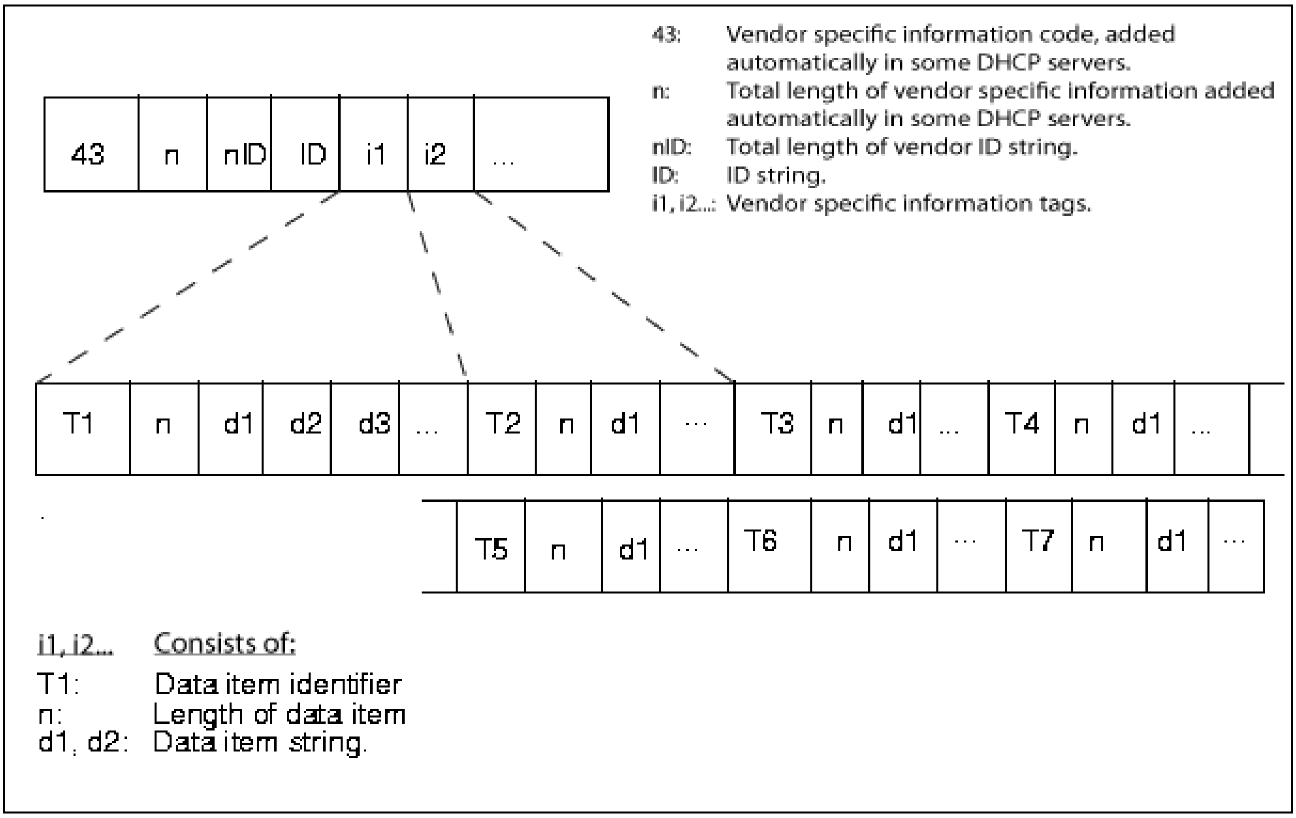

43
n
nID
ID
i1
i2
...
43: Vendor specific information code, added automatically in some DHCP servers.
n: Total length of vendor specific information added automatically in some DHCP servers.
nID: Total length of vendor ID string.
ID: ID string.
i1, i2...: Vendor specific information tags.
T1
n
d1
d2
d3
...
T2
n
d1
...
T3
n
d1
...
T4
n
d1
...
T5
n
d1
...
T6
n
d1
...
T7
n
d1
...
i1, i2... Consists of:
T1: Data item identifier
n: Length of data item
d1, d2: Data item string.

Figure 22: Vendor Specific Information structure

Within this vendor field, a substructure is used with the different tags:

Tag 01 (T1 in the figure): SW server’s IP address in ASCII text format.

Tag 02 (T2 in the figure): Proxy server’s IP address also in ASCII text format.

Tag 03 (T3 in the figure): Proxy port, also this in ASCII text format.

Tag 04 (T4 in the figure): Telephony domain name in ASCII text format.

Tag 05 (T5 in the figure): VLAN identity 1 for the phone, in ASCII text format.

Tag 06 (T6 in the figure): VLAN identity 2 for the phone, in ASCII text format.

Tag 07 (T7 in the figure): VLAN identity 3 for the phone, in ASCII text format.

Note: The VLAN identity for the phone defined here in option 43 must not be equal to the VLAN identity for the PC defined in the configuration file.

For more details about VLAN identity, see section 12.18 Using Virtual LAN (VLAN) on page 38.

The different tags are optional, but if tag 02 is used tag 03 is mandatory.

The following applies for the ID string:

- At new installation the string *Mitel IP-Phone* shall be entered in DHCP option 43.

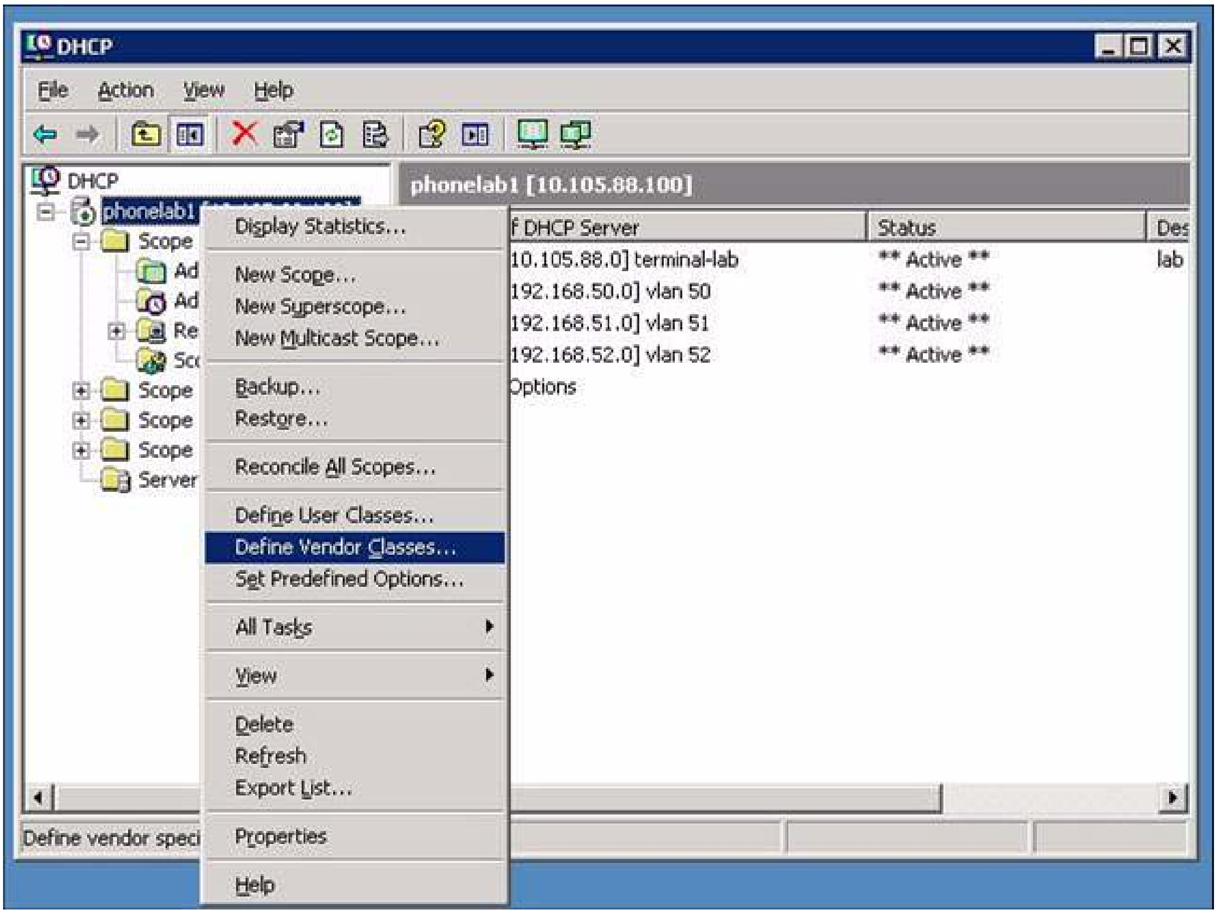
The recommendation is to enter one vendor class for Mitel IP-Phone in the DHCP server.

If DBC 43x and DBC 44x phones shall be mixed with DBC 42x, see installation instructions for DBC42x.

25.4 MICROSOFT® WINDOWS® 2003

Example of settings in Microsoft® Windows® 2003 server.

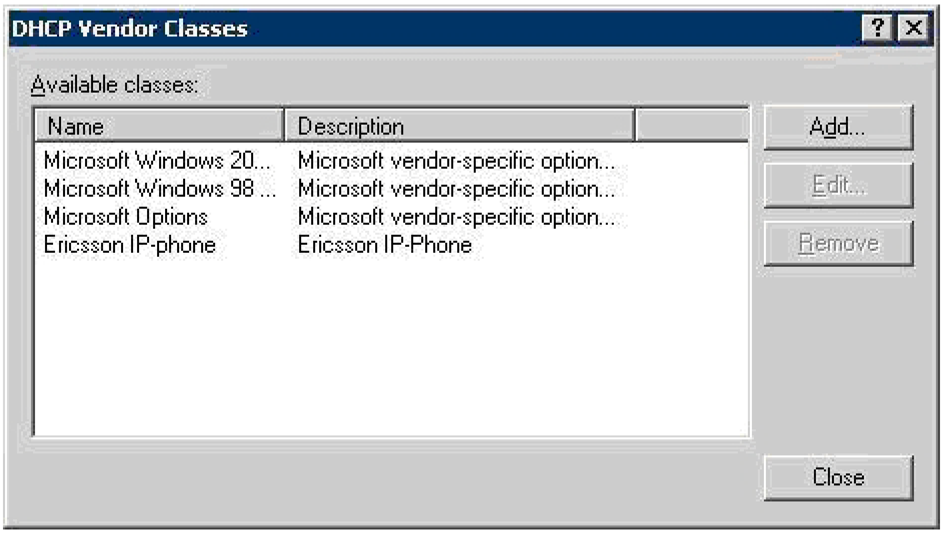
25.4.1 DEFINE VENDOR CLASS



f DHCP Server	Status	Des
10.105.88.0] terminal-lab	** Active **	lab
192.168.50.0] vlan 50	** Active **	
192.168.51.0] vlan 51	** Active **	
192.168.52.0] vlan 52	** Active **	
Options		

Figure 23: Define Vendor Classes

Select *Define Vendor Classes* to get the menu where the vendor classes are entered.



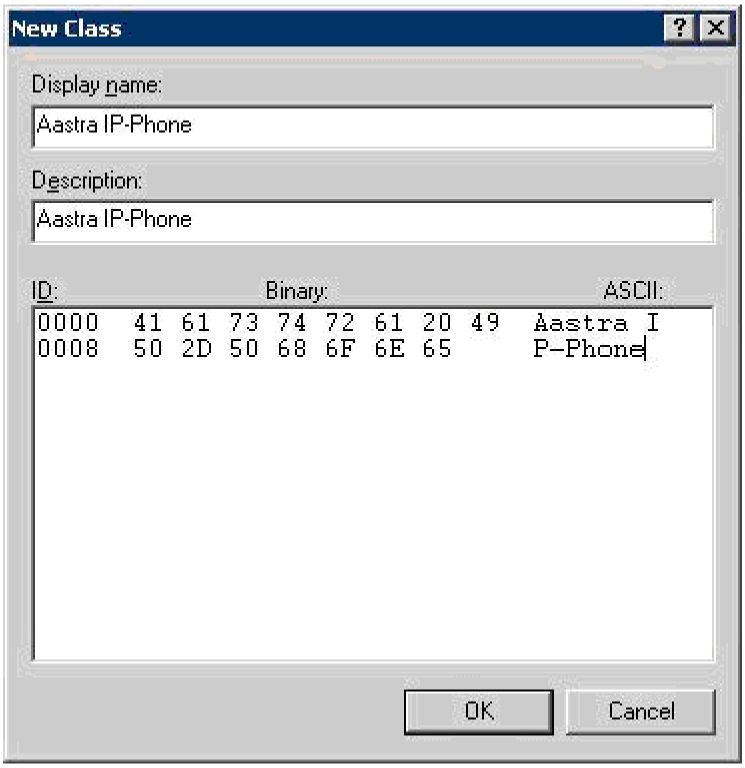
DHCP Vendor Classes

Available classes:

Name	Description
Microsoft Windows 20...	Microsoft vendor-specific option...
Microsoft Windows 98 ...	Microsoft vendor-specific option...
Microsoft Options	Microsoft vendor-specific option...
Ericsson IP-phone	Ericsson IP-Phone

Figure 24: DHCP Vendor Classes

If the vendor class Mitel IP-Phone does not exist, press *Add* to create the new vendor class. In the next menu the ID string *Mitel IP-Phone* has to be entered:



New Class

Display name: Aastra IP-Phone

Description: Aastra IP-Phone

ID: Binary: ASCII:

```
0000   41 61 73 74 72 61 20 49   Aastra I
0008   50 2D 50 68 6F 6E 65      P-Phone
```

Figure 25: Add Vendor Class

It is possible to move the cursor between the Binary and the ASCII area to make it easier to enter the ID data.

When the data has been entered, press *OK*.

Close the window and proceed to set predefined options.

In some scenarios, the vendor class *Ericsson IP-Phone* has also to be initiated, see section 25.3.2 Vendor Specific Information Field on page 90.

The *Standard* vendor class shall be avoided. It is sent out to all devices that ask for option 43 data and if the device does not interpret the data correct, it can cause problem.

25.4.2 SET PREDEFINED OPTIONS

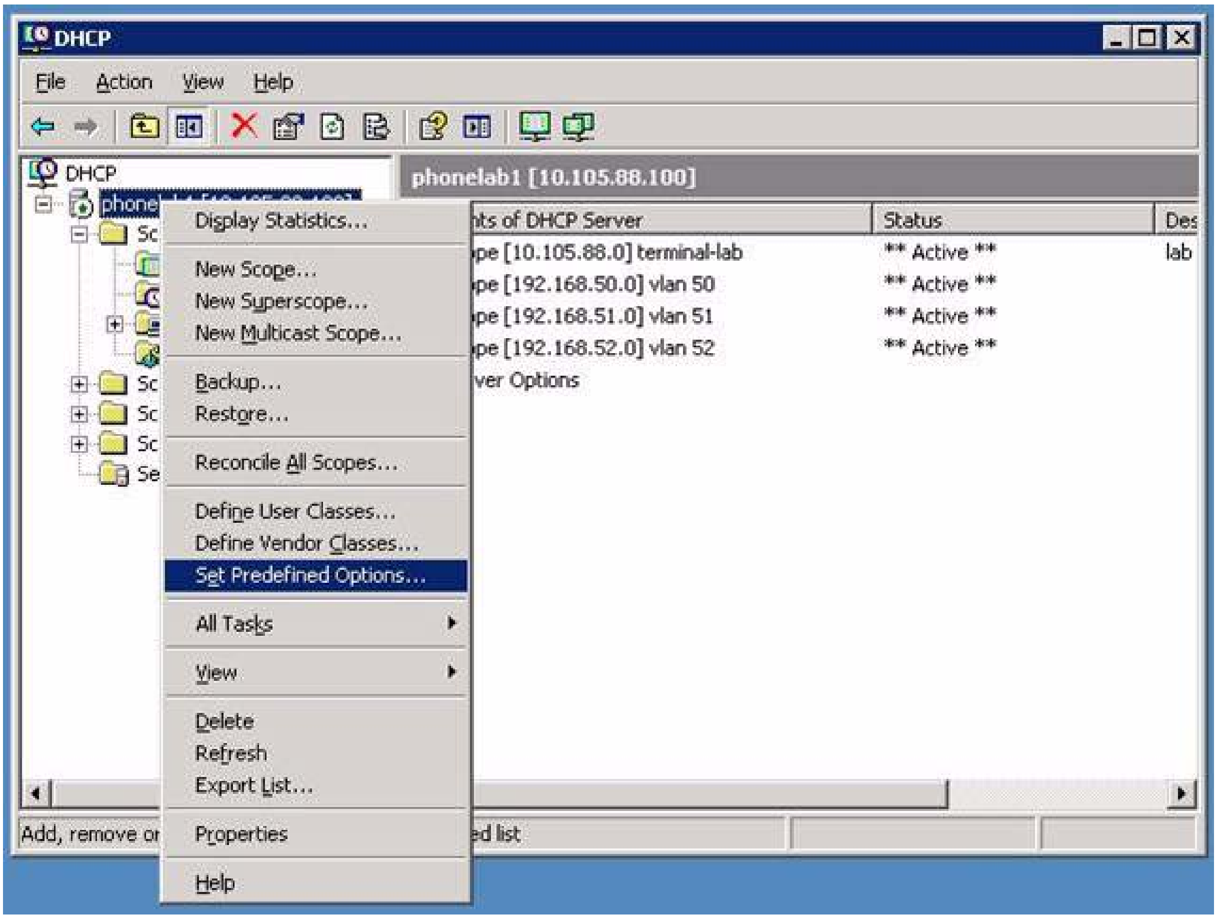
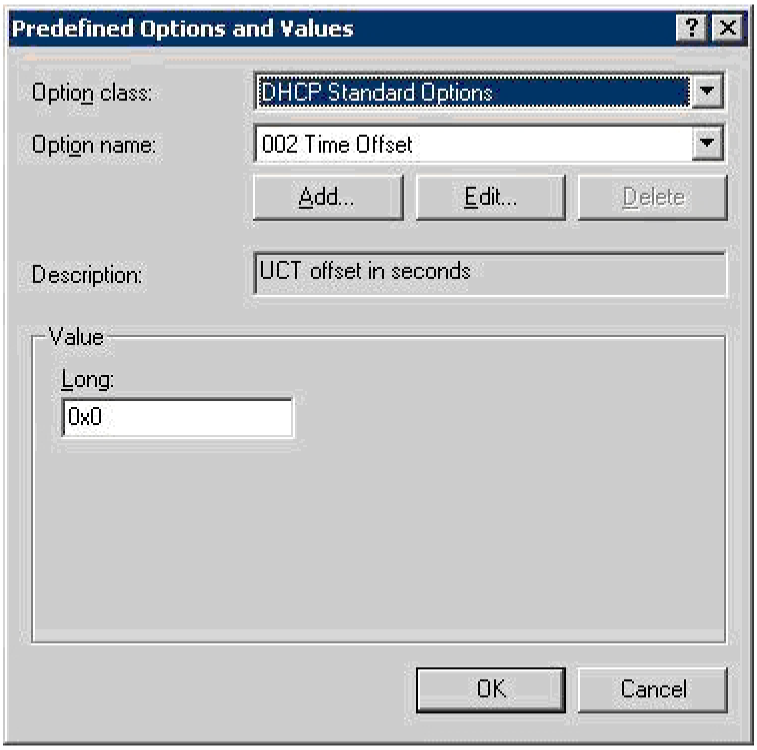


Figure 26: Set Predefined Options

Select *Set Predefined Options* to get the menu to enter option 43 data.



Option class: DHCP Standard Options

Option name: 002 Time Offset

Description: UCT offset in seconds

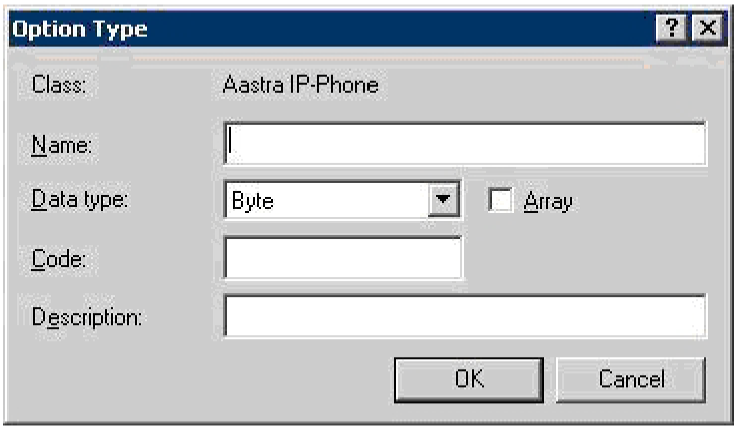
Value

Long: 0x0

Figure 27: Predefined Options and Values

Select Mitel IP-Phone in the drop down list in the Option class field and press the Add button.

The next menu is shown below:



Class: Aastra IP-Phone

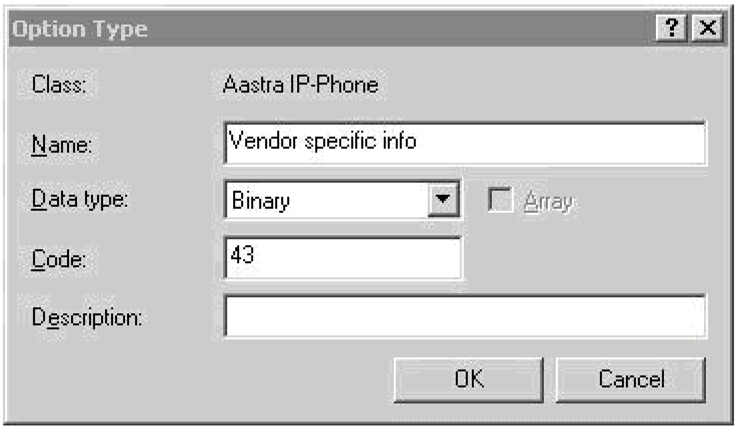
Data type: Byte

Figure 28: Option Type

This is the default view and data has to be entered manually:

Name: Enter *Vendor specific info*
Data type: Select *Binary* in the drop down list
Code: Enter 43
Description: Can be left empty

The filled in dialog will look like:



Class: Aastra IP-Phone

Name: Vendor specific info

Data type: Binary

□ Array

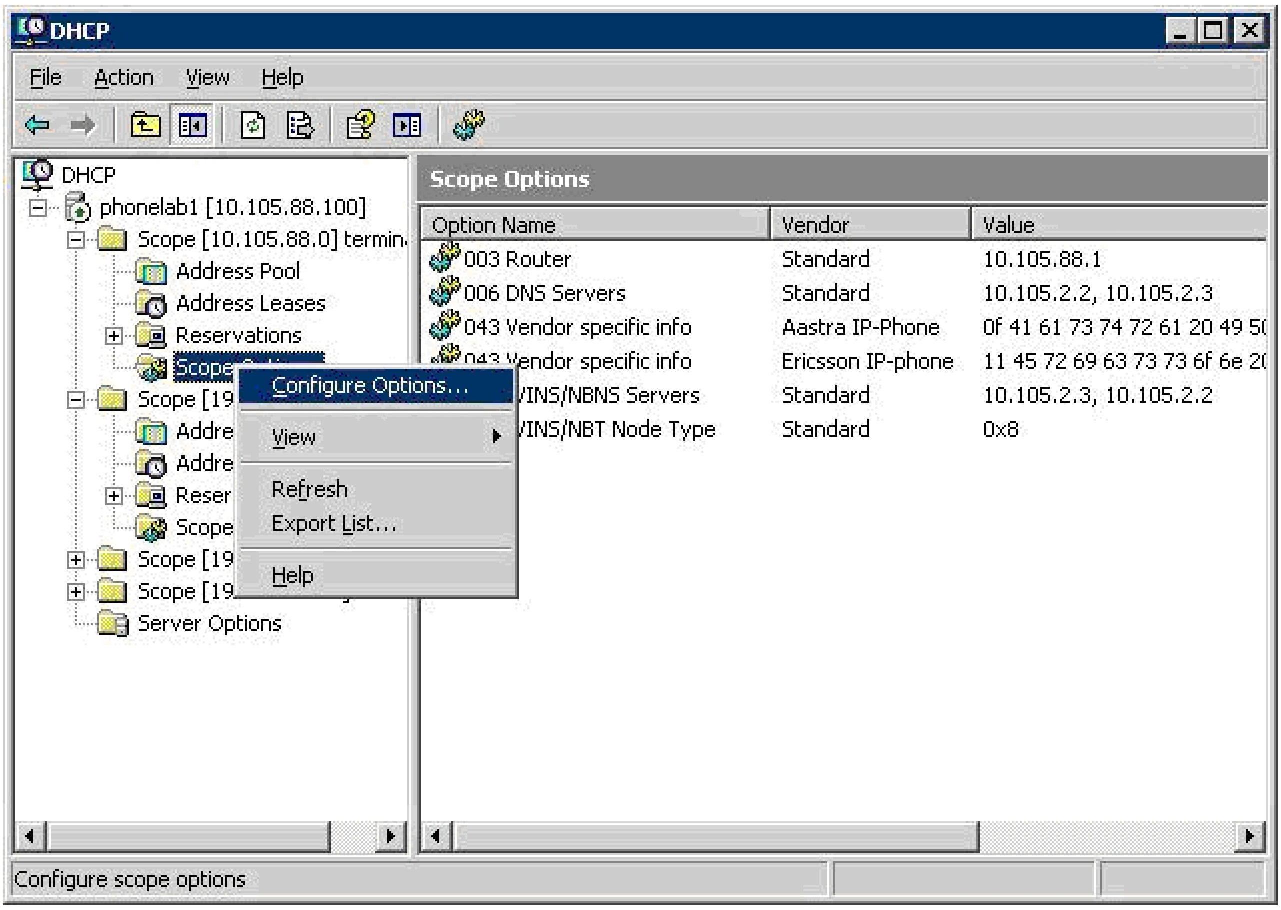
Code: 43

Description:

Figure 29: Filled in Option Type Dialog

Press *OK* and the window with Predefined Options and values will occur again. Press *OK* again and the menu will be closed.

25.4.3 SET SCOPE OPTIONS

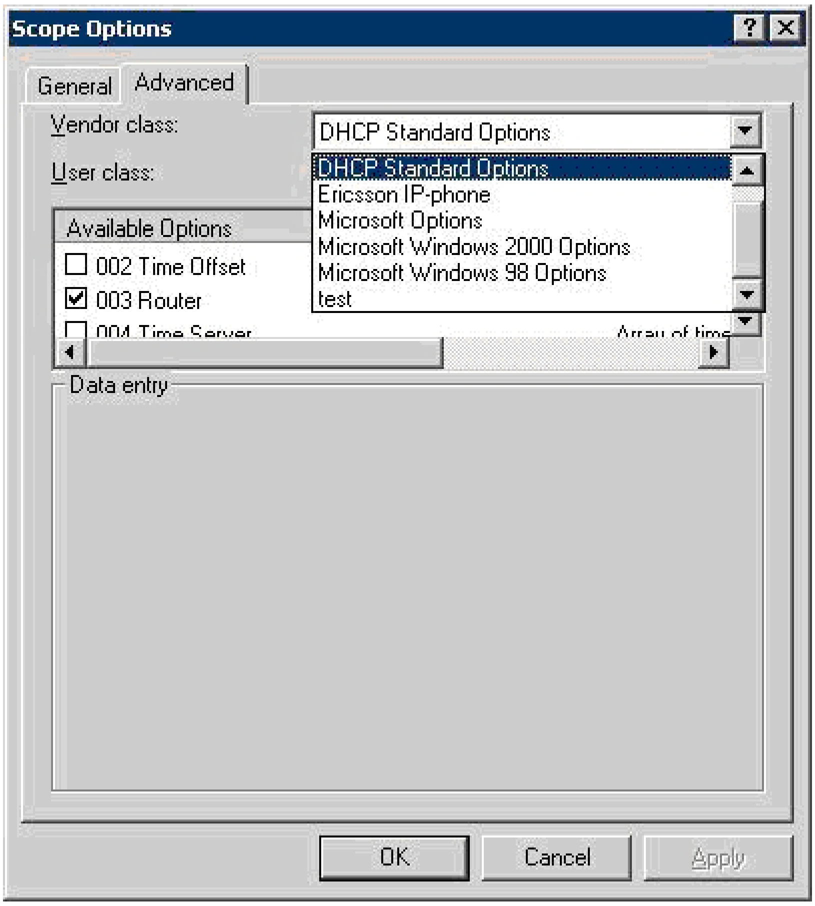


Option Name	Vendor	Value
003 Router	Standard	10.105.88.1
006 DNS Servers	Standard	10.105.2.2, 10.105.2.3
043 Vendor specific info	Aastra IP-Phone	0f 41 61 73 74 72 61 20 49 5(
043 Vendor specific info	Ericsson IP-phone	11 45 72 69 63 73 73 6f 6e 2(
WINS/NBNS Servers	Standard	10.105.2.3, 10.105.2.2
WINS/NBT Node Type	Standard	0x8

Configure scope options

Figure 30: Configure Options

Select *Configure Options*.



Scope Options

Vendor class: DHCP Standard Options

User class:

Available Options

☐ 002 Time Offset

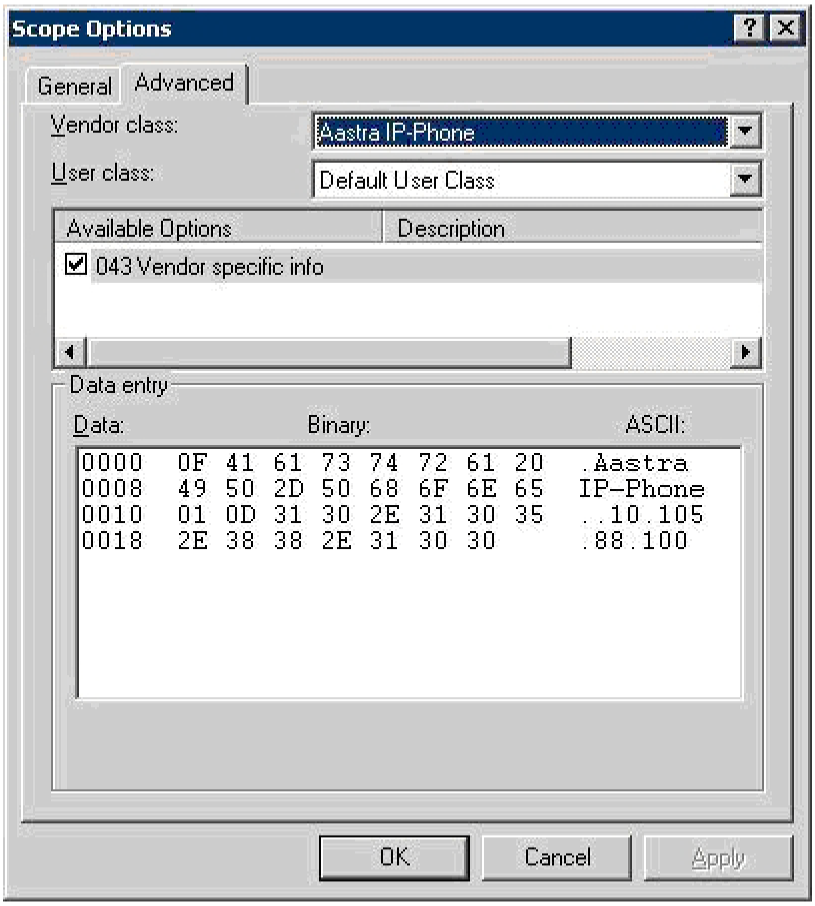
☑ 003 Router

☐ 004 Time Server

Figure 31: Scope Options

Select *Advanced* tab and scroll in the *Vendor class* field until Mitel IP-Phone is selected. Press *OK*.

Next menu is where the ID strings and the tags are set, according to the figure in section 25.3.2 Vendor Specific Information Field on page 90.



Scope Options

General | Advanced

Vendor class: Aastra IP-Phone

User class: Default User Class

Available Options	Description
☑ 043 Vendor specific info	

Data entry

Data: Binary: ASCII:

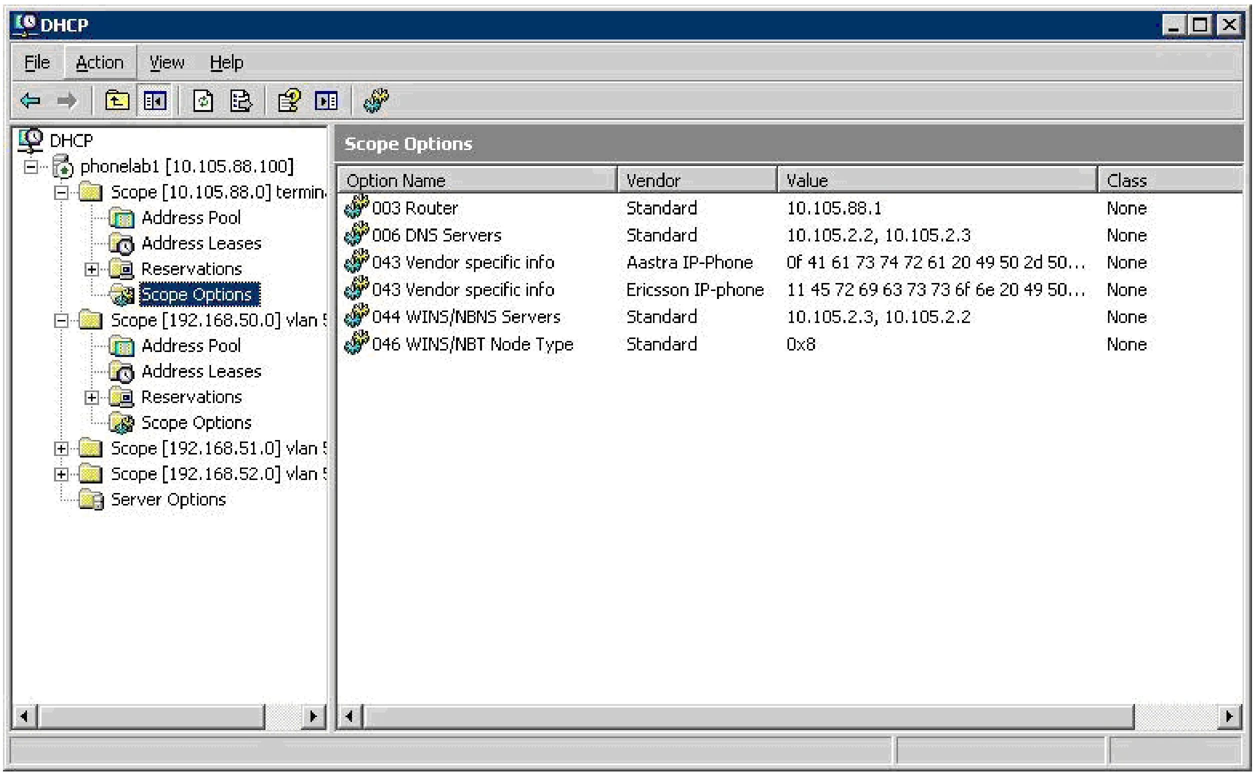
```
0000   0F 41 61 73 74 72 61 20   .Aastra
0008   49 50 2D 50 68 6F 6E 65   IP-Phone
0010   01 0D 31 30 2E 31 30 35   ..10.105
0018   2E 38 38 2E 31 30 30      .88.100
```

Figure 32: Windows® 2003 server DHCP settings

It is possible to move the cursor between the Binary and the ASCII area to make it easier to enter the option 43 data.

This example shows that the total length of the vendor specific information is 0x1F, the length of the ID string is 0x0F and the string is Mitel IP-Phone, The next byte 01 is the tag for the SW server's IP address, 0x0D is the length and then follows the IP address (10.105.88.100). If more tags than tag 01 for the SW-server is needed, add the additional tags according to the figure in section 25.3.2 Vendor Specific Information Field on page 90.

The picture below shows an example how option 43 can look like when two vendor classes are initiated.



Option Name	Vendor	Value	Class
003 Router	Standard	10.105.88.1	None
006 DNS Servers	Standard	10.105.2.2, 10.105.2.3	None
043 Vendor specific info	Aastra IP-Phone	0f 41 61 73 74 72 61 20 49 50 2d 50...	None
043 Vendor specific info	Ericsson IP-phone	11 45 72 69 63 73 73 6f 6e 20 49 50...	None
044 WINS/NBNS Servers	Standard	10.105.2.3, 10.105.2.2	None
046 WINS/NBT Node Type	Standard	0x8	None

Figure 33: Two Initiated Vendor Classes

25.5 LINUX DHCP SETTINGS

Example of settings in the Linux server:

```
subnet 192.168.6.192 netmask 255.255.255.192 {

option routers 192.168.6.254;

# class "Aastra IP-Phone" {
# match option vendor-class-identifier;
#}
# class "Ericsson IP-Phone" {
# match option vendor-class-identifier;
#}
if substring (option vendor-class-identifier, 0, 15) = "Aastra
IP-Phone"
{
    option vendor-encapsulated-options "\x0fAastra
IP-Phone\x01\x0b192.168.0.1\x04\x16aastrado-
main.aastra.se\x05\x03452";
} else if substring (option vendor-class-identifier, 0, 17) =
"Ericsson IP-Phone" {
    option vendor-encapsulated-options "\x11Ericsson IP-Phone
\x01\x0b192.168.0.1\x04\x16aastradomain.aastra.se\x05\x03452";
}
#
# DHCP settings continued
```

Example when using Vendor Class and the IP address for the sw-server is 192.168.0.1, the telephony domain is *aastradomain.aastra.se* and the VLAN identity is 452

26 SECURITY

There are two security features:

- LAN access control, see 12.3 Enabling Automatic LAN Access Control on page 27.
- Protection of VoIP signaling with TLS and media encryption with SRTP.

The TLS and SRTP support can be enabled/disabled from the configuration file, see *Configuration File for DBC 44X and DBC 43X*.

In addition there is a security policy in the telephony system which also affects the behavior of the IP phones. For MX-ONE Service Node, see the description for *SECURITY*.

The security policy is checked at the registration time. Once the phone is registered, all kinds of calls can be established from a security perspective.

When a secure IP to IP call is established, with TLS and SRTP, a secure icon (a padlock) is shown in the display. For gateway calls, known as gateway connection by the system where the phone is registered, the secure icon is not shown, because the other end-party can have an un-secure connection.

26.1 PROTECTION OF VOIP SIGNALING

The signalling between the IP phones and the gatekeeper is protected by means of TLS (Transport Layer Security) according to RFC 2246.

The TLS protection affects the registration and the call handling. Multicast traffic (automatic gatekeeper discovery) is not protected.

The TLS server (gatekeeper) makes use of a digital certificate to authenticate itself towards the terminal. The terminal authenticate themselves by means of the password (ordinary password to register towards the gatekeeper) sent in the RAS/RRQ message.

TCP port 3727 is used for RAS over TCP.

TCP port 1300 is used for Secure Call Setup. For more information, see 12.32 Selection of Transport Addresses (Port Numbers) on page 55.

The cipher suite TLS_RSA_WITH_AES_128_CBC_SHA defined in RFC 3268 is used.

TLS is not supported on top of UDP. In order to support TLS protection of the RAS messages these are sent over a TCP connection, opened by the IP phone, before a TLS connection has been set up.

The TLS support can be enabled/disabled from the configuration file, see *Configuration File for DBC 44X and DBC 43X*.

26.1.1 CERTIFICATES

The digital certificates are in X.509 version 3 format with the file extension **.pem**. For more detailed information about creating the certificate, see *operational directions for Certificate Management* in the CPI library.

In order for the phone to be able to authenticate the server, the phone has a certificate repository with a number of root certificates or trusted certificates (see the table below). These are included in the IP phone firmware in the factory.

It is also possible to add more root certificates beside these by reading in the file with the certificate from the software server. The file must be stored under the folder ***/certificates/H323***, see section 7.2 Creating a Directory Structure on page 11. The path to the certificate file is specified in the configuration file.

Table 4 X.509 root certificates to support TLS server authentication

Certificate Authority	Comment
Baltimore	
Entrust	md5WithRSAEncryption
Entrust	sha1WithRSAEncryption
Equifax CA-1	md5WithRSAEncryption
Equifax CA-2	sha1WithRSAEncryption
Equifax	sha1WithRSAEncryption
Equifax Secure Global eBusiness CA-1	
GTE Cyber Trust	
QuoVadis CA2	
SecureSign Root CA1	
SecureSign Root CA2	
SecureSign Root CA3	
Tawnte Premium Server CA	
Tawnte Server CA	
ValiCert Class 1	
ValiCert Class 2	
ValiCert Class 3	
VeriSign Class 3	
VeriSign Class 3 - G2	
VeriSign Class 4 - G2	
VeriSign Class 3 - G3	
VeriSign Class 4 - G3	
VeriSign Test Root CA	md2WithRSAEncryption
VeriSign Test Root CA	sha1WithRSAEncryption

26.1.2 REGISTRATION TOWARDS THE GATEKEEPER

At log on the phone prompts the user to enter the extension number and the password. If the user do not have a password, the phone tries to log on to the insecure UDP port 1719.

In case the IP phone tries to log on securely but the establishment of the TCP connection fails, this is interpreted as the gatekeeper does not support secure mode. The phone shall back off to RAS over UDP. The possibility to back off to UDP is managed via a parameter in the configuration file, see the description for *Configuration File for DBC 44X and DBC 43X*.

During the TLS negotiation, the server will authenticate itself by using a digital certificate, see 26.1.1 Certificates on page 101.

In the configuration file there is an option whether the client shall validate the server certificate or not. If the option is enabled but the server does not have a certificate that is signed by one of the Certificate Authorities supported in the phone or if the certificate has expired, it will result in a failed authentication.

26.1.3 CALL SETUP AND CALL CONTROL

When the IP phone that is registered securely, sets up a call using H.225 Q.931 messages, it sends the requests to TCP port 1300 instead of TCP 1720.

In order to negotiate the capability of the call, an H.245 negotiation takes place on a new TCP connection between the terminal and the gatekeeper. The TCP port to be used is negotiated during the H.225 signaling. The TCP connection can be initiated by either part. This TCP connection is protected by means of TLS as well.

This implies that during a call there are three TCP connections existing between the terminal and the gatekeeper.

26.1.4 UDP FILTERING

All the UDP ports that are not used, can be blocked for security reasons. For a description of all UDP and TCP ports, see 12.32 Selection of Transport Addresses (Port Numbers) on page 55.

The default value is that the UDP filtering is enabled, but can be disabled with a parameter in the configuration file, see description of Configuration File for DBC 43x and DBC 44x.

26.1.5 TCP FILTERING

All the TCP ports that are not used, can be blocked for security reasons. For a description of all UDP and TCP ports, see 12.32 Selection of Transport Addresses (Port Numbers) on page 55.

The default value is that the TCP filtering is enabled, but can be disabled with a parameter in the configuration file, see description of Configuration File for DBC 43x and DBC 44x.

26.2 SRTP

Secure RTP, SRTP (RFC 3711), is supported by DBC 43X and DBC 44X phones. The supported encryption algorithm is AES 128 (Advanced Encryption Standard) in counter mode for SRTP and SRTCP. HMAC_SHA1_80 is supported for SRTCP.

Media encryption is negotiated using H.245 i.e. both the capability as well as the keys. (The key negotiation phase is based on H.235.8).

The following codecs have SRTP support: G.711 A-law, G.711 µ-law, G.722, G.723.1, G.729a and G.729ab.

Beside the possibility to enable/disable TLS and SRTP via the phone configuration file, SRTP can be temporary disabled for a certain phone via a SSH command. For information on how to configure SRTP when logged on to the phone using SSH, use the **Help** command.