

DBC 420

INSTALLATION INSTRUCTIONS



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>.

PATENTS

Mitel's Power Over Ethernet (PoE) Powered Device (PD) products are covered by one or more of the U.S. patents (and any foreign patent counterparts thereto) identified at Mitel's website: www.mitel.com/patents.

For more information on the PD patents that are licensed, please refer to www.cmspatents.com.

© Copyright 2016, Mitel Networks Corporation

All rights reserved

1

GENERAL

1.1

SCOPE

The MX-ONE IP phone DBC 420 02, also called MiVoice 4420, can be connected to a number of Mitel's PABXes or equivalent.

The DBC 420 02 phone use the H.323 protocol.

Connected to ASB 501 04

The IP phone is connected via a LAN to the IP device board IPLU/ELU32. The board together with the system software works as a gatekeeper, providing address translation, bandwidth management, admission control and call control.

A limited number of IP terminals can be registered towards each IPLU/ELU32 board, for capacity see installation planning for IP EXTENSION.

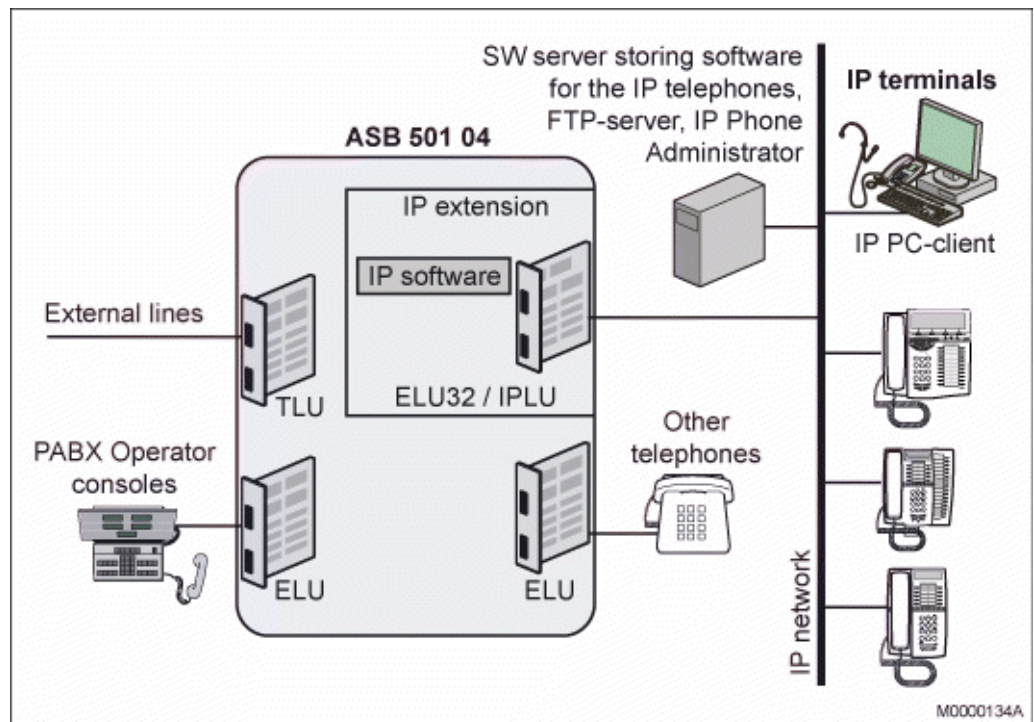


Figure 1: Connection of the IP phone towards ASB 501 04

A password for each IP extension can be initiated in the exchange. The password is used to check that the user is allowed to log on with the entered extension number.

ASB 501 04 has support for automatic gatekeeper discovery, which means that the IP address to the gatekeeper (IPLU/ELU32 board) is retrieved automatically in the IP phone.

Connected to MX-ONE

The figure below shows a typical setup for the MX-ONE.

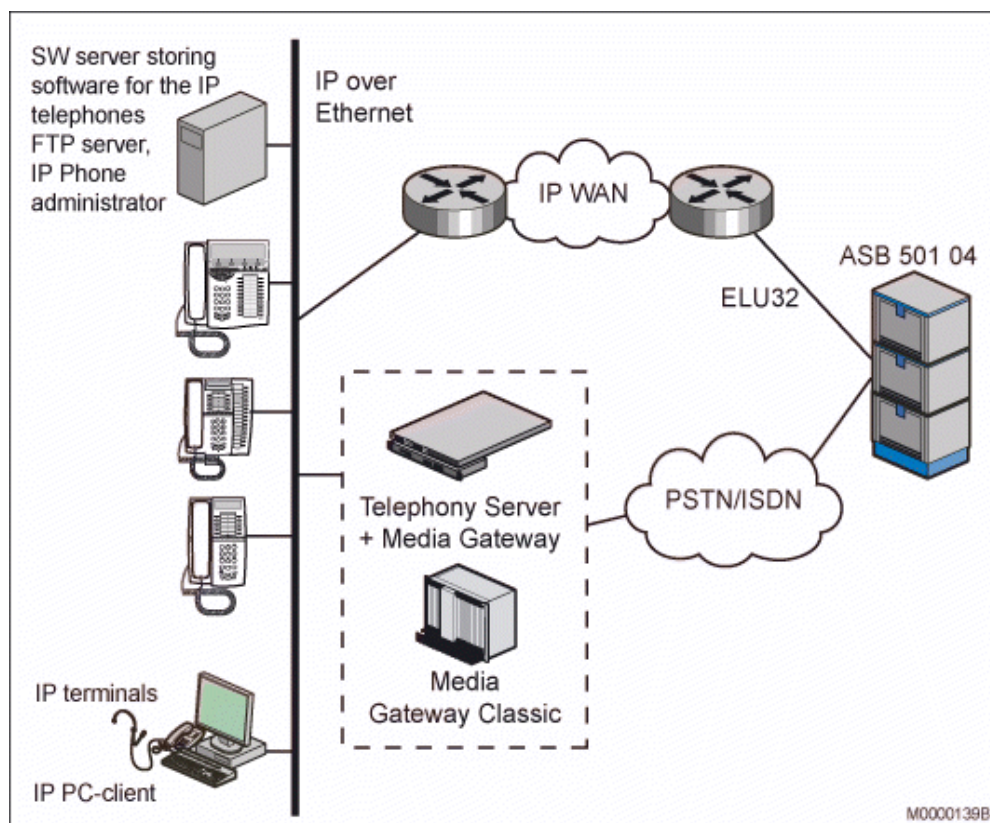


Figure 2: Typical MX-ONE setup

Connected to EBG/WebSwitch

The IP phone can be used with EBG (Enterprise Branch Gateway)/WebSwitch 2.6 or later, yet version 3.0 software is required to support the password protection feature for the phone.

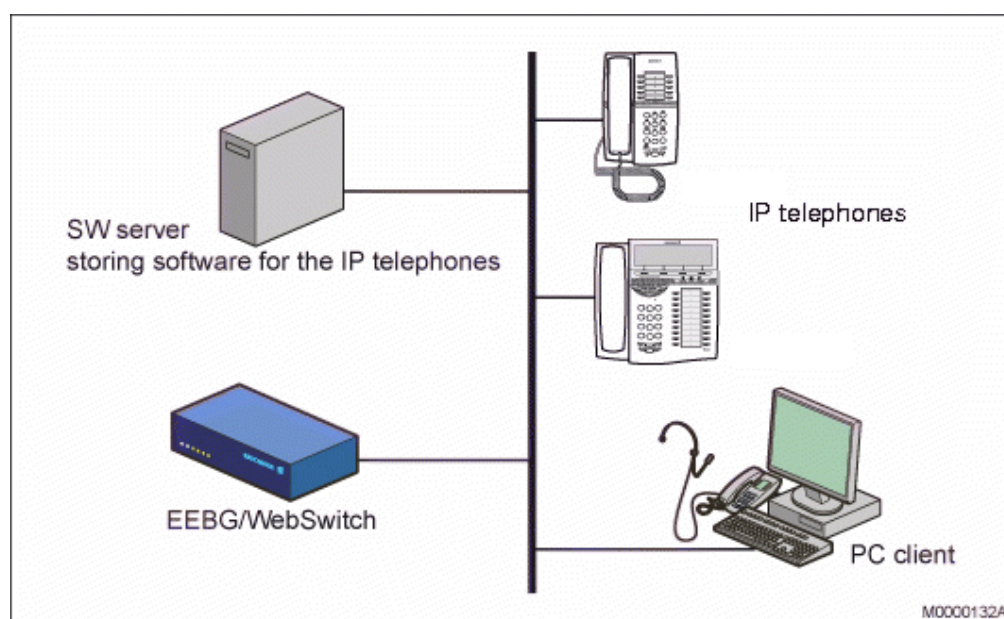


Figure 3: Connection of the IP phone towards EBG/WebSwitch
Connected to BusinessPhone

The IP phone can be used together with BusinessPhone 5.1 or later

1.2

ENVIRONMENTAL REQUIREMENTS

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

2

AIDS

Wall mounting requires additional screws and spacers, see 7.36 Wall Mounting of the IP Phone on page 44 .

3

PREPARATIONS

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

4

POWER EQUIPMENT

The IP phone can either be powered from a 24 V AC/AC adapter or from a power hub. If it is powered from an adapter the following alternatives exist:

- RES 141 312/1 for the EU market except for the UK (230 V)
- RES 141 314/1 for the UK market (230 V)
- RES 141 318/1 for the 110 V markets

For other markets the AC/AC adapter is locally sourced. The phone can also be powered with 24-48 Volts DC.

Power consumption: 1.7 W (only phone) and 3W with the AC/AC adapter included.

As an alternative the IP phone can be powered via the LAN from a power hub. The phone supports the standard IEEE 802.3AF for power over LAN.

In the IEEE 802.3AF standard there is an optional part for the *power class signature* , this is supported by the phone. The phone reports power class 1, which means less than 4W required.

5

EARTHING/GROUNDING

No special earthing/grounding is needed.

The IP phone needs a shielded Ethernet cable for the network connection.

6

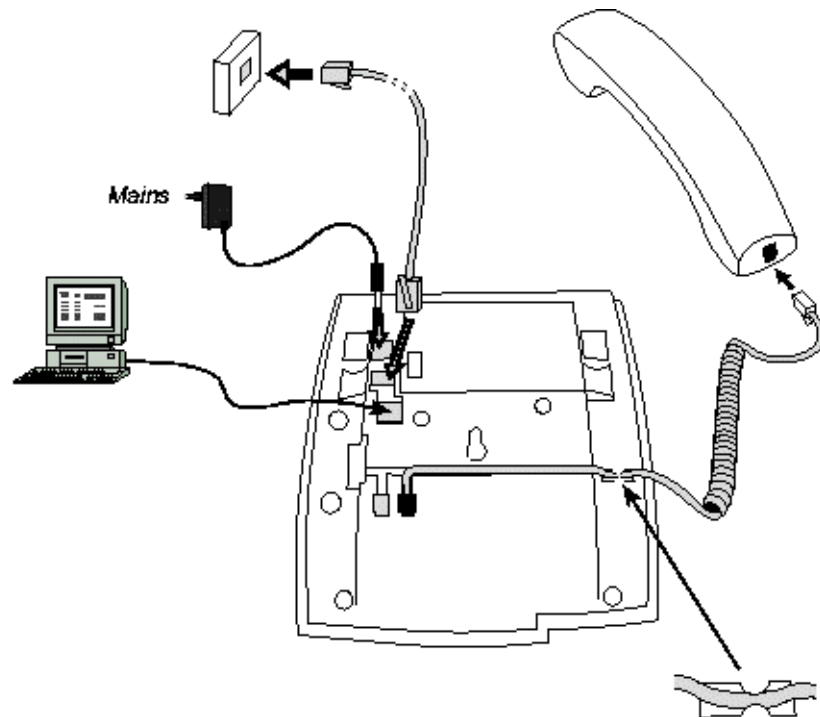
CABLING

The maximum line length between an IP phone and the LAN is 100 meters (328 feet) according to IEEE 802.3. Category 5 cables are recommended.

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

- TSR 901 0452/3000

The figure shows where all the cables are connected in the bottom of the phone.



*) AC/AC adapter is not needed when a power hub is used

Figure 4: Connection of the phone

7 INSTALLATION

7.1 HOW TO START A NEW PHONE

Connect one end of the network cable to the network outlet and the other end to the connector marked LAN on the bottom of the IP phone. See 6 Cabling on page 6.

If there is no LAN connection the **Status LED** will be flashing with double blink.

The DBC 420 02 phone is only intended for use with IP address from DHCP and not with fixed IP addresses. For maintenance reasons it is possible to use a fixed IP address, see 7.1.3 Using a fixed IP address on page 8.

To get the IP address to the software server and to the IP Phone Administrator server, see 7.11 IP Phone Administrator on page 29.

7.1.1 START A PHONE IN A LAN WITH A DHCP SERVER

This section describes the procedure when the phone will use IP addresses provided by a DHCP server, see 7.8.2 Data from DHCP on page 14.

If tagged virtual LAN (VLAN) will be used, see 7.18 Virtual LAN (VLAN) on page 34 .

After power up of the IP phone, the **MUTE LED** will be lit for a few seconds, if there is no network connected the **Status LED** will double flash, otherwise the **Status LED** will flash until the phone is registered and ready to use when this LED is lit.

If the installation personnel want to monitor the progress more closely, the administrator mode must be entered, see 7.25 Administrator Mode on page 38.

When the administrator mode is used the **Admin mode LED** will be lit. The **DHCP LED** will lit indicating that DHCP will be used. During 30 seconds it is possible change between using DHCP or not, see 7.1.3 Using a fixed IP address on page 8. After 30 seconds or if the **C** key is pressed, the boot sequence continues.

The **IP address LED** will flash until the phones has got an IP address from the DHCP server, then this LED flashes slowly.

Next, the phone will try to contact the software server and the **SW LED** will flash. The phone fetches the configuration file and if necessary a new version of the software from the SW server. When the SW transfer is ready the **SW LED** will be steady lit and the administrator mode will be automatically turned off and all the LEDs will be switched off.

The phone performs a test to verify operation of the phone circuits, if all goes well the **Selftest LED** is lit for one second. The **Status LED** will be flashing.

The next step is to set the IP address to the gatekeeper. To set the IP address to the gatekeeper in H.323 mode, see 7.12 Gatekeeper Address on page 32.

Then the phone will register towards the gatekeeper. The IP extension must already be initiated in the system. Enter the directory number and the password or Personal Identification Number (PIN) via the web interface, see 7.29.1 Set data at installation of the phone on page 40. Use the **log off restriction** menu in the web interface.

When the phone is registered the **Status LED** is lit and the phone is ready for making and receiving calls.

The description of how to use the phone with ASB 501 04, see directions for use for *DBC 420*.

The description of how to use the phone with MX-ONE, see directions for use for *DBC 420 FOR MX-ONE*.

For information on using the IP phone in a EBG/WebSwitch environment, please refer to the QUICK REFERENCE GUIDE, DBC 420.

Error case

If there is no response from the DHCP server, the **DHCP LED** used in administrator mode will not stop blinking, if administrator mode is not used, the **Status LED** flashes.

7.1.2

UPDATE OF THE SOFTWARE IN THE IP PHONE

This section is reached from the section, see 7.1.1 Start a phone in a LAN with a DHCP server on page 7

Two types of updates may be performed on the IP phone:

- Update of both the application software and the bootROM.
- Update of only the application software.

Note: It is not possible to only update the boot software. If the boot software will be updated, the application has to be updated as well.

BootROM and/or application software will be updated

The update is fully automatic. The **Status LED** flashes until the phone is ready for use, for more status information, the administrator mode can be entered, see 7.25 Administrator Mode on page 38 . The update may take several minutes, depending on if both the boot and the application or only the boot will be updated. It is important not to disconnect the phone during this time.

7.1.3

USING A FIXED IP ADDRESS

If DHCP cannot be used for some reason it is possible, for maintenance reasons, to use a fixed IP address. The reason for not using fixed IP addresses in normal operation is because it is difficult to set the IP addresses in each phone. The following procedure will be used in the boot sequence for changing to fixed IP address:

1. Create a local LAN with the PC and the phone. The phone will use the default IP address 130.100.17.100. Use an IP address in the PC using the same subnet address.
2. Connect the power to the phone. Enter the administrator mode, see 7.25 Administrator Mode on page 38 .
3. When the **DHCP LED** is lit, press this key. The LED is switched off.
4. The phone will use the default IP address: 130.100.17.100
5. Log in to the phone via the administrator web interface.
6. Set the wanted IP address from the web interface.

To return to the normal case using DHCP:

1. Reboot the phone
2. Enter the administrator mode, see 7.25 Administrator Mode on page 38 .
3. Press the key with the **DHCP LED** to enable DHCP. The LED will be lit.

7.2 DELIVERY METHOD

The IP phone is delivered in a box together with two foot consoles, one handset, one handset cord, designation labels, designation covers and an assembly instruction.

For spare parts, see spare part list for TELEPHONE SETS DBC 220+.

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, see 7.4 SW Loading on page 9.

7.3 CONNECTION OF THE HANDSET

The handset cord is connected with one end (short uncoiled) to the handset and the other end (long uncoiled) to the connector on the bottom of the IP phone marked HANDSET.

7.4 SW LOADING

The software to be loaded into the phone is stored on a web server with the HTTP protocol. This web server is called SW server in the menus and in this document. The following files must be stored on the server:

d42x02-applic_R1A.dat

(CAA 158 0043) The application firmware for the DBC 42x 02 phones. R1A in the file name is an example.

d42x02-boot_R1A.dat

(CAA 158 0044) The boot ROM firmware. This software is used to be able to load the application into the IP phone. R1A in the file name is an example.

d42d02-config.txt

(CAA 158 0042) The configuration file. 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, see the description for *CONFIGURATION FILE FOR DBC 42X*.

d42x02-lang_R1A.txt

(CAA 158 0045) The language file containing all the languages that are supported. R1A in the file name is an example.

When the IP phone is powered up, the phone fetches the configuration file from the SW- server. If the software version defined in the configuration file is different than the software version in the phone, the phone fetches the application software file and/or the boot ROM software file from the SW server. The new software is automatically stored into the flash memory in the phone.

It is possible to load both newer and previous software versions with this method.

It is possible to check the software version in the phone, see 7.23 Software Version on page 37

7.5 SEVERAL CONFIGURATION FILES

A certain group of IP phones will 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:

- 1) Use the DNS (Domain Name Service) domain name received from DHCP, see 7.8.2 Data from DHCP on page 14.
- 2) Use the telephony domain name received in the vendor specific field in the DHCP messages, see 7.8.2 Data from DHCP on page 14.
- 3) Subnet method, see 7.5.3 Subnet method on page 10.

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.

It is also possible to set the IP address of the SW server manually in the phone. In this case there must be one SW server per configuration file.

7.5.1 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/dbc42x02/d42x02-config.txt, see 7.6.3 Directory structure on page 11.

7.5.2 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/dbc42x02/d42x02-config.txt, see 7.6.3 Directory structure on page 11.

7.5.3 SUBNET METHOD

The URI consists of the network address together with the subnet mask length. The network address consists of the IP address of the phone 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/dbc42x02/d42x02-config.txt. The component -26 is the length of the subnet mask (number of ones in the binary value of the subnet mask), see 7.6.3 Directory structure on page 11.

7.5.4 PRIORITY BETWEEN THE DIFFERENT METHODS

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

- 1) The telephony domain tag in option 43
- 2) The DNS domain in option 15
- 3) Subnet method
- 4) The default configuration file is fetched. This file is stored under /dbc42x02/d42x02-config.txt.

7.6

SOFTWARE SERVER (SW SERVER)

A software server with the HTTP protocol is used for storing the firmware for the IP phone.

The IP address to the software server can be provided by one of the following methods:

- 1) Manually via the administrator web interface.
- 2) DHCP, see 7.8.2 Data from DHCP on page 14. This method has priority over the DNS SRV method.
- 3) DNS SRV resource records, see 7.7 DNS SRV Resource Records on page 14.

The priority between the different methods is according to the list above.

In a MX-ONE environment, the host for the MX-ONE Service Node and the IP phone software server cannot be the same.

7.6.1

INSTALLATION

Installation of the HTTP server should be done according to the manufacturer's documentation. Both PC and unix versions are supported.

7.6.2

HTTP SERVERS

As the SW server, the following HTTP servers have been tested with the IP phone:

- Microsoft® NT4.
- Microsoft® Windows® 2000 and 2003 server. When using Windows® server the file type **.dat** must be enabled: Select **Properties**, edit **File type**, set **Associated extension: .dat** and set **Content type (MIME): application /octet.stream**
- Apache 1.3.3 on Microsoft® Windows® or on Redhat® Linux 5.2.
- Apache Tomcat. When the IP Phone Configuration File in MX-ONE Service Node Manager shall be used the Tomcat server is mandatory. For more information see the description for CONFIGURATION FILE FOR DBC 42X

The files according to 7.4 SW Loading on page 9 must be stored on the SW server under the directories as described in 7.6.3 Directory structure on page 11.

7.6.3

DIRECTORY STRUCTURE

The directory structure under the http root directory must be created, see Figure 5 Directory structure using domain names on page 12. When several different configuration files are to be used for different groups of phones where each group is a member of a specific domain, the structure with different domain names are used. In this case the configuration files have the same name although they have different contents to define 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, and not the application and boot, that needs to be stored under each domain directory name.

If the phones do not find any configuration file in a domain directory, the file in the directory **web-server root/dbc42x02** is used for the DBC 420 02 phone.

DBC 420 02, DBC 422 02 and DBC 425 02 use the same configuration file, stored in the **dbc42x02** directory.

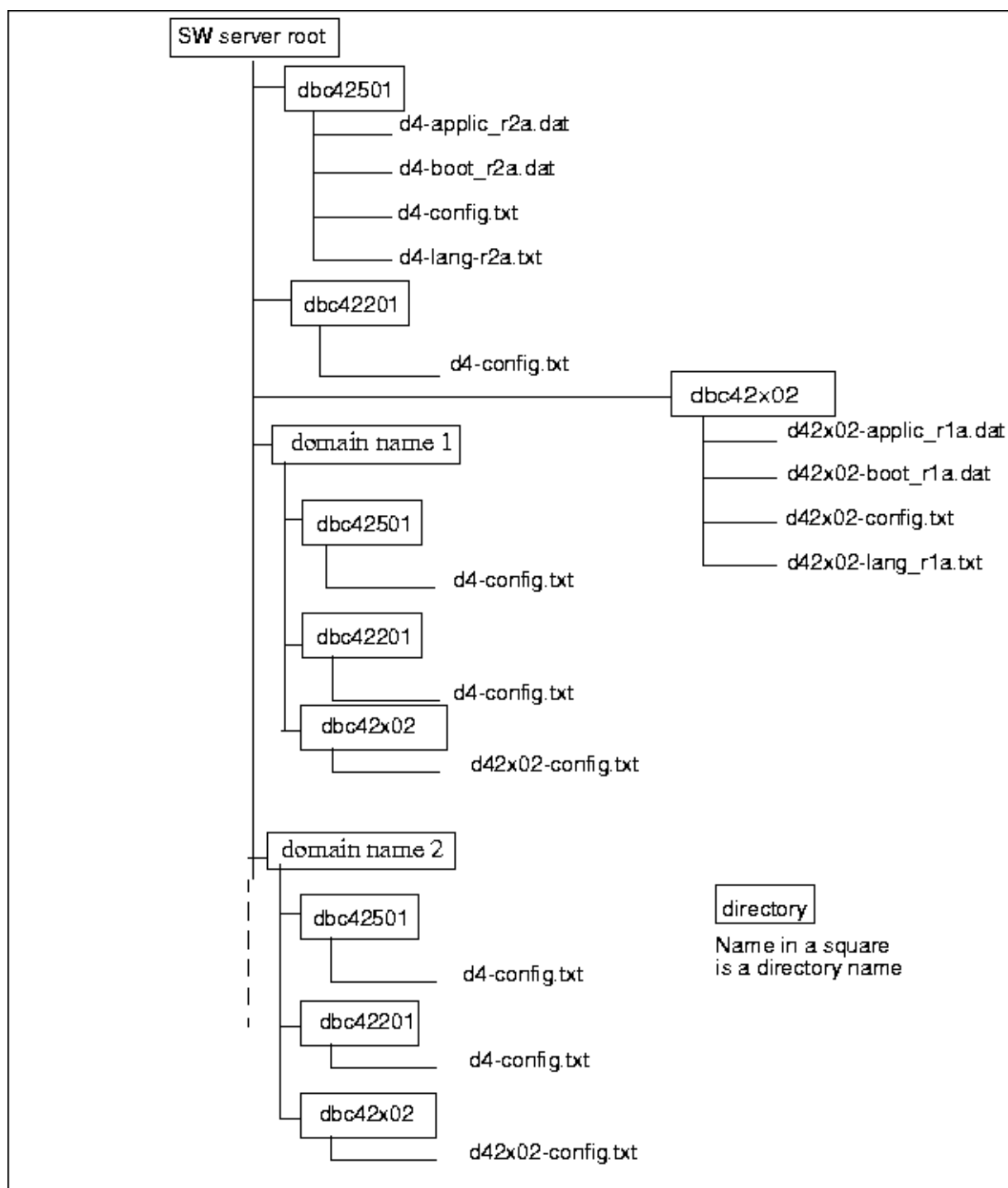


Figure 5: Directory structure using domain names

If the subnet method is used, see 7.5.3 Subnet method on page 10, 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.

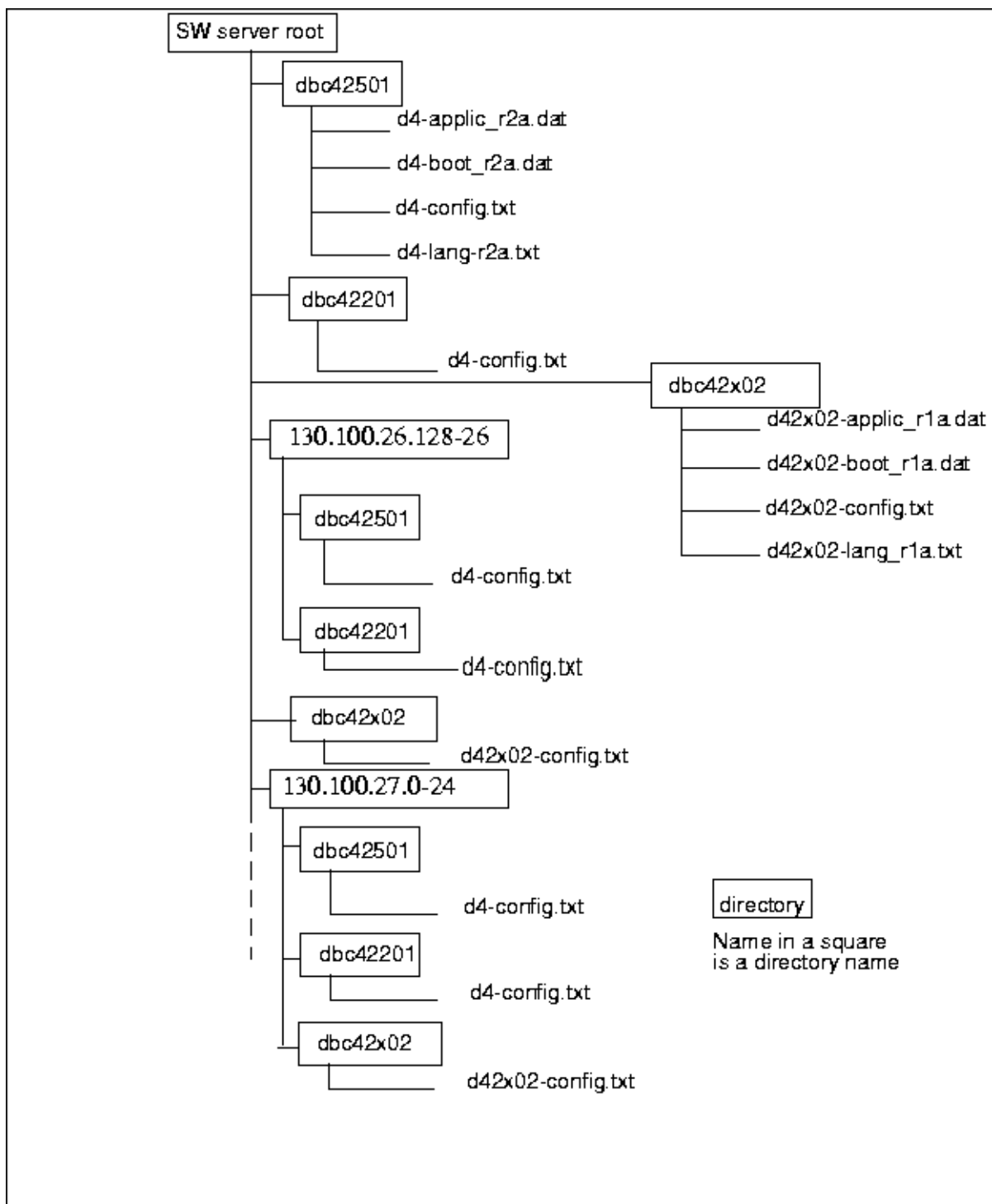


Figure 6: Directory structure using the subnet method

7.7

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:

- 1) The IP address to the software server. To get this option, make sure that the IP address to the SW server is retrieved automatically, which is the default value but can be verified via the administrator web interface. 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.
- 2) 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. This is an advantage compared to using option 43 in the DHCP messages, which all the devices on the LAN receive. If a device does not handle option 43 in a correct way, this can cause problems for this device.

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

To enter data into these records, see installation instructions for *DBC 425* section ENTER DATA IN DNS SRV RESOURCE RECORDS.

7.8

DHCP SERVER

7.8.1

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 telephone:

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

7.8.2

DATA FROM DHCP

The telephone 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 7.13 Automatic Gatekeeper Discovery on page 33. It can also be used when several configuration files are used, see section 7.5 Several Configuration Files on page 9.
- The vendor specific field 43 can be used to get the following data:

- IP address of the software server, see section 7.6 Software Server (SW 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 7.13 Automatic Gatekeeper Discovery on page 33. It can also be used when several configuration files are used, see section 7.5 Several Configuration Files on page 9.
 - A list with VLAN identities. These are used when the telephone will automatically be assigned to a VLAN, see section 7.18 Virtual LAN (VLAN) on page 34.
- DNS identity (web address) for the telephone.

For the complete usage of the domain name, see section 7.15 Domain name on page 33.

7.8.3

DHCP SETTINGS FOR OPTION 43 AND 60

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

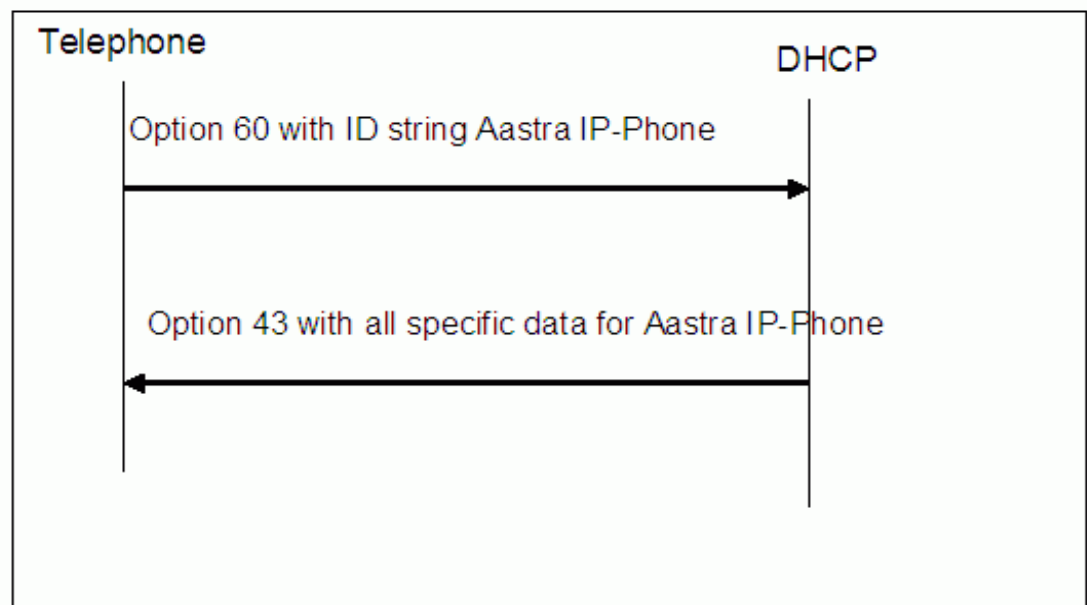


Figure 7:

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)

7.8.3.1

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 telephone sends the vendor class identifier to the DHCP server, which returns vendor specific information for the requested vendor class in option 43 to the telephone.

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 7.8.3.2 Vendor Specific Information Field on page 16.

7.8.3.2

Vendor Specific Information Field

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

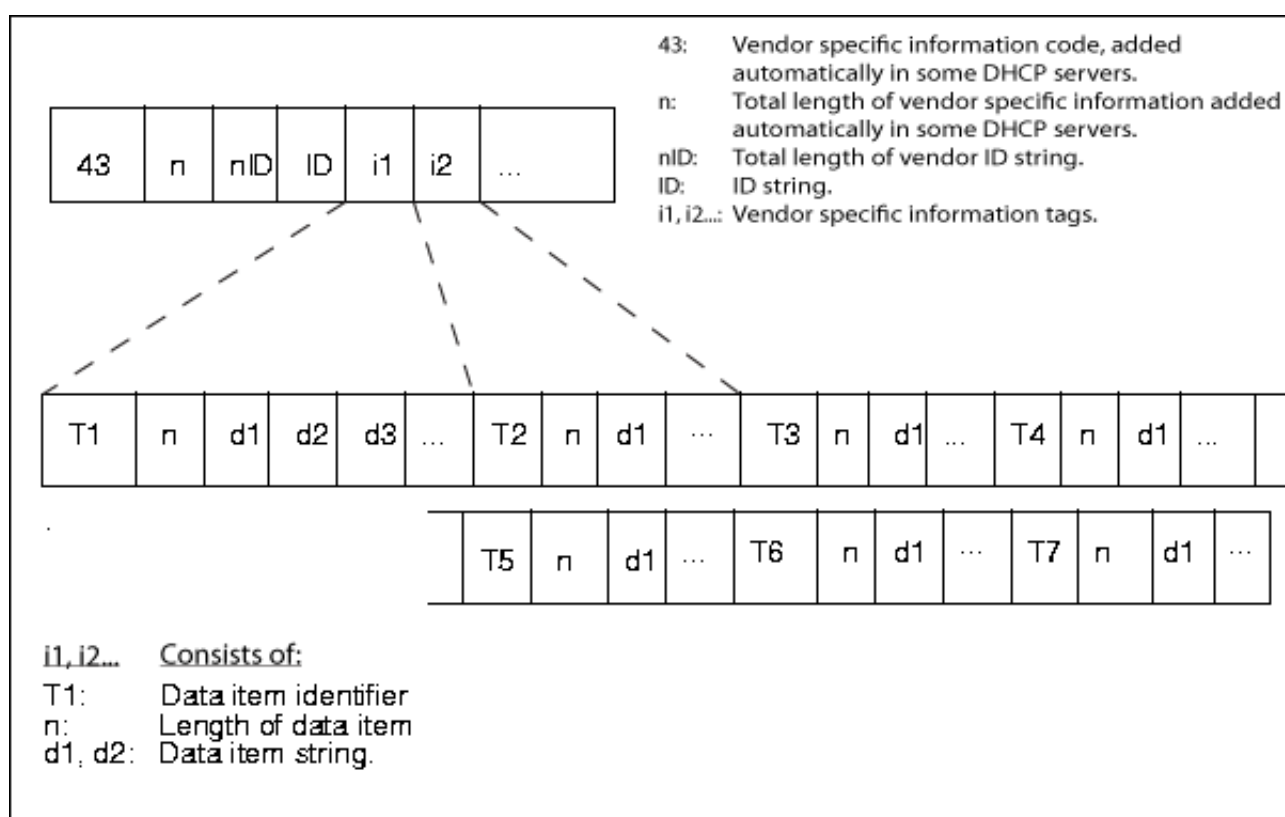


Figure 8: Vendor Specific Information structure

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 telephone, in ASCII text format.

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

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

Note: The VLAN identity for the telephone 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 7.18 Virtual LAN (VLAN) on page 34.

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.
- For DBC 42x02 (version 2) telephones: at upgrading (to application R7K or later and boot R3S or later) of a site where the string *Ericsson IP-Phone* is used in DHCP option 43 and:
 - if vendor class (option 60) is used, **it is mandatory to initiate the new vendor class for Mitel IP-Phone.**
 - if vendor class (option 60) is **not** used, the string *Ericsson IP-Phone* can be kept in the DHCP server. The telephone DBC 42x 02 can handle both strings (but it is not allowed to have both strings in the same option 43 structure).
- For DBC42x 01 (version 1) telephones, the ID string must be *Ericsson IP-Phone*. This means that when mixing version 1 with version 2 phones the following applies:
 - if vendor class (option 60) has been used, **it is mandatory to initiate the new vendor class for Mitel IP-Phone.**
 - if vendor class (option 60) has **not** been used, the string must not be changed, DBC 42x 01 can only handle the string *Ericsson IP-Phone*.

The recommendation is to enter vendor classes in the DHCP server, one vendor class for Mitel IP-Phone and another for Ericsson IP-Phone (in case of new installation it is sufficient with only the first one). The vendor specific information tags shall be equal within the two vendor classes. See also section 7.8.3.1 Vendor Class Identifier on page 16.

7.8.4

MICROSOFT® WINDOWS® 2003

Example of settings in Microsoft® Windows® 2003 server.

7.8.4.1

Define Vendor Class

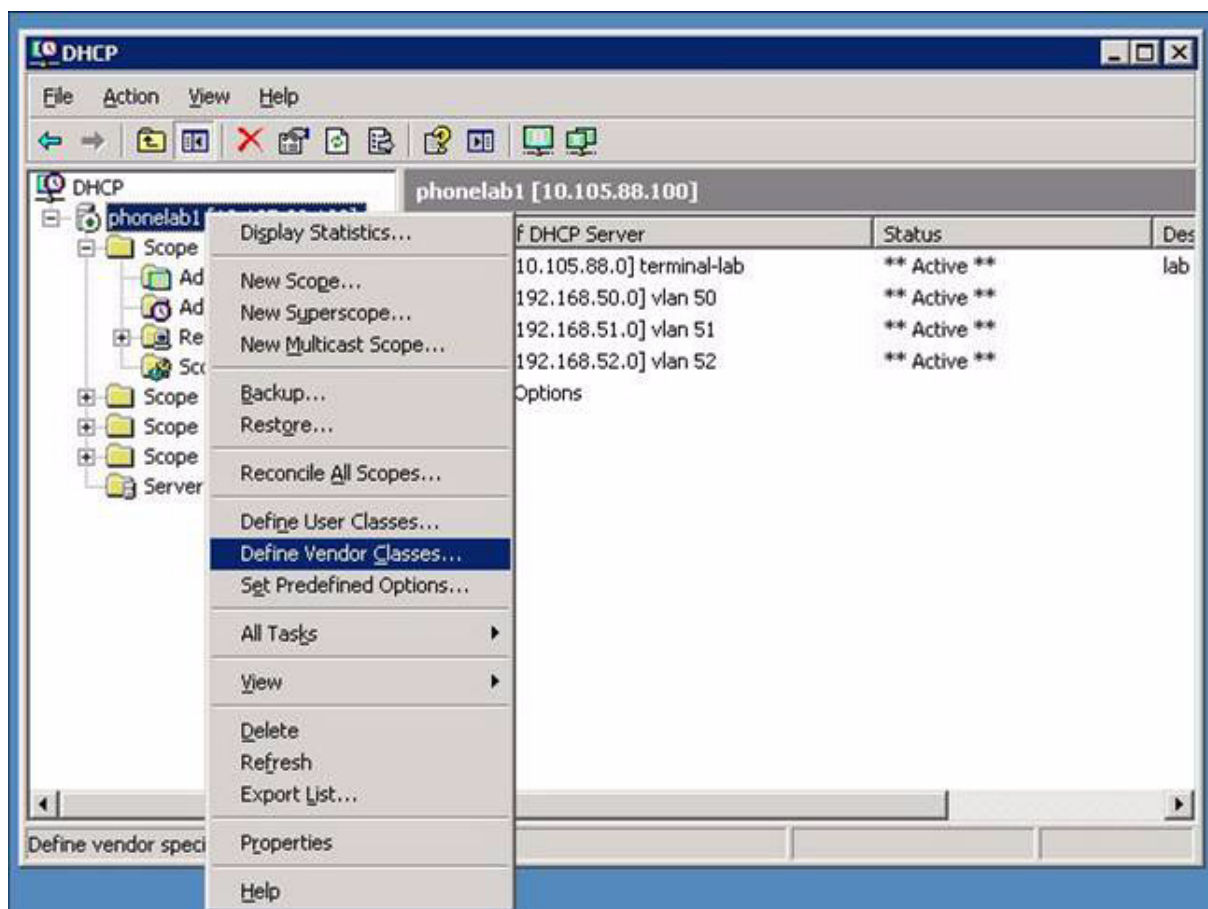


Figure 9: Define Vendor Classes

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

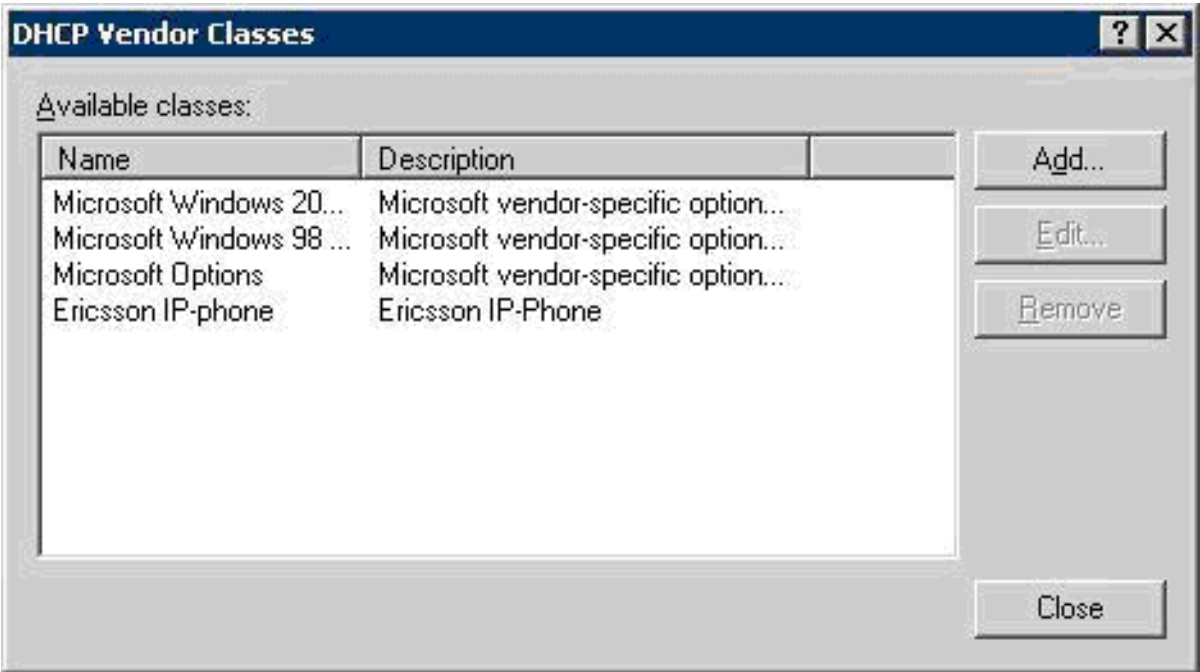


Figure 10: DHCP Vendor Classes

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:

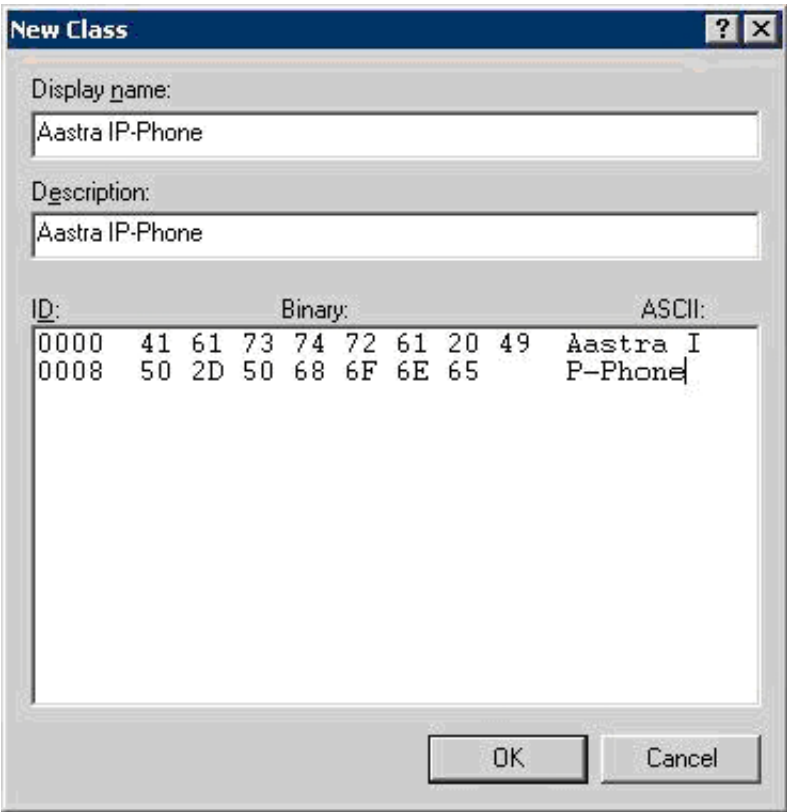


Figure 11: Add Vendor Class

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 7.8.3.2 Vendor Specific Information Field on page 16.

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.

7.8.4.2

Set Predefined Options

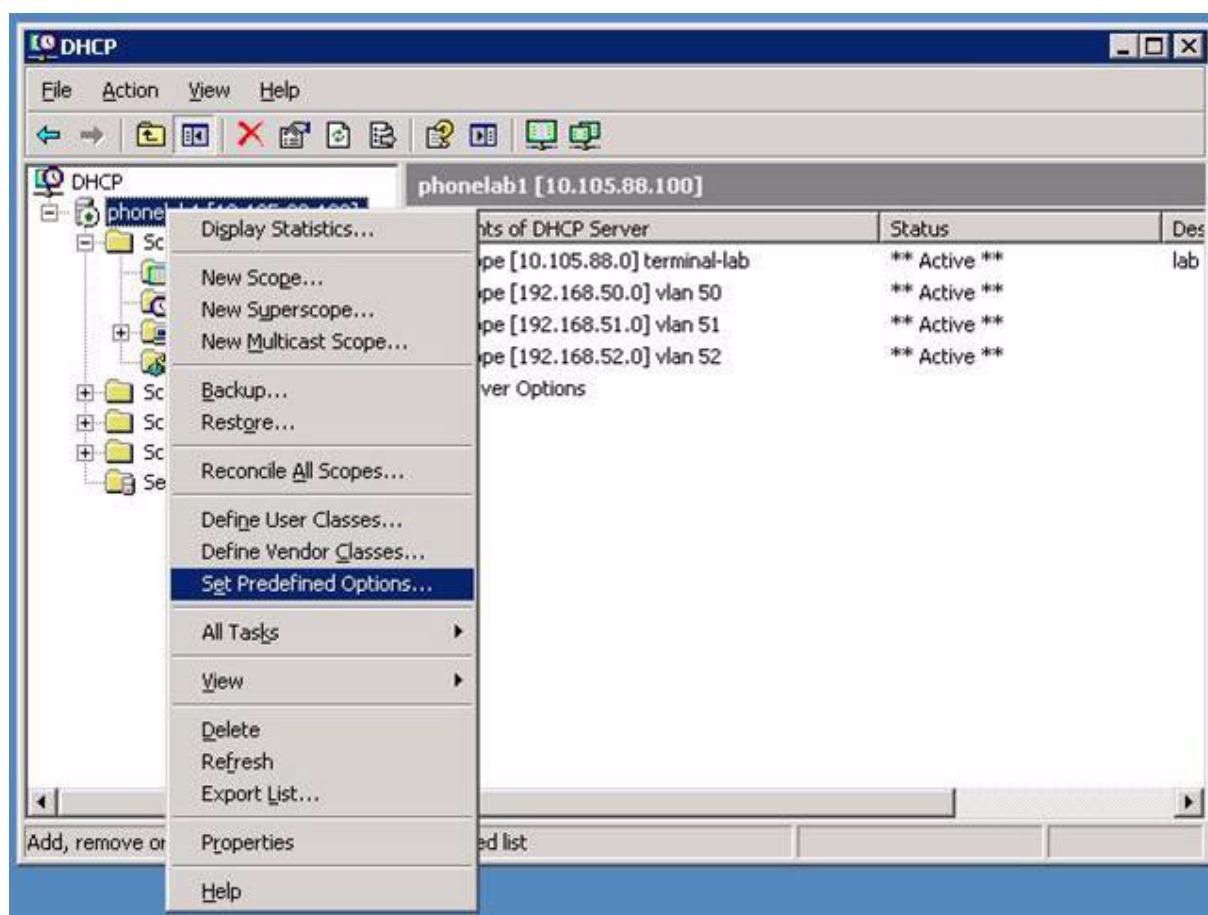


Figure 12: Set Predefined Options

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

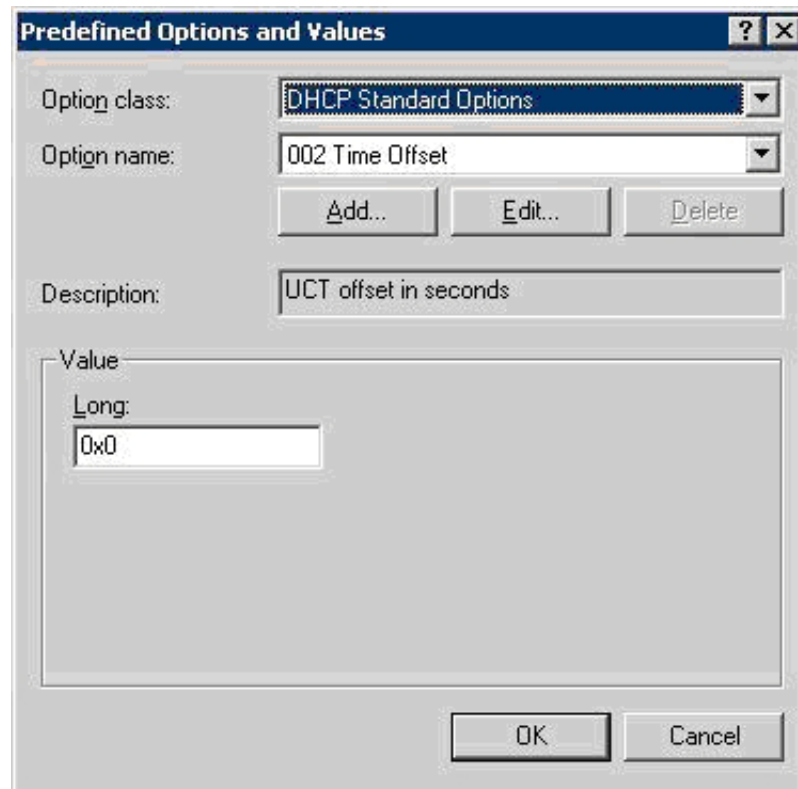


Figure 13: Predefined Options and Values

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:

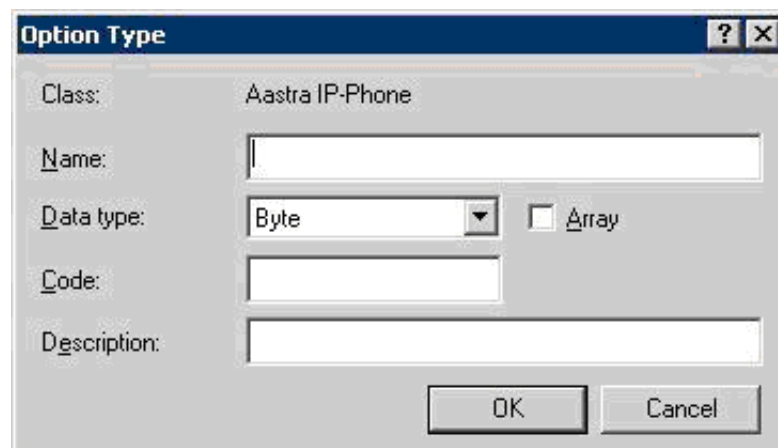


Figure 14: Option Type

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:



Figure 15: 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.

7.8.4.3

Set Scope Options

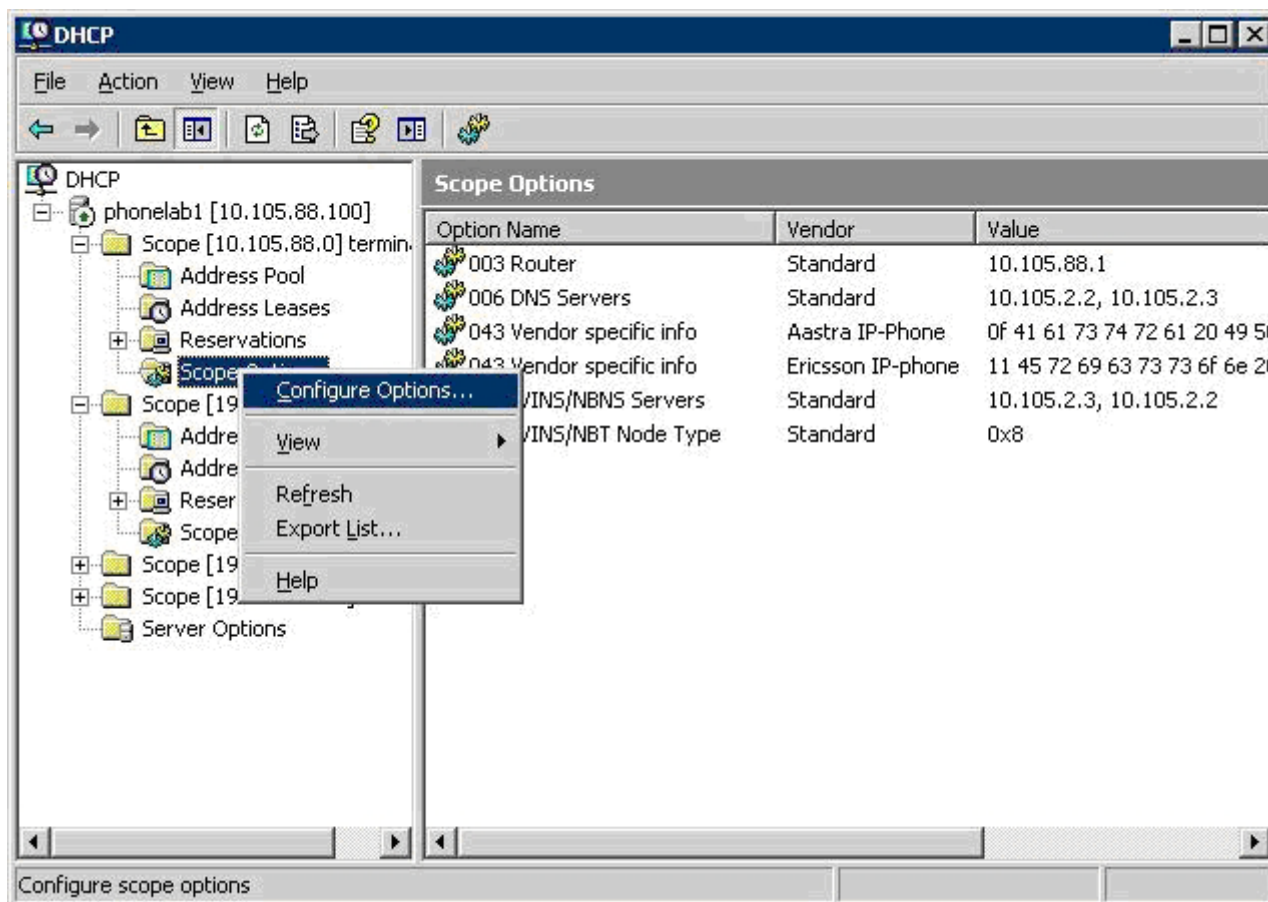


Figure 16: Configure Options

Select *Configure Options*.

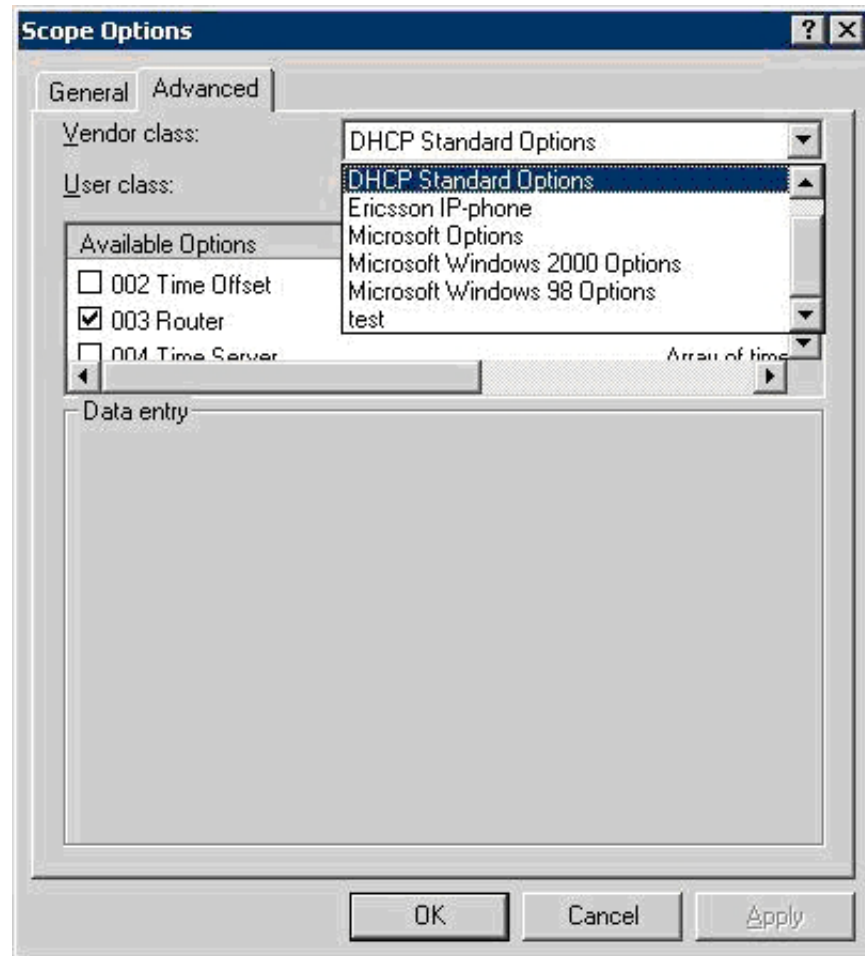


Figure 17: Scope Options

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 7.8.3.2 Vendor Specific Information Field on page 16.

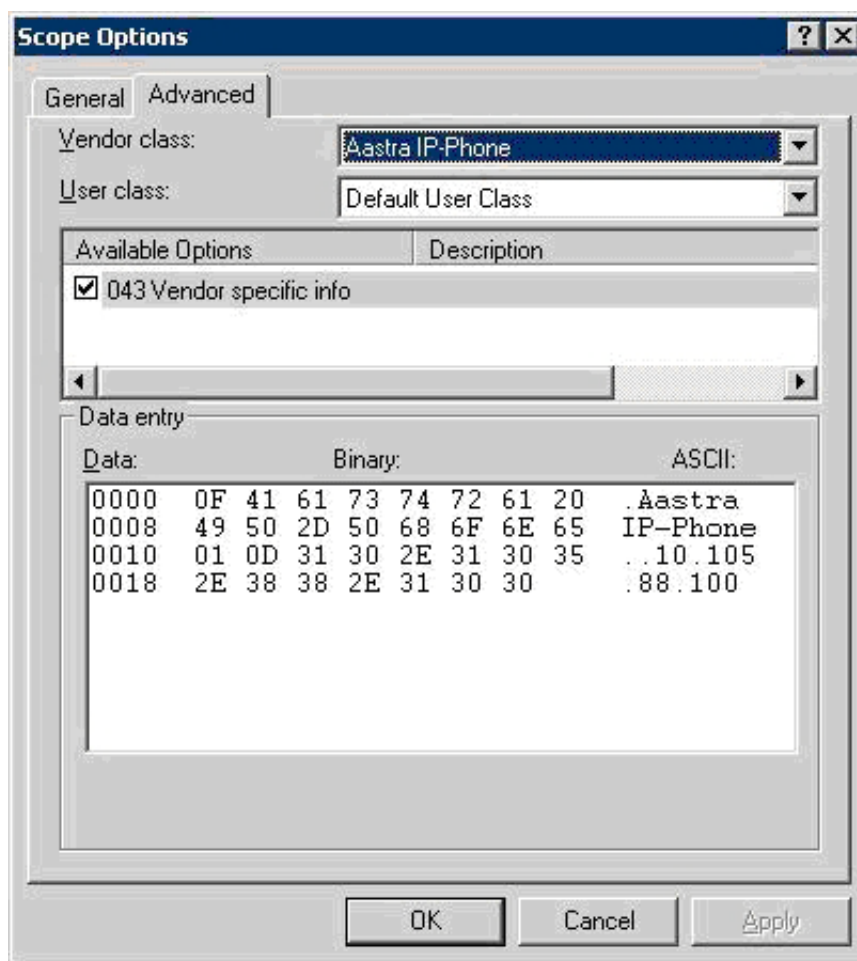


Figure 18: Windows® 2003 server DHCP settings

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 (10.105.88.102). If more tags than tag 01 for the SW-server is needed, add the additional tags according to the figure in section 7.8.3.2 Vendor Specific Information Field on page 16.

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

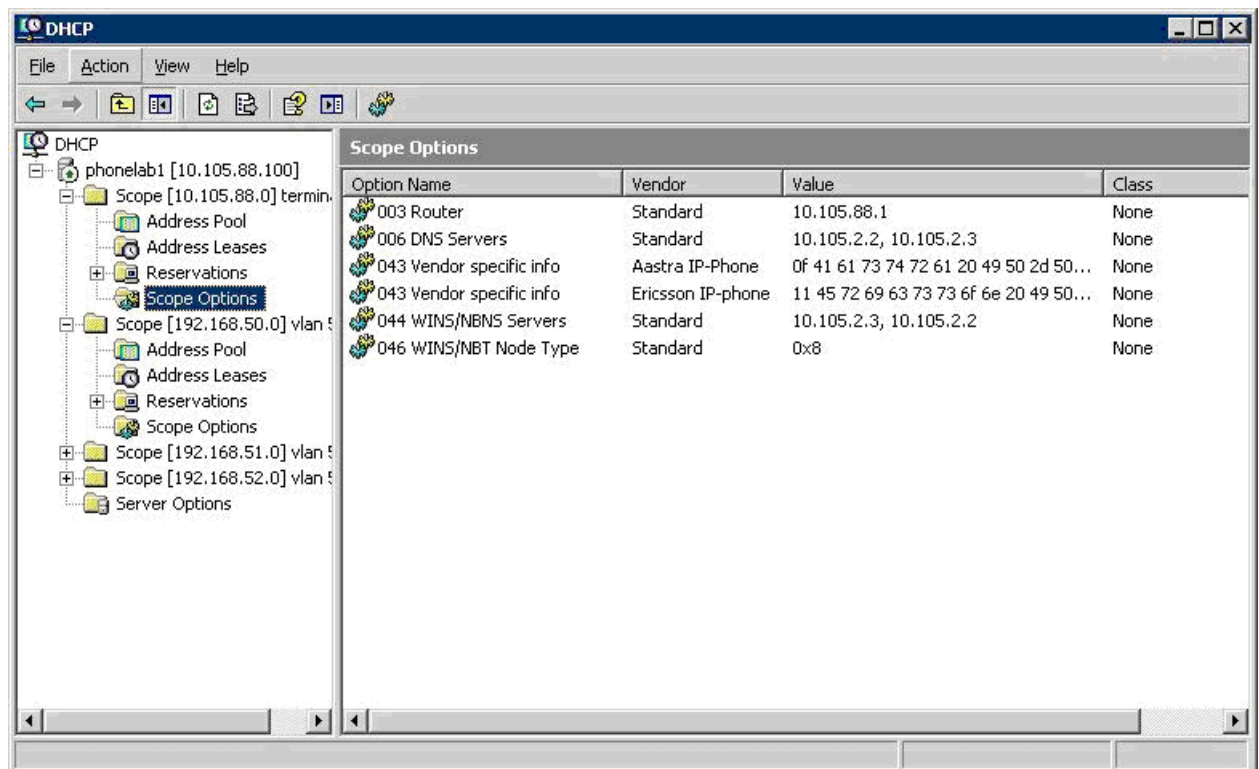


Figure 19: Two Initiated Vendor Classes

7.8.5

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.

7.9

DIFFSERV

Diffserv is a model for handling of priority, based on the type of service (TOS) field in the IP packet heading. For the definition of Diffserv see Figure 20 Diffserv octet on page 26

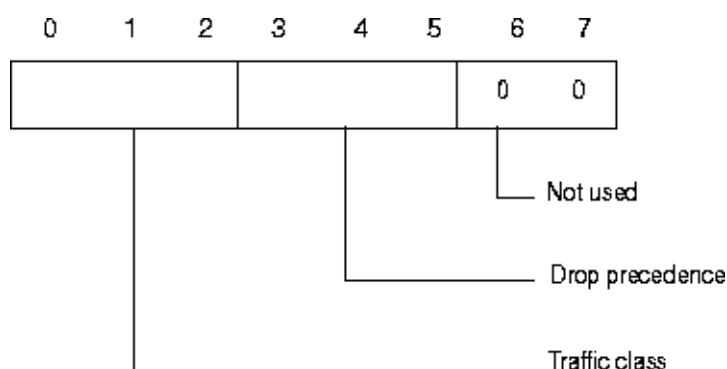


Figure 20: Diffserv octet

The default value for *voice packets* is Expedited Forwarding (EF) which is 101110 (bit 0-5).

The default value for the *signaling packets* is for Traffic class = Class B and Drop precedence = Medium drop precedence (010100 bit 0-5).

It is possible to change the values for Diffserv in the phone via the configuration file, see the description for *CONFIGURATION FILE FOR DBC 42X*.

7.10

FINDING OUT THE IP ADDRESS OF THE PHONE

The DBC 420 02 phone does not have a display. In order to set and read parameters in the phone, it is necessary to use the Web interface. The following methods to find the IP address exist:

- 1) IP Phone Administrator, see 7.11 IP Phone Administrator on page 29.
- 2) Use a port scanning program, see 7.10.1 Example of scanning on page 27. To improve the received information the DBC 42x 02 phones have a built in SNMP (Simple Network Management Protocol) agent which returns the equipment type, FW revisions and MAC-address. It is possible to scan without SNMP but in that case the MAC address will not be returned when scanning another subnet. The SNMP agent is disabled by default.
- 3) Look in the DHCP lease records, see 7.10.2 DHCP lease records on page 29.

7.10.1

EXAMPLE OF SCANNING

The scanning program in the example is a freeware program available on the Web. See <http://www.softperfect.com>

The scanning program must be set up, it is recommended to:

1. scan on port 1720 (used for H.225 signaling)
2. set the number of retries >1. If only one ping is sent there is a risk for no hit and the phone is not shown in the printout.

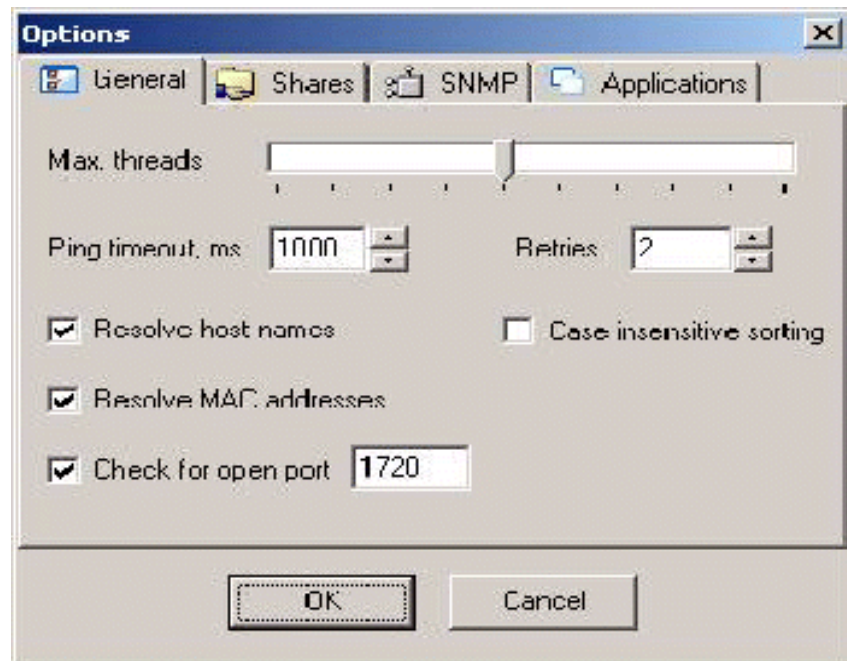


Figure 21: General configuration of port scanning program

The SNMP folder must also be set up, it is important to use exactly the same MIB (Management Information Base) OID (Object Identifier) as in the example below. The OID must be set to the address: 1.3.6.1.2.1.1.1.0 to return the required data.

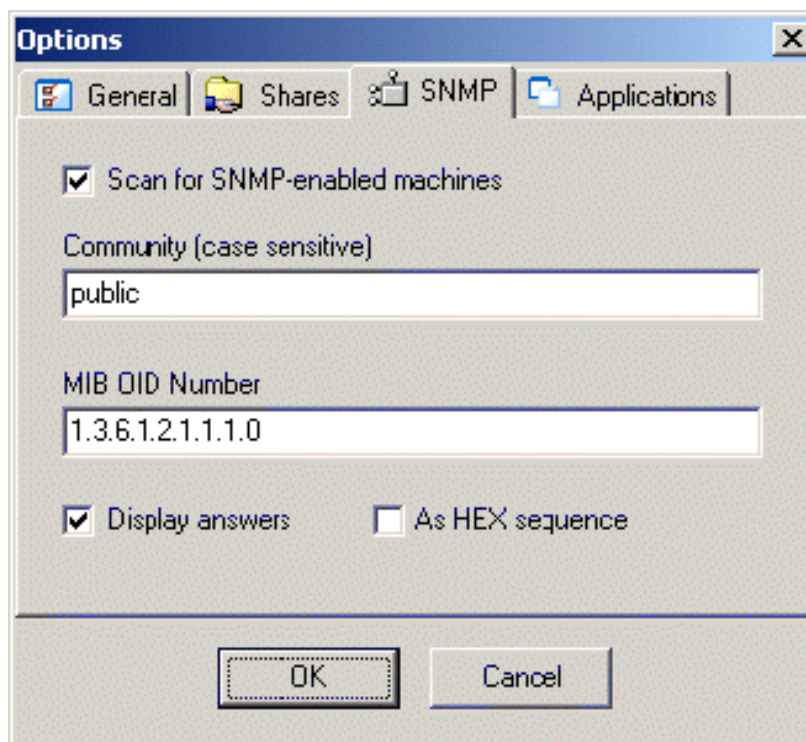


Figure 22: SNMP configuration of port scanning program

The Community field must also be set; this text string is used as a password. If the string is equal to the corresponding parameter set in the configuration file, the telephone responds with the requested information.

The results of the scanning is shown below. In this example the PC that executes the scanning program is located on another subnet than the scanned phones. Therefore there are no values in the MAC address column.

The address 130.100.26.183 and 130.100.26.184 are two terminals that answer with a system description string in column SNMP.

First part, Equipment: gives the type of terminal. Valid values are DBC 420 02 and DBC 422 02. **Second part**, HW/Appl/Boot version: gives the HW revision of the phone and FW revisions of the application and boot files. **Third part**, MAC, gives the MAC address of the phone. This value should correspond to the number printed on the label under the phone.

The addresses 130.100.26.182 and 130.100.26.187 are two terminals without SNMP agents, in this case a DBC 422 01 and a DBC 425 01.

	Host Name	MAC Address	Response Time	Port	SNMP
126.180	E-419D7D7C08764		3 ms		
126.189			9 ms		
126.191			10 ms		
126.183			11 ms	1720: Open	Equipment: DBC42202 HW/App/Boot versions: P1A/P1A4/P1A4 M/
126.184			13 ms	1720: Open	Equipment: DBC42202 HW/App/Boot versions: P1A/P1A4/P1A4 M/
126.187			15 ms	1720: Open	
126.182			16 ms	1720: Open	
126.190			15 ms		

Figure 23: Result of port scanning

7.10.2

DHCP LEASE RECORDS

Another method to find the IP address for the phone is to look in the DHCP lease records. Look for the IP address corresponding to the MAC address for a certain phone.

7.11

IP PHONE ADMINISTRATOR

The tool *IP Phone Administrator* is used to monitor the DBC 42x 02 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 firmware version in both registered and not registered IP phones

IP Phone Administrator exists as a stand alone application (product number CXC 109 0050), 7.11.2 Installation of the IP Phone Administrator server on page 32. It also exists as a task in MX-ONE Service Node Manager.

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, is registered or not registered toward the PABX.

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 / disable the sending of these http messages from the phone with a parameter in the configuration file, see description of *CONFIGURATION FILE FOR DBC 42X*.

The phones gets the IP address to the IP Phone Administrator server by DNS SRV resource records or via the configuration file, see description of *CONFIGURATION FILE FOR DBC 42X*.

Below is an example of a printout from the IP Phone Administrator:

IP Phone Administrator





<u>IP Address</u>	<u>User</u>	<u>Extension</u>	<u>Status</u>	<u>MAC Address</u>	<u>Model</u>	<u>HW Rev</u>	<u>Boot Rev</u>	<u>Applic Rev</u>	<u>Last Report</u>
130.100.169.63	F KJEBON	57157		00:13:5e:0b:19:e7	DBC42002 R2A	P2A9	P2A8t1		2/10/06 3:35:02 PM
130.100.168.113	K Renström	57627		00:01:ec:fb:c8:9f	DBC42202 P1A	P2A9	P2A8t1		2/10/06 3:32:51 PM
130.100.168.196		56602		00:01:ec:fb:cf:ae	DBC42002 P1A	P2A9	P2A8t1		2/10/06 3:17:05 PM
130.100.168.165		56601		00:01:ec:fb:cf:bc	DBC42002 P1A	P2A9	P2A8t1		2/10/06 3:10:27

Figure 24: 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 PABX, 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 PABX, 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 PABX.

- Green icon: the phone is registered.
- Grey icon: no log on attempt towards the PABX 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 bootROM firmware in the phone.

Applic rev

Revision of the application firmware 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.

7.11.1

INSTALLATION OF DBC 420 USING IP PHONE ADMINISTRATOR

When a new DBC 420 phone shall be installed, there are a couple of options for getting the phone into operation.

Scenario 1:

1. The IP address to the IP Phone Administrator server is retrieved from the DNS SRV resource record, see 7.7 DNS SRV Resource Records on page 14.
2. Use IP Phone Administrator tool to get the IP address to the phone. Click on the IP address and the administrator web interface is opened automatically.
3. Log on to the phone administrator web interface and set the requested data, see 7.29.1 Set data at installation of the phone on page 40.

Scenario 2:

1. The IP address to the software server is retrieved in one of the following ways:
 - from the DNS SRV resource record, see 7.7 DNS SRV Resource Records on page 14
 - from the vendor specific information field (43) in the DHCP messages, see 7.8.3.2 Vendor Specific Information Field on page 16.
2. At start up, the phone reads the configuration file with the IP address to the *IP Phone Administrator* server.

3. Use IP Phone Administrator tool to get the IP address to the phone. Click on the IP address and the administrator web interface is opened automatically.
4. Log in the phone administrator web interface and set the requested data, see 7.29.1 Set data at installation of the phone on page 40.

7.11.2

INSTALLATION OF THE IP PHONE ADMINISTRATOR SERVER

This tool can be downloaded from the Service Support Plaza. The files are stored on an Apache Tomcat server. The installation is described in the read me file for the IP Phone Administrator tool.

7.12

GATEKEEPER ADDRESS

The IP address of the gatekeeper can be defined either in the configuration file or via the Web interface. To change these settings from the Web, administrator page must be used.

The IP address of the gatekeeper can be set by any of the following methods:

- 1) Automatic gatekeeper discovery. This is the method to get the IP address automatically, see 7.13 Automatic Gatekeeper Discovery on page 33 . The gatekeeper and the LAN (enabled for multicast) must support this method. Verify that in the Web interface the Settings Network Gatekeeper discovery is set to Yes or *Auto Yes* .
- 2) In the configuration file. Primary gatekeeper can be defined, see the description for *CONFIGURATION FILE FOR DBC 42X*. Verify that in the Web interface Gatekeeper discovery is set to **Auto** and the parameter gatekeeper discovery is set to *No* in the configuration file.
- 3) In the configuration file. Secondary gatekeeper can be defined, which will be used when the primary fails, see the description for *CONFIGURATION FILE FOR DBC 42X* . Verify that in the Web interface Gatekeeper discovery is set to *Auto* and the parameter gatekeeper discovery is set to *No* in the configuration file.
- 4) Manually entered. Use the Web interface and the **Network** page. Verify that Gatekeeper discovery is set to **No**. Enter the IP address of the gatekeeper and press **Save**.
- 5) Backup gatekeeper: the IP address of the backup gatekeeper is defined in the configuration file, see 7.31 Backup Gatekeeper for Branch Offices on page 42.

The table below shows which method that will be used depending on the settings in the menu in the web interface and in the configuration file. The digits refer to the list above.

Table 1

Settings in menu in the web interface	BackupGK Yes	BackupGK 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

Settings in menu in the web interface	BackupGK Yes	BackupGK No	Settings in the configuration file
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

7.13 AUTOMATIC GATEKEEPER DISCOVERY

It is only some of the gatekeepers that have support for Automatic gatekeeper discovery.

Automatic gatekeeper discovery is a method to find a gatekeeper (PABX) 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 see 7.8.2 Data from DHCP on page 147 or from the configuration file, see the description for *CONFIGURATION FILE FOR DBC 42X*. 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 will be registered is defined in the configuration file. See data identifier **GatekeeperID** in the description for *CONFIGURATION FILE FOR DBC 42X*.

To use automatic gatekeeper discovery or not can be defined in the configuration file and via the Web interface. By default the phone uses the value defined in the configuration file.

7.14 HLR REDUNDANCY

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

For details see *INSTALLATION INSTRUCTIONS FOR DBC 425*, section HLR redundancy.

7.15 DOMAIN NAME

The domain name is used:

- 1) In the function Automatic gatekeeper discovery to find a PABX to register to, see 7.13 Automatic Gatekeeper Discovery on page 33 .
- 2) When several configuration files are to be used, see 7.5 Several Configuration Files on page 9 . This domain name cannot be defined in the configuration file.

- 3) In the registration request message when the gatekeeper is ASB 501 04 or MX-ONE.

7.16 SELECTION OF TRANSPORT ADDRESS (PORT NUMBERS)

For a description of the port numbers used for signaling and media in the phone, see installations instructions for *DBC 425*.

7.17 BUILT-IN ETHERNET SWITCH

DBC 420 02 has 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.

7.18 VIRTUAL LAN (VLAN)

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

The following possibilities to assign VLAN identities exist:

- From **DHCP** in option 43 (only the LAN port, but not the PC port). A list of maximum three VLAN identities can be handled, see Figure 8 Vendor Specific Information Structure on page 16.
- From the **configuration file** (both the LAN- and the PC port).

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 42X*.

Note: For DBC 42x 02: The VLAN tagged packets received by the phone must be 68 bytes at the minimum.

7.18.1 AUTOMATIC VLAN DETECTION WITH DHCP

Prerequisites on the LAN

When the phone is connected to a layer 2 switch, the switch will add the IEEE 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 will be assigned to.

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

At installation (and hardware reboot) 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.

Reboot

At warm reboot (the power is not disconnected), the phone will continue to use the previously used VLAN identity.

For DBC 42x 02 phones: At cold reboot (disconnect/connect the power) the phone will continue to use the previously used VLAN identity.

For DBC 42x 01 phones (ARM platform): At cold reboot (disconnect/connect the power), the complete automatic VLAN discovery procedure will start from the beginning. For these phones, the power must be disconnected for at least one minute to achieve a cold reboot.

To change the VLAN identity (for DBC42x 02):

After power up the phone starts and when there is a timeout in the DHCP negotiation; phone will start a complete automatic VLAN discovery procedure from the beginning.

Note: This procedure can take several minutes.

To be able to change the VLAN identity automatically the phone must fail to get contact with the DHCP server in the previously used VLAN, otherwise the previous VLAN identity will still be used. The alternative is to manually edit the VLAN identity.

7.18.2

ASSIGNING THE VLAN IDENTITY VIA THE CONFIGURATION FILE

The description of how to set the parameters, see the description for *CONFIGURATION FILE FOR DBC 42X*.

The configuration file is read from the native LAN

At installation (and hardware reboot) 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 reboot is done automatically in the phone 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 hardware reboot) and the configuration file is available in the VLAN but not in the native LAN, the VLAN identity must be set manually in the boot menu.

This is not possible in DBC 420 02, which means that the option to read the configuration file from the VLAN is not possible.

7.18.3

MANUAL SETTING OF THE VLAN IDENTITY

It is not possible to set the VLAN identity manually in the DBC 420 02.

7.19

SECURITY

The phone has support for protection of VoIP signaling with TLS and media encryption with SRTP. For a description of the security feature, see installation instructions for *DBC 425* section SECURITY.

7.20

LAN ACCESS CONTROL (ACCORDING TO IEEE802.1X)

DBC 420 02 cannot have this feature.

7.21

ACCESS THE PHONE FROM A PC

For maintenance of the terminal, the system administrator can access the phone, from a PC, in one of the following ways:

- Web interface. This interface is recommended.
- Telnet. This interface can be used by experts. Telnet is available in the application CAA 158 0043 up to revision R4A.
- SSH (Secure Shell). SSH is available in the application CAA 158 0043 R4A or later. This interface is similar to the Telnet interface, but the connection is secure.

In the maintenance PC, a SSH client must be used. There are a number of free-ware clients, the most popular is PuTTY for PCs with Windows®.

The default encryption keys are used and not possible to change.

For a description of these interfaces, see maintenance instructions for *IP TELEPHONE DBC 42X*. For the password handling, see 7.22.1 Password for maintenance on page 37 .

The IP address must be known to be able to log on to the phone, see 7.10 Finding out the IP Address of the Phone on page 26.

The end-user can also access the phone via the web interface. Depending on that it is not possible from the phone to read out the IP address needed for Web access, it is recommended that the administrator performs all necessary management, or passes the IP address of the phone to the end user. The end-user web interface is described in the documents for respective system:

For ASB 501 04 see directions for use for *DBC 420*.

For MX-ONE see directions for use for *DBC 420 FOR MX-ONE*.

For the password handling, see 7.22.2 Web interface password for the end user on page 37.

7.22

PASSWORDS

There are different passwords used in the phone:

- 1) to register the phone to the gatekeeper, see 7.1.1 Start a phone in a LAN with a DHCP server on page 7
- 2) for maintenance via Telnet / SSH or the web interface, to be used by the network administrator or other maintenance personnel, see 7.22.1 Password for maintenance on page 37
- 3) for the end user when handling of data in the phone, via the web interface, see 7.22.2 Web interface password for the end user on page 37.
- 4) LAN access control authentication, see 7.20 LAN Access Control (According to IEEE802.1x) on page 36.

7.22.1

PASSWORD FOR MAINTENANCE

A network administrator can log on from a PC to an IP phone via Telnet / SSH. It is also possible to access the phone from a web browser via the web interface. It is the same password for Telnet, SSH and web browser access. The default password is **Telephone**. This password can be changed by using the following procedure:

1. Log in to one IP phone via Telnet / SSH. VxWorks login: admin Password: For more information about the functions when using Telnet, see maintenance instructions for *IP TELEPHONE DBC 42X*.
2. Enter the command **encryptPasswd "new wanted password"** (quotation mark must be used). The password must have at least eight characters.
3. Write the generated encrypted password with the data identifier **AdminPassword** in the configuration file, see the description for *CONFIGURATION FILE FOR DBC 42X*.
Store the updated configuration file on the SW server.
4. Next time the IP phones read the updated configuration file the new password is valid.

7.22.2

WEB INTERFACE PASSWORD FOR THE END USER

The end user can use the web-browser in the PC to access the web interface in the IP phone. The purpose is to set data in the phone like Dial-by-Function keys, hearing level etc.

The password to the end-user web interface is the same as the password or PIN to register the phone to the gatekeeper.

The web interface is described in the DBC 420 user guides and directions for use:

For ASB 501 04, see directions for use for *DBC 420*.

For MX-ONE, see directions for use for *DBC 420 FOR MX-ONE*.

7.23

SOFTWARE VERSION

It is possible to check the software versions in the phone from the IP Phone Administrator tool, see 7.11 IP Phone Administrator on page 29.

It is also possible to check the software versions by using the administrator web interface. The program revisions are shown under **Settings, Show phone configuration**. The HW revision of the phone, the FW revisions of the application and boot are listed.

7.24

RESTART AND REBOOT OF THE PHONE

If it is necessary to restart or reboot the phone manually, press the keys **C** (clear key) **mute** and **#** simultaneously for one or two seconds.

It is also possible to restart the phone from the administrator web interface, see maintenance instructions for *IP TELEPHONE DBC 42X*. Select **Network** and **Apply all settings**.

After a power failure or a reboot, the phone will log on automatically with the stored directory number.

7.25

ADMINISTRATOR MODE

The administrator mode is used to monitor the start up sequence.

To enter the administrator mode, press the keys **C** (clear key), ***** and **5** simultaneously for one or two seconds when the phone is starting and after the **Status LED** has started flashing. This must be done within 5 seconds. In administrator mode the status of the phone during start-up will be indicated by LEDs and the only possible change of the configuration is to switch off DHCP, see 7.1.3 Using a fixed IP address on page 8.

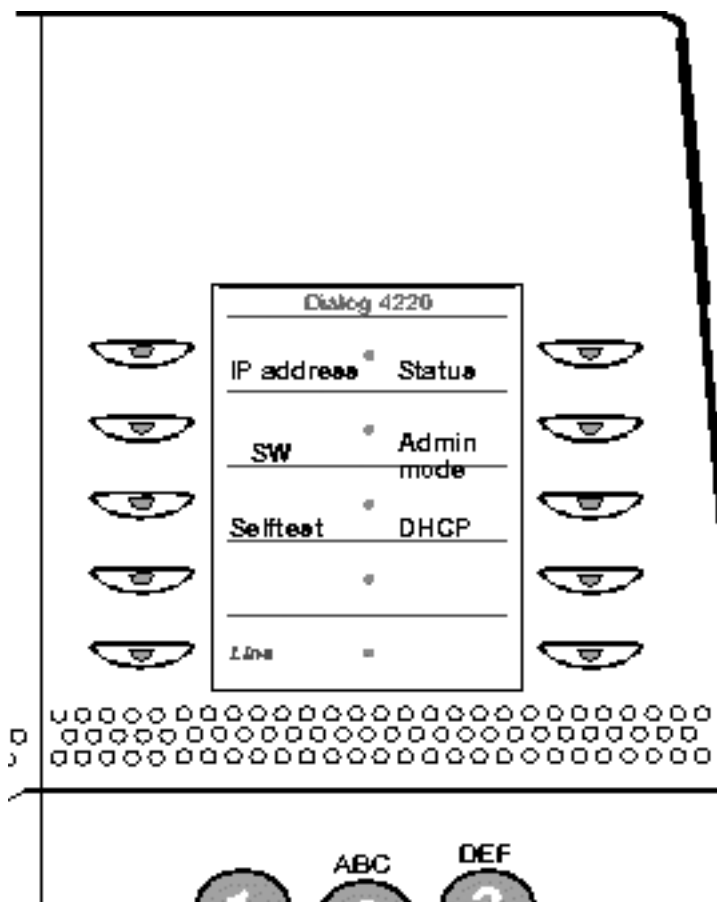


Figure 25: Key layout of DBC 420 02 in administrator mode

IP address

Flashing: when the phone is contacting the DHCP server to get an IP address

Lit: the phone has received the IP address.

SW

Flashing: when the phone is communicating with the SW server.

Lit (for a short while): the correct SW is loaded into the phone memory (either from internal Flash memory or from the SW server, if a software upgrade has been done).

Selftest

This LED is lit for one second if the internal self test is OK.

Status

Double flashing (with the LED cadence 1 second off, 50 ms lit, 50 ms off, 50 ms lit, repetitive): no connection to the LAN.

Flashing (with the LED cadence 300 ms lit, 300 ms off, repetitive): the phone is not registered.

Lit: the phone is registered and it is possible to make and receive calls.

Not lit: no power to the phone.

This LED is also used when the phone is in normal mode (not in administrator mode).

Admin mode

Indicates that the phone is in administrator mode.

DHCP

Indicates that IP addresses are being received from a DHCP server.

Lit: The phone will use DHCP. This is the normal case.

Not lit: The phone will use the default IP address, see 7.1.3 Using a fixed IP address on page 8

7.26

QUALITY OF SERVICE (QOS)

It is possible to view the quality of service statistics of the connection for the last 10 calls. The statistics shows for example the delay, jitter and number of lost packets. See maintenance instructions for *IP TELEPHONE DBC 42X*.

7.27

LANGUAGE HANDLING

Not applicable.

7.28

TIME AND DATE SETTING

The following options exist to set the time and date in the IP phone:

- Via WAP messages. If the gatekeeper has WAP support (as ASB 501 04, MX-ONE, MD-E and BusinessPhone have), the time in the IP phone can be updated automatically as soon as the phone is registered towards the gatekeeper.

- SNTP (Simple Network Time Protocol). If the gatekeeper does not have WAP support, if different time zones shall be used, the time in the phone can be set via SNTP. For details see below.

7.28.1

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 the description for *CONFIGURATION FILE FOR DBC 42X*.

If the LAN does not have SNTP or NTP available, a server with SNTP software has to be initiated. For Windows NT/2000, there is for example, a shareware application called Tardis.

7.28.2

MANUALLY SETTING OF THE TIME AND DATE

Not applicable.

7.29

TO CHANGE THE CONFIGURATION OF THE PHONE

7.29.1

SET DATA AT INSTALLATION OF THE PHONE

The IP address of the phone can be found as described above, see 7.10 Finding out the IP Address of the Phone on page 26.

Log in to the administrator web interface of the phone.

1. Select the **Log off restriction** page. Enter the directory number and password or PIN for this phone, press **Change**.
2. The phone will try to register to the gatekeeper automatically. If this IP address shall be set manually, select the **Network** page.
 - If the IP address of the gatekeeper is to be set manually: Change **Gatekeeper discovery** to **No**. Enter the IP address of the gatekeeper, press **Save**.
 - If the IP address of the software server is to be set manually: Change **Software Server from DHCP** to **No**. Enter the IP address of the SW-server, press **Save**. Press **Apply all settings**. The phone will reboot.

The directory number can be printed on the designation card by using the Designation Card Manager tool. The Designation Card Manager is included on the CD Enterprise Telephone Toolbox. It can also be downloaded from <http://www.mitel.com>. With this tool the directory number of the phone can be written on the top of the label, replacing the text MiVoice 4420 IP Basic.

7.29.2

LOG ON / LOG OFF OPTIONS

The phone is always logged on with a default number. The default number must have an associated password or PIN to avoid logging off by mistake from an other terminal.

The log on procedures are described in the directions for use for respective system:

For ASB 501 04, see directions for use for *DBC 420*.

For MX-ONE, see directions for use for *DBC 420 FOR MX-ONE*.

If the default number is to be **changed**, there is only one possibility:

- Use the administrator web interface.

7.29.3

ALLOCATION OF FUNCTION KEYS

Most of the functions allocated to the function keys can be moved or removed, except the Line key(s) that are fixed. If the default allocation will be changed, the system administrator has to modify the configuration file, see the description for *CONFIGURATION FILE FOR DBC 42X*.

To enable storing the Dial-by-function key (TNS) numbers in the PABX, see 7.34 Dial-by-function Keys on page 44.

In the case when the TNS number is stored in the PABX; to avoid future problems with TNS, MNS keys and other function associated with keys (call back, transfer etc.), see the description for *CONFIGURATION FILE FOR DBC 42X* section FUNCTION KEYS.

When the phone is used with ASB 501 04 or MX-ONE there are no spare function keys available, if the default configuration is used. To make it possible to initiate TNS or MNS numbers the function on at least one of the function keys must first be removed, see the description for *CONFIGURATION FILE FOR DBC 42X* section FUNCTION KEYS.

7.29.4

CHANGE IP SETTINGS

It is only possible to use the web interface to change the IP settings.

7.29.5

CHANGE GATEKEEPER DISCOVERY IN NETWORK SETTINGS

Gatekeeper discovery is the method to automatically get the IP address of the gatekeeper to use. If this method is not used the IP address of the gatekeeper has to be set in the configuration file or manually via the Web interface.

For further information, see 7.12 Gatekeeper Address on page 32.

7.30

UPDATE OF THE IP PHONE SOFTWARE

This section describes the procedure when a new version of the software is to be loaded in the IP phones. DBC 420 02 will fetch the new version of the software from the SW server, when the phone receives a specific command from the gatekeeper or when the phone is restarted. The procedure is:

1. 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 in the same way as a Service Advice:
 - If there are no new parameters in the configuration file: Update the existing configuration file with the new firmware 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, see 7.6.3 Directory structure on page 11.
2. Store the new bootROM and application software on the SW server, see 7.6.3 Directory structure on page 11.

3. Perform the update of the phones according to the method for the current system. For ASB 501 04 see operational directions for *IP EXTENSION*.
4. The phones that are registered in the gatekeeper, can be ordered by a command from the gatekeeper, to load the new software.
5. For the phones that are not registered in the gatekeeper the following is valid: The gatekeeper does not know the IP address to these phones:
 - the phones will once every 24:th hour fetch the configuration file from the SW-server to check if new firmware shall be loaded.
 - the IP Phone Administrator tool can be used to get a list of these phones, see 7.11 IP Phone Administrator on page 29 . 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 reboot and update the software.
6. To start the update process manually from an IP phone, press the keys **C** (clear key), **mute** and **#** simultaneously for a second to restart the phone. The update process may take about one minute.
7. 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.
8. Verify that the right version of the software has been loaded by using a print command in the gatekeeper or see 7.23 Software Version on page 37.

7.31

BACKUP GATEKEEPER FOR BRANCH OFFICES

In a branch office scenario where the IP phones in the branch office are connected to the PABX 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 PABX in the main office.

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

1. Define in the configuration file, used by the phones in the branch office, the type and the IP address of the backup gatekeeper, see the description for *CONFIGURATION FILE FOR DBC 42X*.
2. 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 up to 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 the data identifier **RRQTtl** in the description for *CONFIGURATION FILE FOR DBC 42X*.
3. The frequency of the routine for discovering when the main office connection is working again is also defined by the data identifier **RRQTtl**, see the description for *CONFIGURATION FILE FOR DBC 42X*. When the main office connection is working, the phone will be registered to the main office gatekeeper.

7.32

EMERGENCY CALL

There are two cases of emergency calls:

- 1) From an IP phone which is not logged. See below.
- 2) From an IP phone which is logged on. 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 ASB 501 04 see operational directions for *EMERGENCY CALLS, SOS CALLS*.

An IP phone which is not logged on

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 the description for *CONFIGURATION FILE FOR DBC 42X*.

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 7.5 Several Configuration Files on page 9.

When the emergency call function is enabled in the configuration file, the emergency number must be known by the user. When the user lifts the handset the dial tone is heard although the phone is not logged in. 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 defined in the configuration file is sent. The 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 it is possible to use. But it is very important that the emergency number is set up in the PABX 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 PABX operator assistant.

7.33

MONITORING KEY (MNS KEY)

It is possible to monitor other extensions from programmable function keys on the IP phone. This function is also called MNS (Multiple represented directory number with dial-by-function key) and is often used in Boss-Secretary applications.

The Monitoring keys are initiated in the PABX. The only changes that can be done by the end-user is the changing of the type of ring signal for the Monitoring key. Parameters that can be changed in the configuration file are the delay time before the ring signal is generated for the Monitoring keys and MNS ring signal level when phone is busy, see the description for *CONFIGURATION FILE FOR DBC 42X*.

Note: The software version in the exchange must support this function.

7.34

DIAL-BY-FUNCTION KEYS

The numbers assigned to the Dial-by-function keys can be stored in the PABX (if the software version of the exchange has this function). This makes it possible for the end-user to bring the numbers when logging on to different phones. To enable this storing of the numbers in the PABX, the parameter **EnablePBXStoring** must be set in the configuration file, see the description for *CONFIGURATION FILE FOR DBC 42X*.

Note: When the PABX is upgraded from a software version that cannot store the Dial-by-function key data to a software that has this function, the data of the keys will be lost the first time the phone is logged on.

7.35

OPERATOR MEDIA DEVICE (OMD)

This phone type cannot be used as an OMD phone (PABX operator solution based on IP for MX-ONE).

7.36

WALL MOUNTING OF THE IP PHONE

The phone can be wall mounted, useful for instance in conference rooms or in public areas. Use the wall mounting kit SXX 106 2049/1, which consists of the spacer SXX 112 4753/1 and two screws.

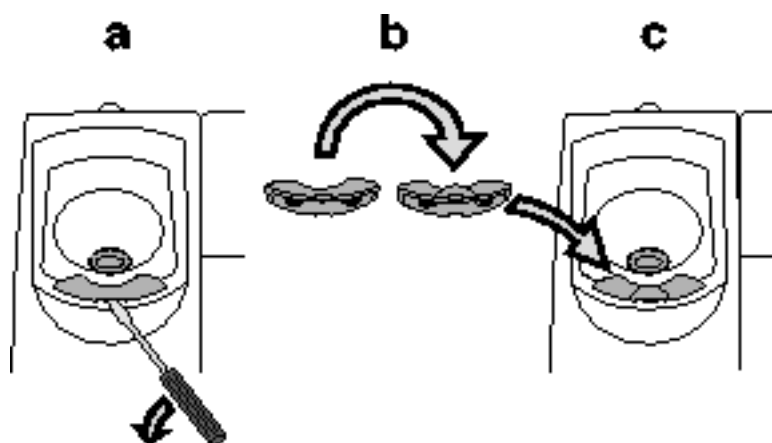


Figure 26:

- Use a screwdriver to remove the handset hook.
- Turn the hook upside down and put it back.

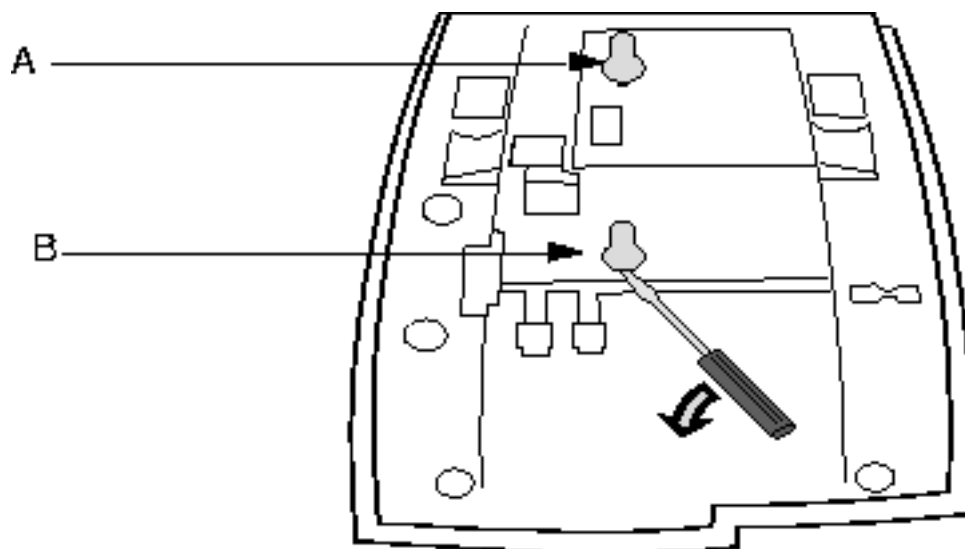
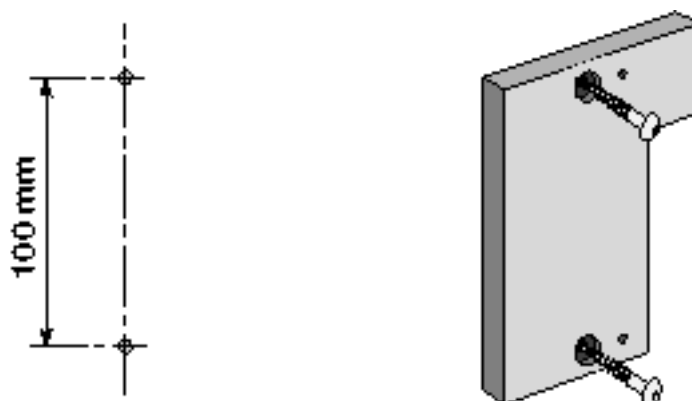


Figure 27:

- Use a screwdriver to remove the two (A and B) plastic covers
- Drill two wall holes and mount the spacer SXA 112 4753/1 on the wall.



**Hole dimensions depending on type of wall.
Wall screws are not supported (\varnothing max. 5 mm).**

Figure 28:

- Fasten supplied screws to the spacer.

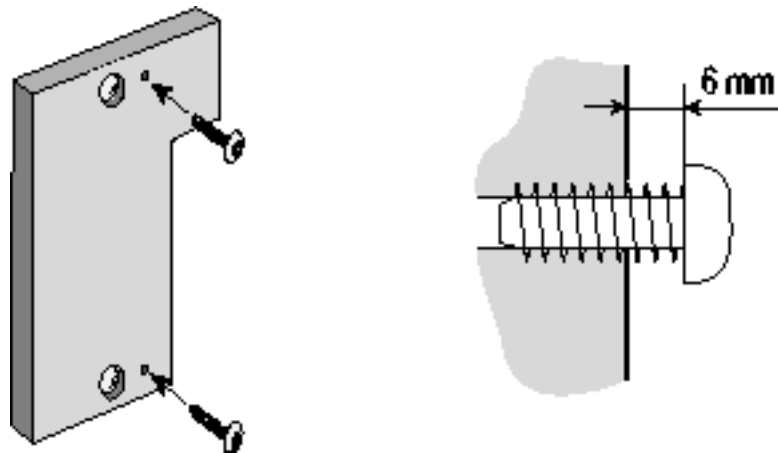


Figure 29:

- Hook the phone on the spacer screws

Measures for a locally manufactured spacer

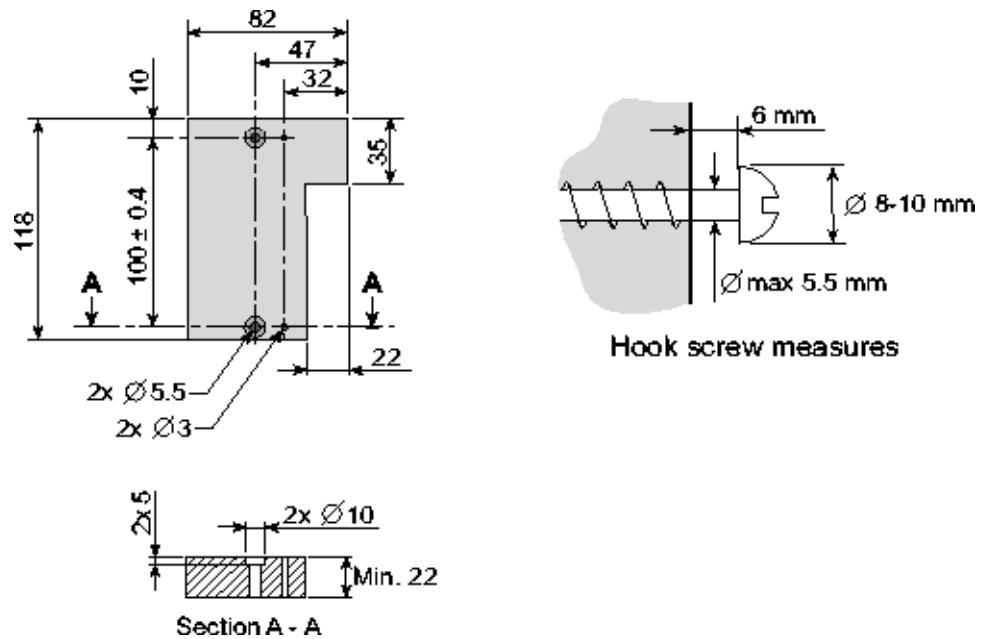


Figure 30:

7.37

POST INSTALLATION MEASURES

Check that it is possible to log on the phone to the system.

Verify that internal and external calls can be established from and to the phone.