Configuration File for DBC 42X

DESCRIPTION

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.

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 CONFIGURATION FILE IN A MX-ONE SERVICE NODE ENVIRONMENT

When the IP telephones are used in an environment with MX-ONE 3.0 or later, the **MX-ONE Service Node Manager** should be used when creating or changing the configuration file for the IP telephones.

The descriptions in this document of the parameters in the configuration file is replaced by the on-line help texts in **MX-ONE Service Node Manager.**

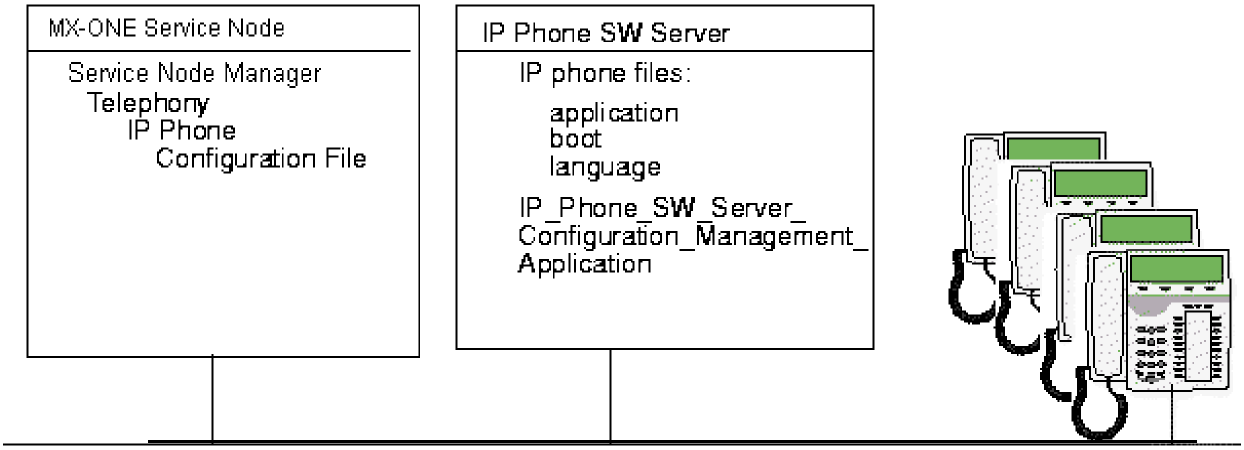


Figure 1: The deployment of Service Node Manager, IP Phone Configuration File

1.1 CREATE A CONFIGURATION FILE - NEW INSTALLATION

The procedure at new installation is:

- Installation of IP Phone SW Server.
- Create a configure file for DBC 42X.

The software to be used in the IP phone software server can be downloaded from the Service Support Plaza. The software consists of two parts:

- IP phone files: application, boot and language file.
- IP Phone SW Server Wizard. This package includes also the Tomcat web server.

1.1.1 INSTALLATION OF IP PHONE SW SERVER

See the IP Phone SW Server installation instruction in document *IP PHONE SOFTWARE SERVER.*

1.1.2 REGISTER AN IP PHONE SW SERVER

Do as follows:

1. Create the **dbc42x02** directory under the web-server root: **jakarta-tomcat-4.1.31\webapps\ROOT** on the IP Phone SW server (where -4.1.31 is an example).
2. Copy the IP phone files to the **dbc42x02** directory: application, boot, and language files.
3. Log in to **MX-ONE Service Node Manager (SNM)**. The welcome page is displayed.
4. Select **Telephony**, **IP Phone** and then **SW Server**. The page **IP Phone SW Server** is displayed.
5. Click **Add**. The page **IP Phone SW Server - Add** is displayed.
6. Register the I**P Phone SW Server;** type information in the fields **Server name**, **IP Address** and **Port Number**.
7. Click **Apply**. If the operation went well, you will get the information, **Add operation successful for: XX (XX= name of the server)**.

1.1.3 CREATE A CONFIGURE FILE

Do as follows:

1. Select **Telephony**, **IP Phone** and then **Configuration file** on **Welcome page** in **SNM**. The page **IP Phone Configuration file** is displayed.
2. Click **Add**, to open a new configuration file. The **IP Phone Cofiguration File - Add step 1/10** is displayed.
3. Type configuration data in the 10 steps. If you need help, use the **SNM online** help, to the right.
4. Click **Apply** to finish the steps and configuration, and to store data under the correct directory in the **IP Phone Software Server**.

To force the telephones to fetch the new configuration file there are a number of cases:

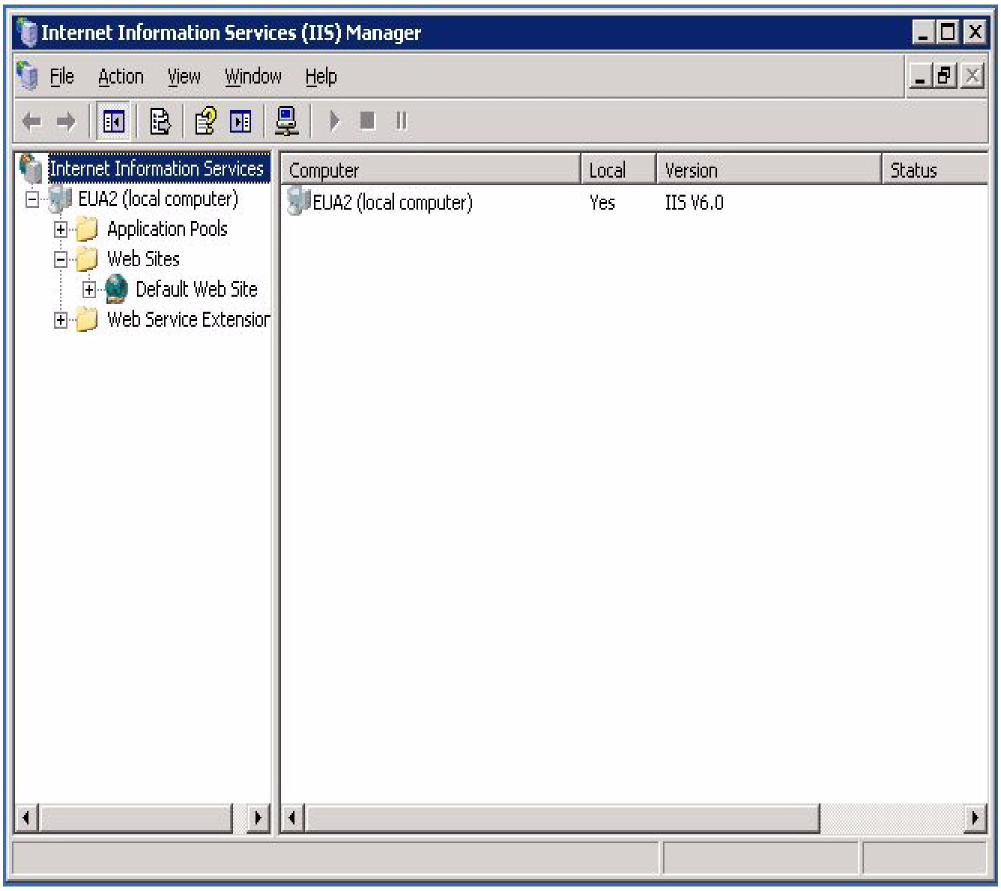
- If the telephones are not started yet: connect the power and the telephones will fetch the new configuration file.
- If the telephones are already registered to the PBX, select the **Unregistration** option to force the telephones to fetch the new configuration file.
- If the telephones are started but not registered to the PBX:
  - use the task IP Phone Administrator (in Service Node Manager) to log on to the telephones and initiate re-boot from the administrator web interface.
  - the telephones will after less than 24 hours automatically fetch the new configuration file and if necessary download a new firmware.
  - re-boot the telephones manually.

1.1.4 PORT CONFLICT

The **IP Phone SW Server Configuration Management Application** runs on a Windows server that often is used also by other applications and their own web servers. If a Windows IIS web server exists there can be a problem with a conflict between the ports for the web servers since both the Tomcat and IIS should use port 80. The IP phones must use port 80 for fetching the firmware files.

Measures to avoid port conflict

- Deploy IIS and run it on port 80
- Deploy IP Phone Configuration Management Application with Tomcat and run it on port 82
- Connect SNM to *IP Phone SW Server Configuration Management Application* on port 82.
- Set up the folder structure required by the terminals in Tomcat and copy application and language files into it. But not the configuration file. Example:
C:\jakarta-tomcat-4.1.31\webapps\ROOT\d42x02\d42x02-applic_R1A.dat
C:\jakarta-tomcat-4.1.31\webapps\ROOT\d42x02\d42x02-boot_R1A.dat
C:\jakarta-tomcat-4.1.31\webapps\ROOT\d42x02\d42x02-lang_R1A.txt
- Create the configuration file in SNM and store it in IP Phone Configuration Management Application
- Redirect IIS to tomcat for the terminal requests like this:
  - Open C:\WINDOWS\system32\inetsrv\inetmgr.exe, navigate to Default Web Site



Computer	Local	Version	Status
EUA2 (local computer)	Yes	IIS V6.0	

  - Right click on Default Web Site and select New Virtual Directory. A wizard will start
  - Enter the directory name to where the telephone firmware shall be stored as Alias, example: d42x02

- Enter the path to the family n folder under Tomcat, example: C:\jakarta-tomcat-4.1.31\webapps\ROOT\d42x02\d42x02-applic_R1A.dat
- Enable the Read option and finish the wizard
- You can now access the Tomcat folder with terminal settings on both port 80 as well as 82, while SNM can update the configuration file on port 82
- If subnets or telephony domains are defined for the configuration file in SNM, the path under Tomcat will include the subnet/telephony domain in its path. Update the IIS virtual directory link accordingly

2 CONFIGURATION FILE HANDLING FOR OTHER SYSTEMS

When the IP telephones are used with all other exchanges than MX-ONE3 (or later) this section is applicable.

This description of the configuration file is valid for the following IP telephones:

- DBC 420 02 (MiVoice 4420)
- DBC 422 02 (MiVoice 4422 version 2)
- DBC 425 02 (MiVoice 4425 version 2)

If a parameter is only valid for a certain telephone, the telephone type is written together with the description of the parameter.

The DBC 42x 02 telephones use the H.323 protocol.

The IP telephones use a configuration file to initiate parameters in the telephone. Examples of parameters that are possible to set in the configuration file are:

- which system the IP telephone shall register towards
- the version of the software to be used
- priority of the codecs
- assignment of function keys

The file shall be stored on a software server (web server) and the IP telephone uses the http protocol (with port number 80) to read the file. The other software files to be loaded into the IP telephone shall also be stored on the same software server.

The IP address to the software server can either be distributed to the IP telephones from the DHCP server, from DNS SRV resource records or entered manually into the IP telephone.

The name of the configuration file must be:

- **d42x02-config.txt** for DBC 420 02, DBC 422 02 and DBC 425 02 (product number CAA 158 00 42)

If the telephone detects a fault in the configuration file when it is read, this is indicated in the display by initiating the self test mode by pressing the keys **C** , ***** and **4** simultaneously for at least one second.

The configuration file can be adapted or changed by the system administrator with any editor.

2.1 REFERENCES

For more information about the software server and about the directory structure where to store the configuration file:

- see installation instructions for *DBC 420*
- see installation instructions for *DBC 422* and DBC 425

3 DESCRIPTION

3.1 SYNTAX

The configuration file contains five different types of data:

- *Headers*, are used to create different groups of data identifiers: e.g. [System], [Software], [Language], [WAP] etc.
- *Data identifier*, is a reserved word which ends with an equal-sign: e.g. System=.
- *Dataless identifier,* is an identifier without data and is not followed by an equal-sign: e.g. G.729A.
- *Data*, is the value after the equal-sign until the end of the line: e.g. MX-ONE.
- *Comment*, a line starting with a semi-colon and the text until end of the line: e.g. ; Default language is English.

If a data identifier is enabled, the corresponding header must also be enabled. The following example shows a combination that is **not allowed**:

; [STOREPHONEBOOK]

EnableStoring=YES

3.2 SYSTEM

3.2.1 H.323

The header [System] has the following data identifiers:

- **System**. Which system (gatekeeper) the telephone shall register toward. The allowed values are:
  - **MX-ONE**. To be used with MX-ONE Service Node. The identifier gives the following features:

    – Function keys for line1, line2, inquiry, transfer, message, follow me, call back and free on 2:nd line. For more information, see 3.16 Function keys on page 18.

    – Uses Q.931 overlap sending, if overlap is set to **YES**.

    – WAP signaling and this enables the use of soft-keys.

    – Time is set via the WAP signaling or via an NTP server.
  - **MD110, TSW, BP, BP-R16, MD-E**. Were earlier supported values, but are out of scope of this document.
  - **System data identifier omitted**. Has the following features:

    – Line1 key

    – At off hook, **setup** is sent to the gatekeeper and the digits are sent according to Q.931 (if overlap sending is used).

    – Local dial tone is generated at off hook.

- **OverLap**. How the entered digits are sent to the gatekeeper, with allowed values:
  - **YES**. The entered digits are sent one by one to the gatekeeper. The default value.
  - **NO**. All entered digits are sent in a block to the gatekeeper and the call is initiated by pressing the call key.
- **AutodialTimeout.** 1-20 seconds. The default time is 5 seconds. The time before the telephone sends the entered number to the PBX. The timeout is only valid in en-block sending (OverLap=NO). If no timeout is wanted, disable the parameter as a comment.
- **RRQTtl**. *Registration Request Time to live* is used to check if the connection between the IP telephone and the gatekeeper is up. This parameter defines the length of the interval between time to live re-registrations in seconds. The parameter values can be:
  - The default value is 600 i.e. 10 minutes
  - The minimum value is 40 seconds.
  - **OFF**: *Registration Request Time to live* is not sent.
  - 0 (zero): the default time will be used and the time to live field will not be included in Registration Request message.

  The RRQTtl parameter is only used when the time to live value is not received (in the RCF message) from the gatekeeper.

  The parameter is also used in the branch office scenario, to discover when the telephone shall register towards the backup gatekeeper and also to discover when the main site is up again and the telephone shall register towards the main site.
- **GatekeeperDiscovery**. Gatekeeper discovery is a method to find a gatekeeper, to which the IP telephone should register. This data identifier has two possible values:
  - **YES**. Automatic gatekeeper discovery will be used by default, but it can be disabled in the settings menu on the IP telephone
  - **NO**. Automatic gatekeeper discovery will not be used unless gatekeeper discovery is set to yes in the menu of the IP telephone.

  If the **GatekeeperDiscovery**data identifier is omitted, the default value **YES** will be used.
- **GatekeeperID**. This is the gatekeeper identity of the PABX that the IP telephone should be registered to. This is used in the gatekeeper discovery procedure to find out which of the gatekeepers the IP telephone should register to, see also operational directions for *IP EXTENSION*. It is possible to use wild cards, example: LIM* accepts all gatekeeper identities that begin with LIM.
- **Domain**. This is the domain name of the LAN to which the IP telephone is connected and it is used for **Gatekeeper discovery** and for **Load distribution**, see also operational directions for *IP EXTENSION, IP*. This identifier is a text string. This domain name is a text string and only used when a domain name is not received from the DHCP server.

  If the **Domain** identifier is omitted in the configuration file and is not received from the DHCP server, no domain name will be used by the IP telephone.

- **PrimaryGKAddress.** This is the IP address to the primary gatekeeper, which will be used only if the **GatekeeperDiscovery** identifier is set to **NO** and gatekeeper discovery is set to the value default in the menu of the IP telephone. If this identifier is omitted and **GatekeeperDiscovery** is set to **NO** the IP telephone will use the manually set address in the **Settings menu** in the display.
- **SecondaryGKAddress.** This is the IP address to the secondary gatekeeper, which will be used if the primary fails. This identifier should only be used if **PrimaryGKAddress** is also used. Primary and secondary gatekeeper must be the same **system**, see heading [System].
- **AdminPassword.** This identifier is used to set the **Administrator password** which is used in telnet/SSH and in the built-in web server. The password must be in encrypted form, this is done in telnet/SSH by calling the function **enctryptPasswd** with the desired password as argument. The administrator user name is admin, and the name is fixed.
- **LogOffRestriction**. This parameter does not affect DBC 420. When all the telephones shall have the same log off restriction option, this parameter can be used. When this parameter is used in the configuration file, *it is not possible to change this parameter locally in the telephone*. The values are:

  – **LogOffAllowed**. The end-user is allowed to log on and log off the terminal. Se also parameter LogOffTime below.

  – **DefaultNumberUsed**. The telephones are always logged on with a default number.

  – **PermitIndividualLogOn**. The telephones are always logged on with their default number, but the end-user can log on with his/her individual number.

  For more information see installation instructions for *DBC 422* and *DBC 425*.
- **LogOffTime=hh:mm.** where hh mean hours and mm minutes. When this parameter is enabled all the users will be logged off at the specified time. This parameter is only used when *LogOffRestriction=LogOffAllowed*. The default value is that this parameter is disabled.

3.3 SOFTWARE

The header [Software] has the following data identifiers:

- **BootFile**. The path and file name for the bootrom. The path must be according to the description in the installation instructions, 2.1 References on page 7.
- **BootVersion**. The version of the bootrom software.
- **ApplicationFile**. The path and file name for the application. The path must be according to the description in the installation instructions, 2.1 References on page 7.
- **ApplicationVersion**. The version of the application software

These identifiers can be repeated for different hardware versions e.g. R1*, R2*, R3* etc in the same configuration file.

If **ApplicationVersion** in the config file is not equal to the revision in the application software, shown in the display by pressing **C** , ***** and **4**, the application file is always fetched from the web server. Example: if the **ApplicationVersion** is R2G and the revision shown in the display in the telephone is R2F, the file with the application R2G will always be fetched.

3.4 802.1X

The header [802.1x] is used to setup the parameters for LAN access control according to IEEE802.1x. This function is only valid for DBC 422 02 and DBC 425 02.

Enabled data identifiers in the configuration file override the values in the telephone.

The following identifiers exist:

- **LANAccessControl:** To enable or disable the IEEE802.1x function:
  - **Auto**: The telephone will initiate IEEE802.1x signaling in the boot sequence and if the LAN supports IEEE802.1x, the telephone enables this function. The default value is **Auto**.
  - **No**. The telephone disables the IEEE802.1x function.
- **StoreUserIDPassword: YES / NO**. If the user identity and the password shall be stored in the telephone or not. The default value is **YES**.
- **UserType**. Indicates if the user identity and password shall be valid for the telephone or for the end user.
  - **User**: The telephone will be logged off from the LAN when the end-user registers with a different extension number towards the PABX. The end user has to enter the LAN access control user identity and password each time he/she registers with a different extension number.
  - **Phone**: The telephone will not be disconnected from the LAN when entering a different extension number to register towards the PABX. The default value is **Phone**.
- **UserIdentity**: The user identity is loaded into the telephone from the configuration file.
- **UserPassword**: The user password is loaded into the telephone from the configuration file.

The UserIdentity and UserPassword identifiers are used in the case when all the telephones shall have the same user identity and password. This is a convenient option compared to enter this from the key pad, especially if many telephones shall be installed. The recommendation is to use a configuration file with the UserIdentity / UserPassword activated at installation and then remove these identifiers once the telephones are installed.

3.5 ABSENCE SERVICES

(Only DBC 425 0x). This is a group of procedures to be sent to the gatekeeper when absence services is used. Each procedure is a combination of digits, * and #. [Absence] is the header used for setting up these procedures. The identifiers are:

- **Profile** = code for activating a profile, code for deactivating profile. Example: *10*profileNo#,#10#. Only the digits can be changed.
- **FollowMe** = code for activating follow me, code for deactivating follow me.
- **ExtFollowMe** = code for activating external follow me, code for deactivating external follow me.
- **AbsenceReason** = code for activating absence reasons, code for deactivating absence reason. Example: *23*reasonCode#,#23#.

The format of reasonCode is name of *reason=reason number*hhmm*, where hh is hours, mm minutes when a time is used, mmdd are used for dates where mm is month and dd is day.

The star (*) between reason number and the time shall not be used in BusinessPhone.

If any of the codes for the AbsenceReason are within the comments (;) in the config file, it will not be displayed on the telephone. The total number of possible absence reasons are according to the list, but maximum 10 reasons can be used in a site:

- **Lunch**
- **GoneHome**
- **OfficialMatter**
- **Meeting**
- **Trip**
- **Illness**
- **FreeTime**
- **Course**
- **Busy**
- **Absent**
- **Special**
- **ParentalLeave**
- **DayOff**
- **Vacation**

For MX-ONE: The date format must correspond to PARNUM=62 in the ASPAC command.

For DBC 425 02: It is possible to change the Absence reason text string shown in the display by editing the language file, see the description for *LANGUAGE FILE FOR DBC 42X 02*.

3.6 AUTHORIZATION

The header [Authorization] is used to replace the digits with a dash (-) in the display for password codes and similar. The same identifier is used for all codes:

- **Code** = the code to replace. Example syntax: *funcCode*pinCode*telNo.#, **-** means not visible, **n** means visible. Example: *75*-*n# is entered in the configuration file, the end-user enters *75*123456*67609# on the keypad and the display will show *75*------*67609#.

3.7 AUTO NEGOTIATION

The header [AutoNeg] is used to setup speed and duplex mode for the LAN and PC port. The following identifiers are used:

- **AutoNegLANPort**: this identifier can be set to YES or NO. YES means that the port uses auto negotiation to decide speed and duplex. If the parameter is omitted, the default value is YES.
- **SpeedLANPort:** this identifier can be set to 10 Mbit/s or 100 Mbit/s. This identifier is only used when **AutoNegLANPort** is set to NO.
- **DuplexLANPort**: this identifier can be set to FULL or HALF. FULL means that the LAN port can receive and send at the same time. This identifier is only used when **AutoNegLANPort** is set to NO
- **AutoNegPCPort**: this identifier can be set to YES or NO. YES means that the port uses auto negotiation to decide speed and duplex. If the parameter is omitted, the default value is YES.
- **SpeedPCPort:** this identifier can be set to 10 Mbit/s or 100 Mbit/s. This identifier is only used when **AutoNegPCPort** is set to NO
- **DuplexPCPort**: this identifier can be set to FULL or HALF. FULL means that the LAN port can receive and send at the same time. This identifier is only used when **AutoNegPCPort** is set to NO

DuplexLANport and **DuplexPCPort** should only be set to **FULL** if the remote LAN port to which the IP telephone is physically connected to is manually set to full duplex.

Note: If a server or switch port is set to full duplex, but the other end is trying to make auto negotiation, there will be a half / full duplex mismatch.

If the [AutoNeg] header is omitted, auto negotiation will be used.

3.8 AUTOMATIC CHECK FOR NEW FIRMWARE

The telephone will read the configuration file every 24th hour to check for new firmware. For not registered telephone this check is always done and if new firmware is available it will be loaded. For registered telephones this check can be enabled via the configuration file and new firmware will be loaded. If the telephone is busy, the check will be performed if the telephone becomes idle before the delay time elapses, otherwise the check will be done at next scheduled time.

The header is [AutoResync] and following parameters can be used:

- **Time= hh:mm**: The time when the check shall be done.
- **MaxDelay=**: Value range 0-1439 minutes. The maximum time that the phone waits past the scheduled time before starting the check. The actual check will be done after a random time between the times stated in the **Time** parameter and the **MaxDelay** parameter.

The default value is that the automatic check is disabled.

3.9 BACKUP GATEKEEPER

The backup gatekeeper is a gatekeeper that will be used if **Gatekeeper discovery** fails or the primary and secondary gatekeeper fails, depending on configuration, see installation instructions for *DBC 420* and see installation instructions for *DBC 422* and *DBC 425*.

The header for backup gatekeeper is [BackupGK]. The identifiers are:

- **System:** the type of backup gatekeeper. Possible value: MX-ONE (earlier also BP, BP-R15, MD-E, MD110/TSW). The backup gatekeeper **system** does not have to be the same as the main site **system**.
- **IPAddress:** the IP address of the backup gatekeeper.

3.10 CODEC PRIORITY

The supported codecs and their priority are defined below the header [Codecs]. The following dataless identifiers can be used:

- G.711A
- G.711U
- G.729A
- G.729AB
- G.723

The identifiers must be written as a list with only one on each line and in priority order. The codecs that are not in the configuration file will not be used by the IP telephone. The default priority is as in the example above. G.711 µ-law is the American standard and G.711 A-law is the European.

3.11 DEBUG LEVELS

The header [DebugLevel] is used to change the debug level for all the telephones via the configuration file for fault locating reasons. The following parameters exist:

H323Debug
The events that occur in the H.323 module in the telephone.

UIDebug
The events that occur in the user interface module in the telephone.

RTPDebug
The events that occur in the voice (media stream module) in the telephone.

WAPDebug
The events that occur in the WAP module in the telephone. This module handles services and display messages.

WEBDebug
The events that occur in the web server module in the telephone.

The following parameter values exist:

0 = No printouts

1 = Error printouts

2 = Major events

3 = Minor events

4 = All printouts

3.12 DEFAULT PACKET SIZE

It is possible to change the default packet size for the RTP stream. The used packet size is negotiated with the other end-point. When the telephone is master, the telephone will select the parameter value defined for the identifiers below, as the preferred packet size.

A shorter packet size means less delay and lower risk for echo, but means on the other hand more overhead and more traffic on the network.

The header is [DefaultPacketSize]. The identifiers are:

- **DefaultMsPerPacket711**: The size of the packets in ms for the G.711 µ-law and A-law codecs. Possible values are: 10, 20, 30 ms. The default value is 30 ms. If DBC 42x 01 or DBC 413 01 telephones are used in the network the default value must be 30 ms to ensure speech connection.
- **DefaultMsPerPacket729**: The size of the packets in ms for the G.729A and G.729AB codecs. Possible values are: 10, 20, 30, 40, 50 and 60 ms. The default value is 30 ms. If DBC 42x 01 or DBC 413 01 telephones are used in the network the default value must be 30 ms to ensure speech connection.

3.13 DIFFSERV SETTINGS

Diffserv is a re-interpretation of the ToS (Type of service) field used to give priority to the IP datagrams. The Diffserv octet consists of the field DSCP (Differentiated Services Codepoint, bits 0 to 5) and Reserved (bits 6 and 7). The reserved field is always 0. The DSCP field consists of the fields Traffic class (bits 0, 1, 2) and Drop precedence (bits 3, 4, 5). Bit 0 is the leftmost bit.

The Traffic class field may take the values 0 (Best effort), 1 (Class A), 2 (Class B), 3 (Class C), 4 (Class D), 5 (Expedited forwarding) and inherited from ToS, 6 (Internet control) or 7 (Network control). Traffic class 6 and 7 should never be used in the IP telephone.

The Drop precedence field may take the values 1 (Low drop precedence, bit value 2), 2 (Medium drop precedence, bit value 4) or 3 (High drop precedence, bit value 6). Low drop precedence means that the corresponding packet has a higher probability of surviving router congestions. When Traffic class is set to Expedited forwarding the Drop precedence field will have the value 110 independent of which value has been set in the configuration file.

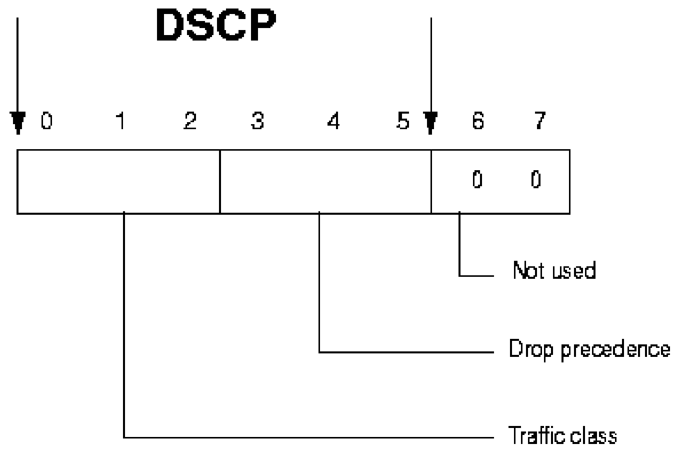


Figure 2: The Diffserv octet

The header [DIFFSERVUDP] is used to set the diffserv DSCP field in voice packets and in UDP signaling packets (RAS and WAP).

The header [DIFFSERVTCP] is used to set this field in TCP signaling packets.

These headers have two data identifiers used to set the Traffic class and the Drop precedence:

Traffic Class , this data identifier can be set to eight different values:

- 7 (Network Control bit 0-2: 111) Should not be used.
- 6 (Interned Control bit 0-2: 110) Should not be used.
- 5 (Expedited Forwarding bit 0-2: 101)
- 4 (Class D bit 0-2: 100)
- 3 (Class C bit 0-2: 011)
- 2 (Class B bit 0-2: 010)
- 1 (Class A bit 0-2: 001)
- 0 (Best Effort bit 0-2: 000)

Drop Precedence , this data identifier can be set to three different values:

- 3 (High Drop Precedence bit 3-5: 110)
- 2 (Medium Drop Precedence bit 3-5: 100)
- 1 (Low Drop Precedence bit 3-5: 010)

By default the setting is Expedited forwarding.

The default value for UDP is Expedited forwarding and the default value for TCP (H.225, H.245) packets is Class D and High drop precedence.

3.14 DISPLAY

The header [Display] is used to define how certain kinds of text or events shall be shown in the display. This parameter does not affect DBC 420. Possible data identifiers:

- **ShowDTMFDigits=**
  - **NO** The digits will not be shown in the display while pressing digit keys in a call.
  - **YES** The digits will be shown. Default value.
- **ShowIPSettings**=
  - **ENABLED** The IP settings (IP addresses, sub net mask, default gateway etc.) are shown in the display, which means that the end-user can see these settings by pressing **Settings** and **Network**. Default value.
  - **DISABLED** The IP settings are not shown in the display for the end-user. The IP settings are only shown if the administrator mode is entered in the telephone.
- **BacklightMNSIncoming.** Indication of calls on an MNS key (only for DBC42502).
  - **YES**. Independent of ring signal type for the MNS key, the display backlight is lit when there is a call on the MNS key. This is the default value.

  - **NO**. If type of ring signal is set to silence, the display backlight is **not** lit when there is a call on the MNS key.

- **BlinkOpuMNSIncoming.** When using an option unit OPU, it is possible to define when the extra bell or lamp shall be activated.
  - **YES**. The lamp or extra bell shall indicate incoming calls to the MNS keys. This is the default value.
  - **NO**. The lamp or extra bell shall not indicate incoming calls to the MNS keys.
- **MissedCallAtBusy.** When the user has disabled free on busy (he/she does not want to receive a second call while there is an ongoing call), it is possible to chose if the new call shall be visible as a missed call or not. The parameter values can be:
  - **YES**. Incoming calls while the terminal is busy shall be visible in the list with missed calls. This is the default value.
  - **NO**. Incoming calls while the terminal is busy shall **not** be visible in the list with missed calls.
- **MissedCallTimer = (0 - 1860 seconds).** Time in seconds before an incoming call in ringing state is regarded as a missed call.
  0 = the call is regarded as a missed call independent of the time in ringing state. This is the default value.
- **MissedCallTime**

- Default 0 (no timer). Time in seconds in ringing state before unanswered (incoming) calls are logged as missed.

3.15 EMERGENCY

(Only H.323). The header [Emergency] is used to set up the possibility to make emergency calls from an unregistered telephone. The following identifiers are used:

- **System1 =** the system of the emergency call server or gatekeeper. This identifier supports the same systems as the **System** data identifier belonging to the header **[SYSTEM]** see 3.2 System on page 8.
- **Address1 =** the IP address of the emergency call server or gatekeeper.
- **Port1 =** the call signaling port number of the emergency call server or gatekeeper.
- **System2** = the system of the secondary emergency call server or gatekeeper.
- **Address2** = the IP address to the secondary emergency call server or gatekeeper.
- **Port2** = the call signaling port to the secondary emergency call server.
- **EmergencyNr =** the emergency telephone number, maximum 7 digits, e.g.: EmergencyNr=112. This number can be combined with the **RouteAccessNumber** see 3.35 WAP on page 36 to make it possible to dial for example 112 and 00112.
- **A-Number =** the telephone number sent to the emergency centre and can be used for dial back by the emergency centre.
- **RouteId =** the identifier/password used by the emergency call server to identify the call from the telephone, maximum 15 ASCII characters (digits and letters).

- **NumberingPlanOfA-Number =** the type of numbering plan (according to Q.931) that is used for the A-number. Two values are allowed.
  - **ISDN**: This value is used when the emergency centre is in the public network. This is the default value.
  - **Private**: Private numbering plan is used for the A-number. This can be used for example when the emergency centre is inside the campus and the centre expects internal numbers.

3.16 FUNCTION KEYS

In this section the expressions TNS and MNS are used:

TNS - Telephony Name Selection. Phone numbers and function codes (e.g. *21#) can be assigned to TNS keys.

MNS - Phone number to a monitored extension.

The function keys on DBC 420, DBC 422, and DBC 425 can be assigned as function keys (e.g. call back), as TNS keys and as MNS keys. The assignments of some types of the function keys are made from the configuration file, see below.

The assignments of the following types of functions are made from the PBX:

- MNS
- TNS but can also be done from a menu in the phone, or via the web interface in the phone.
- Malicious Call Trace (MCT)
- Recording key to start the recording of a call
- Personal Number (PEN) key

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

System > Subsystem > create or change > Terminal Password

After this it is possible for PM to fetch and then show the key data.

3.16.1 FUNCTION KEYS

The headers [FunctionKeysDBC420], [FunctionKeysDBC422] and [FunctionKeysDBC425] are used to set the positions of the function keys and to set if the TNS keys shall be stored in the PABX. The function key data identifiers are according to the figures.

Note: When the IP telephones are used with MX-ONE and if the numbers associated with the function keys (TNS or MNS) are stored in the PABX, the system administrator has to consider the following:

At new installation of the IP telephones, it is very important to decide which function that shall exist on which key, to avoid future problems when functions shall be added or removed.

If a function associated to a function key is removed, all the existing TNS and MNS numbers will be moved one key upwards. To avoid this try to replace the function that shall be removed with another function.

If a function associated to a function key shall be added, try to replace an existing function key. If this is not possible all the existing TNS and MNS numbers will be moved one key downwards.

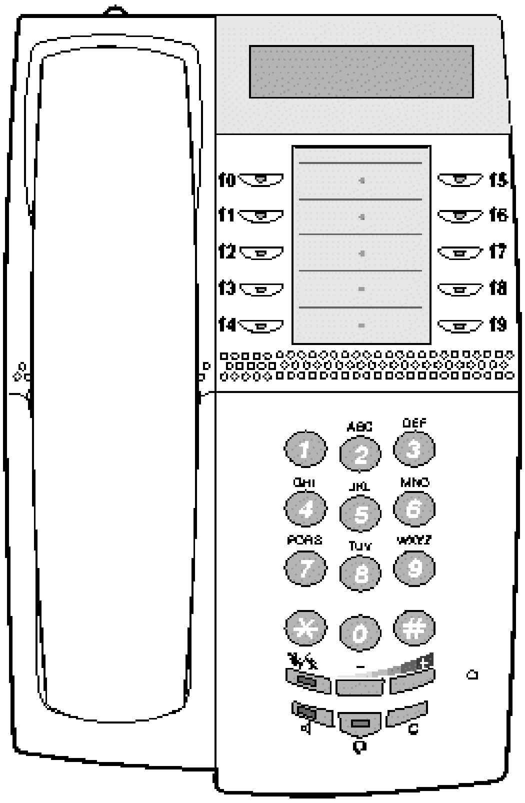


Figure 3: Numbering of the function keys in DBC 420 and in DBC 422

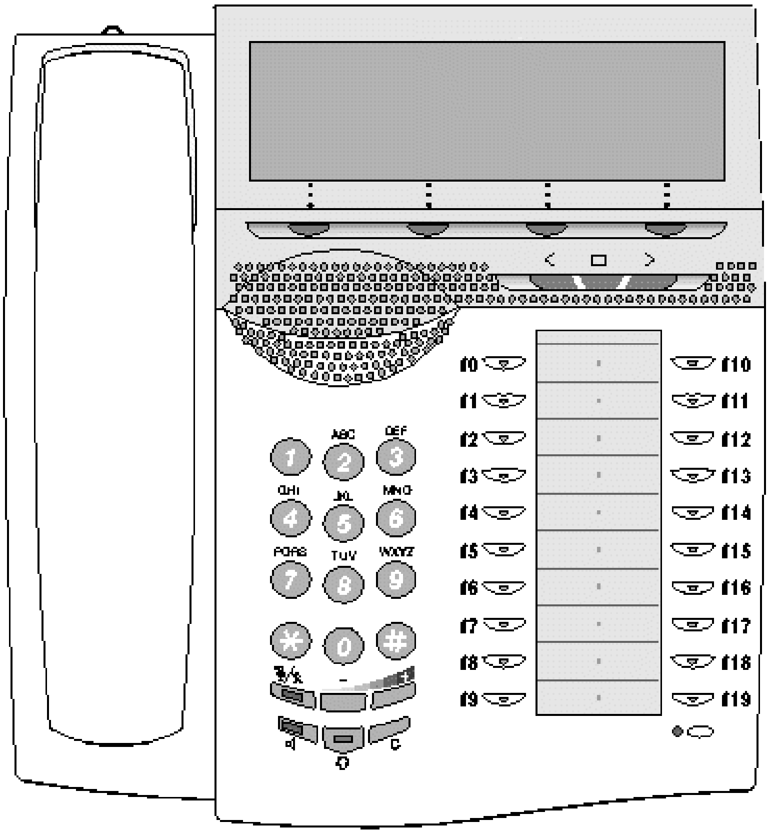


Figure 4: Numbering of the function keys in DBC 425

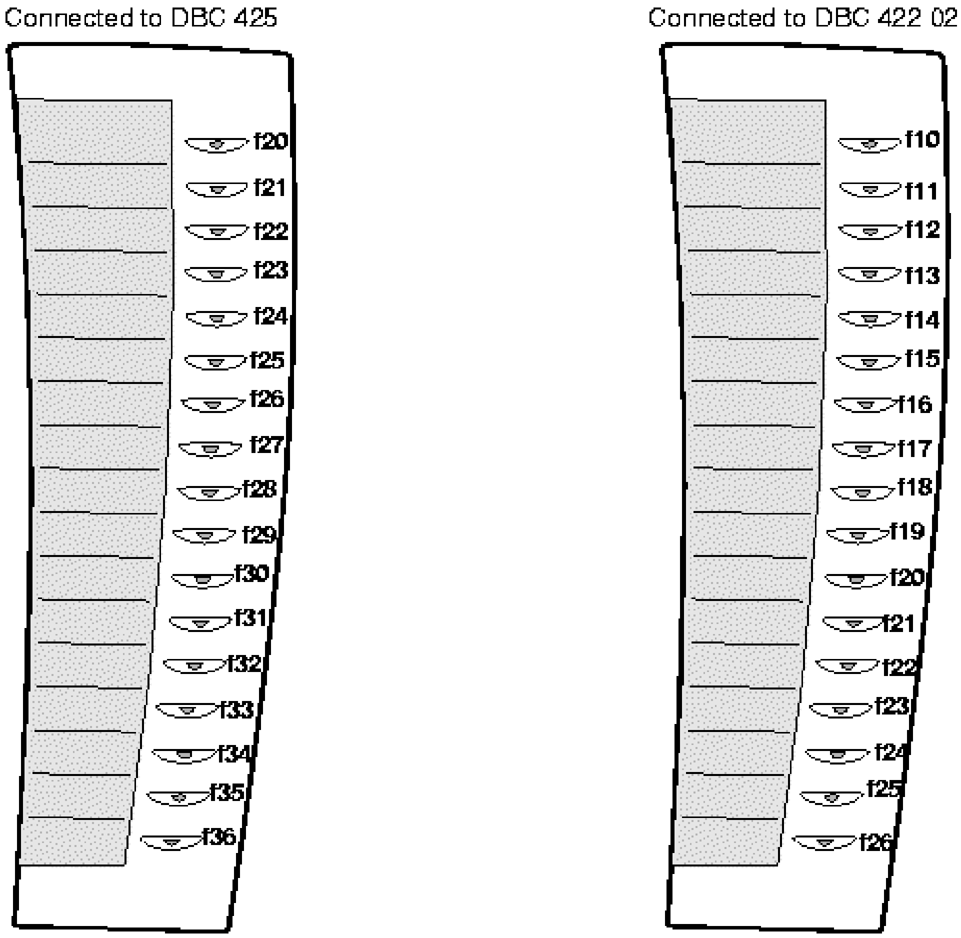


Figure 5: Extra key panel DBY 419 01.

The table below shows which key number that corresponds to the extra key panels, when connecting the key panels to **DBC 425**.

Table 1

No. of key panels	Key number
1	f20 - f36
2	f37 - f53
3	f54 - f70
4	f71 - f87

Table 2 Function keys for DBC 420, default values

Function key	MX-ONE	Configuration file
Line 1	f4	No
Line 2	f3	No
Inquiry	f2	No
Transfer	f1	Yes
Message waiting	f7	Yes
Free on 2:nd	f8	Yes
Follow me	f6	Yes
Call back	- 1)	Yes
Conference	f0	Yes
Call pick up 2)	- 1)	Yes
Call waiting	- 1)	Yes
Intrusion	- 1)	Yes
Status	f5	No
Call list	-	N/A
Settings	-	N/A
Menu	-	N/A
Directory Address	-	N/A
Home Address	-	N/A

1) This features can be initiated with suffix dialing, see 3.32 Suffix services on page 34

2) Individual call pickup

Table 3 Function keys for DBC 422, default values

Function key	MX-ONE	Configuration file
Line 1	f4	No
Line 2	f3	No
Inquiry	f2	No
Transfer	f1	Yes
Message waiting	f7	Yes
Free on 2:nd	f8	Yes
Follow me	f6	Yes
Call back	- 1)	Yes
Conference	f0	Yes
Call pick up 4)	- 1)	Yes
Call waiting	- 1)	Yes
Intrusion	- 1)	Yes
Status	-	N/A
Call list	f9	Yes
Settings	f5	Yes 2)

Function key	MX-ONE	Configuration file
Menu	-	N/A
Directory Address	-	N/A
Home Address	-	N/A

1) This features can be initiated with suffix dialing, see 3.32 Suffix services on page 34

2) The key can be moved, but must not be removed.

3) A special configuration file is delivered with MD-Evolution where the Message waiting key is placed on key f0 and the call list key is placed on key f7.

4) Individual call pickup.

Table 4 Function keys for DBC 425, default values

Function key	MX-ONE	Config file
Line 1	f9	No
Line 2	f8	No
Inquiry	f7	No
Transfer	f6	Yes
Message waiting	f5	Yes
Free on 2:nd	f4	Yes
Follow me	f2	Yes
Call back	f1	Yes
Conference	-	Yes
Call pick up 1)	-	Yes
Call waiting	-	Yes
Intrusion	-	Yes
Status	-	N/A
Call list	-	No
Settings	-	N/A
Menu	-	Yes
Directory Address	-	Yes
Home Address	-	Yes

1) Individual call pickup

The data identifiers are:

- **CallBack**
- **Transfer**
- **Menu**
- **FollowMe**
- **CallList**
- **FreeOnSecond**
- **MessageWaiting**
- **Conference**

- **Settings**
- **CallPickUp**
- **CallWaiting**
- **Intrusion**
- **DirectoryURL**, to define the function key for Directory Address, see 3.35 WAP on page 36
- **HomeURL**, to define the function key for Home Address, see 3.35 WAP on page 36
- **EnablePBXStoring**, set to **YES** to store the TNS key data in the PABX.

If the **EnablePBXStoring** is omitted, the default action is not to store the TNS keys in the PABX.

Note: If this parameter is enabled, the software in the PABX must support the storing of TNS key data.

If a function key data identifier is omitted, the corresponding function key will be removed. If the header is omitted the function keys will be in their default position. If one key shall be removed, all other keys must be defined.

Example: the message waiting key shall be omitted and the rest of the keys shall be in the same positions as in the default settings. The TNS numbers shall be stored in the PABX.

```
[FunctionKeysDBC422]
Transfer=1
FollowMe=6
FreeOnSecond=8
;MessageWaiting=7
Conference=0
CallList=9
Settings=5
;CallBack=
;CallPickUp=
;CallWaiting=
;Intrusion=
EnablePBXStoring=YES
```

3.17 HEADSET RING TONE

If headset preset mode is used and if automatic answer is selected, it is possible to get a tone in the headset to announce that there is a new call. It is also possible to select if a ring signal shall be initiated or not.

The header [HeadsetPreset] has the following parameter:

- **HeadsetTone: YES** or **NO**. A tone in the headset announces a new call. The default value is **NO.**
- **SpeakerRinger: YES** or **NO.** A ring signal announces a new call. The default value is **YES.** If this parameter is set to yes, the option Delayed Auto Answer must be enabled in the telephone.

3.18 IP PHONE ADMINISTRATOR

The tool IP Phone Administrator is used to monitor registered and un-registered IP telephones. This tool can also be used to know the IP address to DBC 420 02 telephones (without any display).

For MX-ONE Service Node the tool is integrated in the Service Node Manager (SN Manager).

For MX-ONE TSW and other platforms the tool is a stand alone application.

The header [IPPhoneAdministrator] is used to define data for the IP Phone Administrator tool:

- **IPPhoneAdministror:** can be set to **YES** or **NO**. The value **YES** means that the telephones will sent http messages to the IP Phone Administrator server, if there is an IP address initiates to this server. The value **NO** means that the telephone does not send such messages. The default value is **YES**.
- **ServerAddress**. The IP address to the IP Phone Administrator server can be set manually in the configuration file. The ordinary way to get this IP address is from a DNS SRV resource record, see installation instructions for *DBC 422 and DBC 425* section DNS SRV RESOURCE RECORDS. When using the telephone with MX-ONE SN, it is the IP address to MX-ONE Service Node Manager in LIM 1 that shall be defined.
- **ServerPort**. The port number to the IP Phone Administrator server can be set manually in the configuration file. The ordinary way to get this port number is from a DNS SRV resource record, see installation instructions for *DBC 422 and DBC 425* section DNS SRV RESOURCE RECORDS.

3.19 LANGUAGE

The header [Language] has the following data identifiers:

- **LanguageFile**. The path and the file name of the language file.
- **LanguageVersion**. The version of the language file.
- **OptionalLanguage**. Here can the procedure to change language in the gatekeeper also be stated, e.g. *08 *3# (if the gatekeeper supports such a procedure). The languages stated here are shown in the language menu in the IP telephone.
- **StartupLanguage**. During the boot sequence only English is available, but when the telephone is running, another language can be used. This start up language is defined here.

  When the user has set the language in his telephone, using the menu or the procedure (e.g. *08*3#), this specific language will be saved in the telephone. After a reboot the telephone will start up with this language, ignoring the start-up language defined in the configuration file.

  Translated languages:

  AN - Lithuanian
  CS - Czech
  DA - Danish
  DE - German
  EN - English
  ES - Spanish
  FI - Finnish

FR - French
HU - Hungarian
IT - Italian
LT - Estonian
NL - Dutch
NO - Norwegian
PB - Brazilian Portuguese
PL - Polish
RO - Romanian
RU - Russia
SK - Slovak
SL - Slovenian
SV - Swedish
XL - Spanish Latin America

3.20 LEVEL 2 QUALITY OF SERVICE

The header [L2QOS] is used in the IP telephone switch to:

- give different priorities for PC traffic and voice traffic (according to 802.1Q). See 3.20.1 Virtual LAN settings on page 26.
- define VLAN tagging (according to 802.1Q) and set the VLAN identity. See 3.20.1 Virtual LAN settings on page 26.
- limit the number of broadcast messages that the telephone shall handle. See 3.20.2 Broadcast message limit on page 28.

3.20.1 VIRTUAL LAN SETTINGS

The switch has three ports:

- **LAN Port:** The port to the network.
- **PC Port:** The port to the PC.
- **Phone Port** (called **MII Port** for DBC 42x 01): The port to the IP telephone.

The VLAN configuration file header is [L2QOS]. The following identifiers can be set:

- **PhonePort=m,n (called MII Port for DBC 42x 01):** this identifier has two values separated by a comma.

m User priority, see below. This value is used when the VLAN identity is defined in the configuration file or in DHCP option 43. The default value is 6.

n VLAN identifier, a number from 1 - 4094.

- **PCPort=m,n:** this identifier has two values.

m User priority, see below. The default value is 0.

n VLAN identifier, a number from 2- 4094.
Note: The value 1 cannot be used.

- **LANPort=r,s:** this identifier has two values.

r 0 = VLAN not used (untagged). 1 = VLAN used (tagged). When VLAN is not used the IP telephone always has higher priority than the PC.

s 0 = No VLAN for PC originating traffic (untagged).1 = VLAN will be used for PC originating traffic (tagged).

The user priority is defined as follows:

Table 5

0	Best effort, same as normal LAN traffic.
1	Background.
2	Spare, not recommended
3	Excellent effort.
4	Controlled load.
5	Video, less than 100 ms delay.
6	Voice, less than 10 ms delay.
7	Network control.

For default values see the examples below.

If the value entered manually in the boot menu shall be used after the telephone has started, the [L2QOS] header has to be omitted.

Examples: If X is the voice VLAN and Y is the data VLAN. If only the voice traffic shall be tagged and the data traffic shall use the native LAN, use the following settings:

```
[L2QOS]
PhonePort=6,X
PCPort=0,2
LANPort=1,0
```

If both the voice traffic and data traffic shall be tagged, use the following settings:

```
[L2QOS]
PhonePort=6,X
PCPort=0,Y
LANPort=1,1
```

- **RememberVLAN**. This parameter defines the VLAN tagging after a reboot.

COLD After a power reboot (the power is disconnected) or a software reboot, the telephone retains the previous VLAN identity. This option can be used in a network with VLAN in combination with IEEE802.1x, or if a limited scope with IP addresses in the native LAN are available.

WARM After a software reboot (the power is connected), the telephone retains the previous VLAN identity. After power reboot the telephone starts a new VLAN negotiation. This is the default value.

Note: When the VLAN identity shall be changed, the RememberVLAN parameter must not be set to COLD. If the parameter was previously set to COLD, the configuration file with the new parameter value must be downloaded to the telephone before the VLAN identity can be changed. When the parameter value is changed from COLD to WARM, a new VLAN negotiation is started. When the VLAN identity is defined via the configuration file, it is important that the VLAN identities are correct, otherwise the telephone may access the native LAN and the VLAN in a loop. The alternative to automatic VLAN detection is to edit the VLAN identity manually via the telephone menu or via the web interface.

Note: If the VLAN identity shall be set manually, the header [L2QOS] with associated parameters have to be disabled in the configuration file.

3.20.2 BROADCAST MESSAGE LIMIT

With the broadcast message limit parameter it is possible to set the limit for number of broadcast messages that the switch in the telephone shall handle. This can be useful if broadcast storms occur on the LAN.

If the limit is too high, there is a risk that the telephone freezes when trying to handle all the messages. If the limit is too low there is a risk that messages important for the telephone traffic are lost, which can mean that calls can be lost.

BroadcastStormControlLimit: Define the number of broadcast messages to handle within 100 millisecond. The default value is 80 which mean that 800 broadcast messages per second are handled by the telephone.

3.21 NETWORK

The header [Network] is used to define how the telephone shall handle information about duplicated IP addresses. The following parameter exists:

DuplicateIPAddressIgnore. The parameter defines if the telephone shall ignore information about duplicated IP addresses or not.

- **DISABLE**. The ARP protocol has reported a duplicated IP address and the telephone will not use this address. An error message is shown in the display. This is the default value.
- **ENABLE**. The ARP protocol has reported a duplicated IP address but the telephone will use the IP address anyway. If the protocol reports duplicated address three times, the telephone will not use this address. Please note that the telephone may not function properly if duplicated IP address is ignored. This parameter value can be useful if a device in the network propagates (G-ARP) the same IP address as the one telephone uses, but in fact this device does not hold this IP address (wrong configured DHCP server, possible intrusion/hacking attempt).

3.22 LED CADENCE SETTINGS

Three different LED cadence settings can be set. The header [LEDs] has the following data identifiers:

- **Cad0:** in a call.
- **Cad1:** call parked.
- **Cad2:** incoming call.

For each of these three LED settings, four intervals must be set. First value is how long the LED should be on, the second is how long it should be off, the third is on and the fourth is off, then the first value is used again and so on. The values have the range 0-255, one unit is 10 ms. For default values 4 Examples on page 42.

3.23 CALL CLEARING

(Only H.323). The header [NewCallClearing] is used to define how the call shall be cleared. This parameter has only to be considered when the system is MX-ONE.

The identifier is [NewCallClearing] and this has the parameter values:

- **YES**. The call clearing follows the H.323 standard strictly. If the parameter is YES and the MX-ONE Service Node software is old, there can be problems at clearing of calls. For example when initiating call back and after getting accept, the call is not possible to clear. This parameter shall be YES when new MX-ONE Service Node software is used.
- **NO**. If the parameter is NO and if the MX-ONE Service Node software is old, problem can occur at call clearing when using MiContact Center Solidus and when the two parties (the call center agent and other party) clear the call at the same time. This is the default value.

Note: MX-ONE Service Node software is regarded as new when MX-ONE 3.0 Service Pack 4 or MX-ONE 3.1 Service Pack 1 or later is used.

3.24 OMD SETTINGS (ONLY WITH MX-ONE)

The header [OMD] is used to set the signaling address to the telephony server when a DBC 422 or a DBC 425 is used as an OMD (Operator Media Device). Two identifiers are used:

- **SNAddress =** the IP address of the telephony server.
- **SNPort =** the operator signaling port number of the telephony server.

The identifiers for the address and the port number can be defined twice, if the redundancy feature is used. Example:

```
[OMD]

SNAddress=130.100.188.111

SNPort=1700

SNAddress=130.100.86.18

SNPort=1700
```

DBC 422 02 and DBC 425 02: The telephone can be initiated to OMD from one of the menus or from the administrator web interface.

Only the following configurations in the configuration file will be relevant when DBC 42x is used as an OMD:

- Software
- Codec priority
- Tone configuration
- LED cadence settings
- Tone ringer cadence settings
- VLAN settings
- Auto negotiation

The OMD can only be used for MX-ONE Service Node. The OMD is initiated in the MX-ONE Service Node with the OPSAI command, see the command description for *PBX OPERATOR TRAFFIC*.

3.25 PASSWORD

The header [Password] is used to define how passwords and PIN (personal identity number) shall be handled in the telephone. Possible data identifier:

- **ServiceCodeChangePIN**: The service code for changing the PIN. Example *74*
- **PINorPassword**: It is possible to choose if a password or a PIN shall be used when register the telephone to the system.
    - PIN: Shall be selected when the telephone is used with MX-ONE3.2 or later. The menu for changing PIN can be selected. It is only possible to enter digits as the PIN. The text string when register the telephone is Enter PIN instead of Enter password.
    - Password: The menu for changing PIN is not available. The text string at log on is Enter password. Default value.
- **PasswordInputFormat**: This parameter has only affect when PINorPassword=Password:
    - Alphanumeric: When entering the password at registration of the telephone, alphanumeric characters are allowed. Default value.
    - Digit: When entering the password at registration of the telephone, only digits are allowed.

3.26 VOICE RECORDING

It is possible to record calls to a central recording equipment. There are two options:

- Active recording: all calls to the monitored extensions are recorded.
- Record on demand, ROD: the user can start and stop the recording by pressing a function key.

The header [Recorder] is used to define data for voice recording. For more information see also Installation Instructions for DBC 422 and DBC 425.

The following data identifiers can be used:

- **LoggerIPAddress1**. The telephone checks that the IP address from which the recording is ordered corresponds to the IP address in this parameter value. If it does not correspond the recording will not start. The reason for this check is to improve the security to make it more difficult with unlawful recording. Three IP addresses can be defined.
- **LoggerIPAddress2**. See LoggerIPAddress 1 above.
- **LoggerIPAddress3**. See LoggerIPAddress 1 above
- **LoggerIPAddress4**. See LoggerIPAddress 1 above
- **LoggerIPAddress5**. See LoggerIPAddress 1 above
- **LoggerIPAddress6**. See LoggerIPAddress 1 above

Recording on demand settings when using a NICE® recording system:

- **RODServerIPAddress**. The IP address to the server to which the telephone sends the record on demand requests.
- **RODServerName**. The name of the ROD server. This data must be provided by the administrator for the NICE Perform® recording system.

- **RODServerCredentials=username:password**. The login credentials towards the ROD server. The format of the parameter value must be as described above. This data must be provided by the administrator for the NICE Perform® recording system.
- **RODServerGKId**. The telephone must send this identity to the ROD server. This data must be provided by the administrator for the NICE Perform® recording system.

Recording on demand settings when using another vendor of recording system:

- **RODStart.** URL sent by the phone to the recording system when the recording key is pressed to start the recording. Example: http://192.105.88.152:80/recbutton?command=start&user=12345678. The phone needs the IP address but the rest of the URL can be specified according to what the recording system requires.
- **RODStop**. URL sent by the phone to the recording system when the recording key is pressed to stop the recording. Example: http://192.105.88.152:80/recbutton?command=stop&user=12345678. The phone needs the IP address but the rest of the URL can be specified according to what the recording system requires.
- **RecordingTone**

  ENABLED. A defined tone will be heard when call is recorded.

  DISABLED. Default value.

3.27 RING CADENCES

The header [RingCads] has the following data identifiers:

- **Internal=** ring signal when receiving internal calls.
- **External=** ring signal when receiving external calls.
- **Callback=** ring signal when the callback function is used.
- **Extra=** ring signal for other purposes.

For each of these settings, six intervals must be set. The intervals have the same meaning as for the LED cadence settings, but with two additional intervals. The values have the range 0-255, one unit is 50 ms. For default values see section 4 Examples.

- **Delay=** the alerting delay before the ring signal starts after the call is received. The delay is valid for alert 1st call, alert 2nd and 3rd call and for MNS keys. It is not valid for call back.The delay time is in second. The default value is 7 seconds.
- **CallWaiting=** When the telephone receives call waiting, the alerting can be of two types with the following parameter values:
  - **Tone**. Call waiting tone
  - **RingSignal.** Ring Signal. This is the default value

3.28 RINGLEVEL

- **RingLevel**. Used to control incoming MNS ring level at speech state.
- **Normal.** Default value. Latest user programmed ring level will be used.

- **LOW**. Minimum ring level will be used.
- **SILENCE**. No ring signal will be heard.

3.29 SECURITY

The header [Security] is used to define the parameters for security in the telephone. The telephone has support for signaling encryption with TLS and support for media encryption with SRTP (Secure RTP).

If the security is enabled and a valid password provided, the telephone will at registration try to use TLS for encryption of the signaling. Signaling encryption according to TLS is also used in the call set up phase (H.245 and H.225).

For H.323, the RAS signaling will use TCP instead of UDP. If the TLS/TCP negotiation fails, it is the security policy in the system and the other security parameters below, that decides what will happen.

If security is enabled, the telephone will try to use SRTP for media encryption.

- **Security=**
  - **ENABLED** If a valid password is provided, the telephone will try to use signaling encryption with TLS and if this is successful it will announce that it has support for media encryption with SRTP.
  - **DISABLED** The telephone will not announce TLS and SRTP capability. (Default value)
- **SecurityFallback=**
  - **YES**: If the TLS/TCP negotiation fails, it shall be permitted to continue the registration with RAS over UDP in a not secure way. (Default value).
  - **NO**: It shall not be permitted to continue the registration if the TLS/TCP negotiation fails.
- **CertificateValidate=**
  - **YES**: The telephone shall validate the server certificate. If the parameter value is YES, but the server does not have a valid certificate that is signed by one of the Certificate Authorities (CA) supported by the telephone, this will result in failed authentication. (Default value).

    Note. The parameter NTP= must be set, see 3.33 Time on page 35. The reason is that the terminal must have correct time before it is registered.
  - **NO**: The telephone shall not validate the server certificate.
- **SaveUserPassword=**
  - **YES**: The end-user password (used to register towards the gatekeeper) is stored in the memory in the telephone in the same way as when security is disabled. (Default value).
  - **NO**: The end-user has to enter the password each time the telephone tries to register towards the gatekeeper, after power failure, network problems, firmware upgrade etc.
- **SignalingEncrypted=**
  - **YES**: The signaling is encrypted. This is the default value.

  - **NO**: Null cipher which means that no of the signaling is done but the signaling sequence is the same as when the signaling is encrypted. This option can be used at fault locating.
- **RootCert=**
  - **file name.pem**. The file name of the root CA certificate stored on the software server. The path where the file shall be stored must be according to the Installation Instructions for DBC422 and DBC 425. The parameter is only used when a new certificate which does not already exists in the application shall be loaded.

    It is possible to remove a certificate that has earlier been loaded, by comment the file name. Example:
    ;RootCert=cacert.pem
- **UDPFilter=**
  - **ENABLED** All UDP ports that are not used in the call are blocked. Default value.
  - **DISABLED** All UDP ports are open.
- **UDPRateLimit=**

  With this parameter it is possible to set the rate limit for incoming UDP packets. If the limit is exceeded within 2 seconds, the additional packets will be discarded. Then new counting will start at the start of the next two seconds.

  Too low value can cause choppy speech, especially when short packet size (10 or 20 ms) is used.

  The default value in the application is 250 packets per two seconds.
- **TCPFilter=**
  - **ENABLED** All TCP ports that are not used are blocked. Default value.
  - **DISABLED** All TCP ports are open.
- **OpenTCPPort1**
  - 1720. Default open port.

  OpenUDPPort1
  - 9200. Default open port.
- **OpenUDPPort2**
  - 9200. Default open port.
- **OpenUDPPort3.**
  - 9200. Default open port.

3.30 SNMP AGENT

The header [SNMP] is used to manage the built in SNMP agent in the telephone. The following parameters exist:

- **SNMPAgent**. Used to enable/disable the SNMP agent in the telephone. The parameter values can be:
  - **DISABLED**. The default value.

  - **ENABLED**.
- **CommunityString**. When the agent is enabled, the system administrator must set this text string. The community string is used as a password.

  If the community string in the phone is equal to the community string set in the scanning tool, the telephone responds with the requested information. If the community string is incorrect, the telephone simply discards the request and does not respond.

For more detailed information about the SNMP agent, see installation instructions for DBC 420.

3.31 STORING LOCAL PHONE BOOK ON A FTP SERVER

The header [STOREPHONEBOOK] is used to store the telephone’s local phone book (Contacts) on a central FTP or SFTP server. The following parameters exist:

- **EnableStoring:** defines if the contacts shall be stored in the memory in the or on the FTP (SFTP) server:
  - **YES**: the contacts are stored on the FTP (SFTP) server.
  - **NO**: the contacts are stored in the flash memory in the telephone
- **IPAddress:** The IP address to the FTP (SFTP) server. The default value is the IP address to the software server where the FTP server also can be located.
- **FTPUname:** The user identity (or user account) under which the Contacts files are stored on the FTP (SFTP) server. Maximum 24 characters, the default user name is *Telephone*.
- **FTPPword:** The password for the user name (or account) under which the Contact files are stored on the FTP (SFTP) server. Maximum 24 characters, the default password is *Telephone*.
- **UseSFTP:** The type of server to be used when storing the phone book.
  - **YES**: Use a SFTP server for storing the files for the phone book data.
  - **NO**: Use a FTP server for storing these files. This is the default value.

3.32 SUFFIX SERVICES

3.32.1 SUFFIX SERVICES

In H.323 this feature is only for DBC 420 and DBC 422 with MX-ONE. The header [SuffixServices] is used to setup services that can be used by pressing one digit after a call has been made to a busy extension, except for callback which can be initiated even if the extension is not busy. The following data identifiers can be used:

- **Intrusion**
- **CallWaiting**
- **CallBack**
- **CallPickUp**

Permitted values are: digits 0-9.

The identifiers shall be set to the digit which shall be used to initiate the service: e.g. CallBack=5.

3.33 TIME

The time that is shown in the telephone display can be updated via:

- WAP messages. The header [Time] has no effect.
- An NTP server. NTP (Network Time Protocol) is a standard protocol used to retrieve the time in a LAN network. The telephone has support for SNTP (Simple Network Time Protocol), which is a subset of NTP.

The header [Time] shall only be used if time is updated via SNTP. If the header is omitted, the telephone uses the time received in the WAP signals from the gatekeeper (only H.323). The header has the following data identifiers:

- **TIMEZONE** =id:D1:D2:D3:D4.
  - id= name of the time zone created. Examples:
  - CET = Central European Time
  - D1 = time in minutes east of UTC (Universal Coordinated Time) which also known as Greenwich mean time (GMT).
  - D2 = time in minutes west of GMT time
  - D3 = daylight savings time begins (month-day-hour)
  - D4 = daylight savings time ends (month-day-hour)

  If no daylight savings time shall be used, D3 and D4 shall be omitted.
- **NTP-server**. The IP address to the NTP server from where the IP telephone shall fetch the time.

If different time zones shall be used in a system, the time shall be received via SNTP.

When the phone is used with MX-ONE SN in H.323, time is fetched from:

1. NTP server
2. Primary gatekeeper
3. Secondary gatekeeper.

If security is enabled and certificate is validated, time must be fetched from a NTP server.

3.34 TONE CONFIGURATION

The header [Tones] has the following data identifiers:

- Dial tone
- Special dial tone
- Busy tone
- Alerting tone
- Congestion tone

- Special information tone (number unobtainable)
- Call waiting tone
- Offhook queuing tone
- On hold tone
- External dial tone
- Recording tone
- Waiting voice tone (also called *Connection in progress tone*). This tone can be used in traffic cases when it takes some time to establish the speech channel, for example answering on a monitoring key. The tone starts when the key is pressed and stops when the speech channel is established.
- Headset ring tone. See 3.17 Headset ring tone on page 24

Each tone has 16 values that must be set. The values have the following meaning:

- Number of cadences, 0 means constant tone.
- Number of frequencies, 0 means one frequency, 1 means 2 frequencies modulated, 2 and 3 are not implemented and 4 means three frequencies with one cadence each.
- First tone on, time in milliseconds.
- First tone off, time in milliseconds.
- Second tone on, time in milliseconds.
- Second tone off, time in milliseconds
- Third tone on, time in milliseconds.
- Third tone off, time in milliseconds
- First frequency in Hertz (minimum 300, maximum 2000 Hertz).
- Tone level for the first frequency, cannot be changed, it is always -10 dBm0.
- Second frequency in Hertz (minimum 300, maximum 2000 Hertz).
- Tone level for the second frequency, cannot be changed, it is always -10 dBm0.
- Third frequency in Hertz (minimum 300, maximum 2000 Hertz).
- Tone level for the third frequency, cannot be changed, it is always -10 dBm0.
- Tone in voice, 0 is off, 1 is on. A tone locally generated in the telephone is mixed with the received RTP stream. Tone in voice = off, means that if a tone is played in voice, the voice will be switched off until the tone stops.
- Tone not sine wave, only 0 is implemented which means sine wave.

To get a silent dial tone, value number nine (frequency of the first interval) should be set to zero. For default values see 4 Examples on page 42. Tone level cannot be changed, it is always -10 dBm0.

Note: Only parameter values with integers can be used. No decimal point is allowed.

3.35 WAP

The header [WAP] has the following data identifiers:

- **WapProxyIP**. (Only used by DBC 425 02). The IP address to the proxy server, see 3.35.1 WAP proxy on page 39.

- **WapProxyPort**. (Only used by DBC 425 02). The port number used by the proxy server, see 3.35.1 WAP proxy on page 39.
- **AddressWithoutProxy**. (Only used by DBC 425 02). The IP address to the corporate directory WAP server, when no proxy shall be used between the IP telephones and the server, see 3.35.1 WAP proxy on page 39.
- **DirectoryServer**. (Only used by DBC 425 02). This identifier defines which type of corporate directory interface that shall be used. The parameter value affects the placing of the soft keys used for searching in the directory. The following values exist:
  - **Softkey** (parameter value DME works also). Can be used with Mitel CMG. The phone assigns a softkey for searching in the directory. Default value.
  - **Generic**. The telephone will place the soft-keys in the same way as when using the Web menu in the top menu bar.
- **HomeAddress**. (Only used by DBC 425 02). The URL to the home WAP page (portal). It is possible to define a variable in the URL, see 3.35.2 Substitute a variable in the URL on page 39.
- **UseWAPforCorpDir**. (Only used by DBC 425 02).
  - **YES**. Use the WAP browser in the telephone to display Corporate Directory. This is the default value. Can be used towards the directories in Mitel CMG but also towards other directory systems supporting WAP.
  - **NO**. Use the XML parser in the telephone to display Corporate Directory. Can only be used towards the directories in Mitel CMG.

  The XML method supports more language dependent characters than the WAP browser. The GUI for searching in the directory is improved when using XML compared to the WAP method, which can be another aspect when deciding which method to use.
- **MaxAttempts**. Maximal number of attempts to resend a WAP message if no answer is received. WAP messages are sent on unreliable UDP which means that re-sending is necessary at loss of packages. Minimum is 1 and maximum is 4.
- **RetransPeriod**. The time in milliseconds between each re-sending. Minimum is 2000 and maximum is 7000 with 1000 ms steps.
- **CountryCode**. The country code of the country where the PABX is located.
- **RouteAccessNumber**. The route access number.
- **CountryCodePrefix**. The prefix of the code of the country where the PABX is located.
- **NumberWithAreaCode:** if the area code shall be sent or not. This parameter is only used for calls within the own country.
  - **YES** include the area code and area code prefix when converting international phone number to dialling number. This is the default value.

    Example: +46 8 56867000 converted to 00 08 56867000, where 00 is the route access number.
  - **NO** remove the area code and area code prefix if the number is within the same area as the PBX, that is the area code in the number to dial is equal

to the AreaCode in the configuration file. If the area code does not match the AreaCode in the configuration file, the area code will be sent.

Example: +46 8 56867000 is converted to 00 56867000 when the AreaCode=8 in the configuration file.

- **AreaCodePrefix**. The prefix of the code of the area in the country where the PABX is located.
- **AreaCode**. The remaining part of the area code when the area code prefix is removed.

  Example: If the total area code is 08, the AreaCodePrefix=0 and the AreaCode=8

Match a dialled number to get the name from Contacts

When a dialled number shall be matched with the number in Contacts to display the corresponding name, the following is valid:

If the area code is optional when making calls, the parameter AreaCode must be given.

Example: In Contacts the name and number + 46 8 568 6700 Peter Smith is stored (where 08 is the total area code). The end-user dials either 00 08 568 6700 or 00 568 6700 (where 00 is the route access code) because the area code is optional. If the telephone shall be able to match this dialled number with the number stored in Contacts, to display Peter Smith, the AreaCodePrefix=0 and AreaCode=8 must be defined in the configuration file.

Compose a B-number

The CountryCode and RouteAccessNumber are used to compose a B party number to dial out via the PBX when a telephone number received from the corporate directory WAP server is a global international telephone number that has the format plus sign (+) CountryCode national telephone number.

If the country code in the received number is equal to the CountryCode in the configuration file, the plus sign and the country code will be replaced by the RouteAccessNumber. For the area code there are the following options:

- If NumberWithAreaCode=YES, the AreaCodePrefix and AreaCode will be added. Example: +46 8 56867000 will be dialed as 00 08 56867000.
- If NumberWithAreaCode=NO, the AreaCodePrefix and AreaCode will not be added. Example: +46 8 56867000 will be dialled as 00 56867000 if the AreaCode=8 in the configuration file.

If the country code in the received number is not equal to the CountryCode in the configuration file, it will not be removed, but the plus sign will be replaced by the RouteAccessNumber and CountryCodePrefix. The B party number to dial will consist of RouteAccessNumber, CountryCodePrefix, country code and the national telephone number. Example: +46 8 56867000 will be dialled as 00 00 46 8 56867000 if the country code is not equal to 46 in the configuration file. In this case the parameter NumberWithAreaCode does not have any impact.

Table 6 URL for different corporate directory servers

Corporate Directory	URL in Directory Address
CMG	<IP address:port>/CorpDir/d4/d4.aspx

3.35.1 WAP PROXY

If a proxy shall be used for the WAP browsing function, but not for the Corporate Directory function, the parameters shall be set in the following way:

- **WapProxyIP** and **WapProxyPort** shall be enabled
- **AddressWithoutProxy** shall be set to the same IP address as the **Directory** address**.**

If no proxy shall be used between the IP telephones and the WAP server for the Corporate Directory and if the WAP browsing shall only be done on the intra-net (without any proxy, the parameters **WapProxyIP**, **WapProxyPort** and **AddressWithoutProxy** shall be omitted.

3.35.2 SUBSTITUTE A VARIABLE IN THE URL

In the corporate directory URL and in the home URL it is possible to define a variable for the directory number and a variable for the IP address of the telephone. When the URL is used, the variable is replaced by the current telephone number and/or IP address.

The syntax of the URL parameter is: //<address>/<path>?<query>

address

The network location (for example the IP address) of the WAP server.

path

String of names (directories) separated by slashes.

query

Variables to substitute. Separated by the character &. This parameter is optional.

Name1=%NUM% Directory number of the telephone. The variable identifier is NUM. Name2=%IP% IP address of the telephone. The variable identifier is IP.

Example: Create the URL parameter for the WAP server with the IP address 192.168.1.1 and use the directory *cgi-bin/home.cgi*. The directory number and the IP address of the telephone shall be sent in the URL. The URL defined in the configuration file:

http://192.168.1.1/cgi-bin/home.cgi?Dirnum=%NUM%&IPaddress=%IP%

The URL sent from the telephone 67609 with the IP address 192.168.1.10 will be:

http://192.168.1.1/cgi-bin/home.cgi?Dirnum=67609&IPaddress=192.168.1.10

3.36 WEB INTERFACE

The header [WebServer] is used to enable or disable the web interface for the end-user.

From a web-browser in a PC, it is possible to log on to the telephone for handling of the contact list, call list, and so on. It is possible to log on as an end-user or as a system administrator. One parameter exists:

- **webInterFaceForUser**:
  - **Enabled**: the end-user web interface is enabled. This is the default value.
  - **Disabled**: the end-user web interface is disabled. The web interface for the system administrator is not affected.

- **Enabled_with_default_pwd**: if the end-user has a PIN or password, they are used for logging in to the web interface. If the end-user has no PIN or password it is possible to log in with the default password *Welcome*.

Note: When using the option **Enabled_with_default_pwd**, and the user does not have any PIN or password, it is very easy to log in to someone else's telephone and look in the call list and contacts.