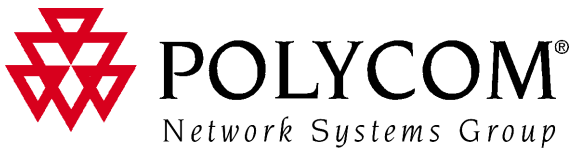
MGC
Administrator's Guide

Version 9.0



Polycom Moscow
zakaz@polycom-moscow.ru
T +7 495 924-25-25
www.polycom-moscow.ru

Catalog No. DOC2192A
Version 9.0

Notice
While reasonable effort was made to ensure that the information in this document was complete and accurate at the time of printing, Polycom, Inc. cannot assume responsibility for any errors. Changes and/or corrections to the information contained in this document may be incorporated into future issues.
Portions, aspects and/or features of this product are protected under United States Patent Law in accordance with the claims of United States Patent No: US 6,300,973; US 6,496,216; US 6,757,005; US 6,760,750; and US 7,054,620.
PATENT PENDING

Canadian Department of Communications (EC) Declaration of Conformity

Polycom, Inc. declares that the MGC-50/MGC-100 with NET-8 card is in conformity with the following relevant harmonized standards:
EN 60950: 1992 Including Amendments 1,2,3 & 4
EN 55022: 1994
EN 50082: 1997

and follows the provisions of the Council Directive 1999/EC on radio and telecommunication terminal equipment and the recognition of its conformity.

Notice: The Industry Canada label identifies certified equipment. This certification means that the equipment meets telecommunication network protective, operational and safety requirements as prescribed in the appropriate Terminal Equipment Technical Requirements document(s). The Department does not guarantee the equipment will operate to the user's satisfaction.

Before installing this equipment, users should ensure that it is permissible to be connected to the facilities of the local telecommunications company. The equipment must also be installed using an acceptable method of connection. The customer should be aware that compliance with the above conditions may not prevent degradation of service in some situations.

Repairs to certified equipment malfunctions, may give the telecommunications company cause to request the user to disconnect the equipment.

Users should ensure for their own protection that the electrical ground connections of the power utility, telephone lines and internal metallic water pipe system, if present, are connected together. This precaution may be particularly important in rural areas.

Caution: Users should not attempt to make such connections themselves, but should contact the appropriate electric inspection authority, or electrician, as appropriate.

Table of Contents

1

Before You Begin

Scope of Manual

This manual describes the MGC Manager software installation, the configuration procedures and advanced system settings procedures. It is intended for service engineers and system administrators who need to configure, manage and maintain the MGC unit.

Only MGC Manager operators with Suppressor rights can perform MGC Manager configuration tasks. In addition the user must have Superuser rights on the computer on which the MGC Manager application is running, or any other permission than enables the application to access the Registry (read/write) and read/write files on the C: drive (root directory) and under the Windows directory folder.

Detailed information on using the system, including starting and shutting down the system, is provided in the MGC Manager User's Guide Volume I and Volume II.

This manual assumes the user has knowledge of the following:

- Familiarity with the Windows 95/98/2000/NT/XP environment and interface
- Basic knowledge of video conferencing concepts and terminology
- Basic knowledge of the MGC Manager application

Contents

The MGC Administrator's Guide includes the following chapters:

- **Chapter 1 - Before You Begin**

  Provides a general description of the MGC unit, its system requirements and its prerequisites, and describes the topics and conventions to be found in this manual.

- **Chapter 2 - Software Installation**

  Includes step-by-step instructions for installing the MGC Manager software, downloading the software to the MGC unit, and configuring the IP address of the MGC unit.

- **Chapter 3 - Defining Network Services**
  Includes step-by-step instructions for defining Network Services that supply ISDN and T1-CAS lines, ATM, IP, Serial or leased lines to the MGC unit. In addition, it describes the assignment of the Network Service to the appropriate Network module installed in the MCU.

- **Chapter 4 - MCU Card Management**
  Describes how to:
  - List the installed functional modules (cards)
  - View and configure functional module parameters
  - Reset the functional modules and their units
  - Remove and restore a functional module

- **Chapter 5 - System Management**
  Describes how to use various utilities provided with the system to perform tasks such as:
  - View the system resources status
  - Use various MCU Utilities to view and modify configuration files residing on the MCU's hard disk
  - Work with the MCU in general
  - Access the MCU with IP Terminal
  - Set the communication default parameters

- **Chapter 6 - Defining Operators**
  Provides instructions for defining new MGC Manager operators and managing the operators connected to the system

- **Chapter 7 - Configuring the Gateway**
  Describes the various routing methods and provides step-by-step instructions for configuring the gateway.
- **Chapter 8 - Audio and Video Conversion Tools**
  Describes how to use the Greet and Guide tools to create audio messages and video slides and how to convert them into the MGC format.
- **Appendix A - Faults**
  Lists the fault codes and their descriptions.
- **Appendix B - PPP Setup**
  Describes how to establish TCP/IP communication between the MGC Manager and the MCU via a telephone line, modem or serial connection.
- **Appendix C - Performance Monitoring Net-T1/Net-E1**
  Describes how to monitor the performance of the ISDN lines connected to the Net-T1/Net-E1.
- **Appendix D - The Falcon Diagnostic Tool**
  Describes how to use the Falcon diagnostic tool which is an add-on to the MGC application that enables you to run diagnostic tests on the hardware and software of the MGC-25, MGC-50 and the MGC-100 units.

Conventions

Before using this manual, it is important for you to understand the terms and conventions used:

- The term “Double-click” is used when you need to activate a menu command or a command button in the dialog box.
- The term “Select” or “Click” is used to highlight a part of the window, dialog box or menu that you want to be changed with your next action.
- The term “Right-click” is used when you press and release the right mouse button to open a pop-up menu.
- The term “Click OK” means that you can either click the OK button with the mouse, or press the <Enter> key on the keyboard.
- Keyboard keys appear in capital letters, between these two symbols < >. For example, the Shift key appears as <Shift>.
- The plus sign (+) between two key names indicates that you must press and hold down one key while pressing down the second key. For example, “press <Alt>+<P> means that you press and hold down the Alt key while you press the P key.
- **Bold** type appearing in the text, or in a procedure indicates the word or the character that you should type into a text box or the name of the menu, command, option or button that you should select.
- *Italic* type appearing in the text or in a procedure indicates the name of the menu, dialog box or field from which an option should be selected or into which parameters should be entered, or an icon name.
- Tips and notes are indicated by an icon and appear in a special format on a gray background. For example:

This is an example of the type of note that you encounter in this Administrator’s Guide.

List of Abbreviations

Following is the list of abbreviations used throughout this manual:

Table 1-1: List of Abbreviations

API	Application Programming Interface
CSU	Channel Service Unit
DPR	Dual Port Ram
ESD	Electro-Static Discharge
HDLC	High-level Data Link Control
HSD	High Speed Data
IP	Internet Protocol (H.323 and SIP)
LAN	Local Area Network
LED	Light Emitting Diode
LSD	Low Speed Data
MCU	Multipoint Control Unit
MPI	Multi Protocol Interface
MUX	Multiplexer
PBX	Private Branch Exchange
PRI	Primary Rate Interface
TCP	Transmission Control Protocol
TDM	Time Division Multiplexing
UIF	User Interface

Installation and Configuration Workflow

The MGC configuration includes the following main steps: Hardware Installation, Software Installation, Network Services definition and the MGC unit configuration. The hardware installation is described in the MGC Hardware and Installation Guide. The remaining steps are described in this guide as illustrated in the following chart.

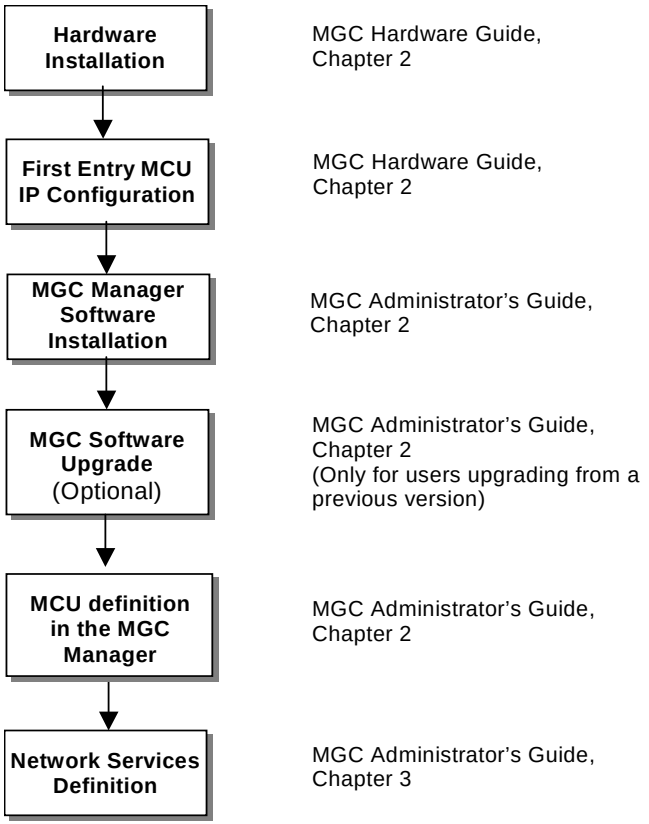


Figure 1-1: Installation and Configuration Workflow

2

Software Installation

This chapter describes the MGC Manager software installation and the definition of the MCU(s) in the MGC Manager application.

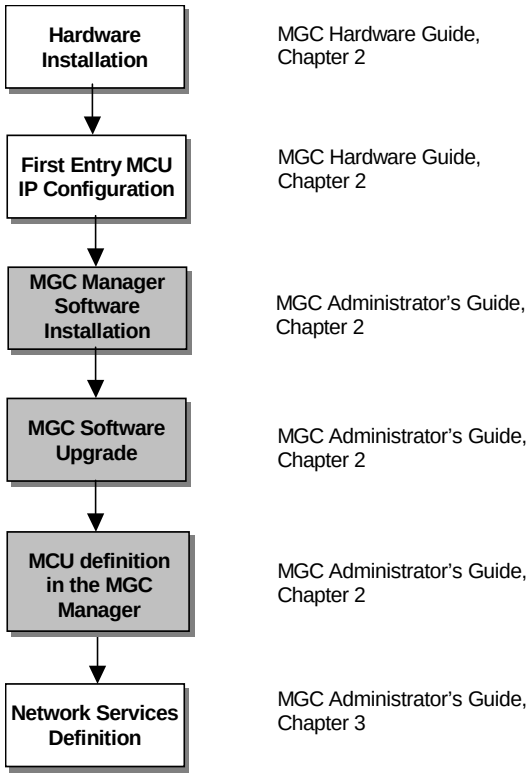


Figure 2-1: Installation and Configuration Workflow - Software Installation

Only users (MGC Manager operators) with Superuser rights can perform MGC Manager configuration tasks. In addition the user must have Superuser rights on the computer on which the MGC Manager application is running, or any other permission than enables the application to access the Registry (read/write) and read/write files on the C: drive (root directory) and under the Windows directory folder.

MGC Manager Software Installation

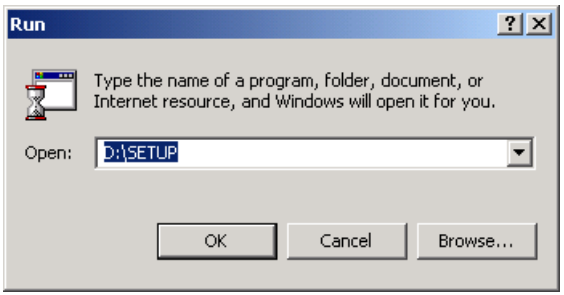
To set up conferences and control the MGC unit you need to install the MGC Manager software on your computer.

Close all programs before installing the MGC Manager software.

To install the MGC Manager software:

The MGC Manager software installation procedure is identical for new installations and for upgrades from previous versions.

1. Insert the software CD into the CD drive.
2. On the *Start* menu, click **Run**.
   The *Run* dialog box opens.

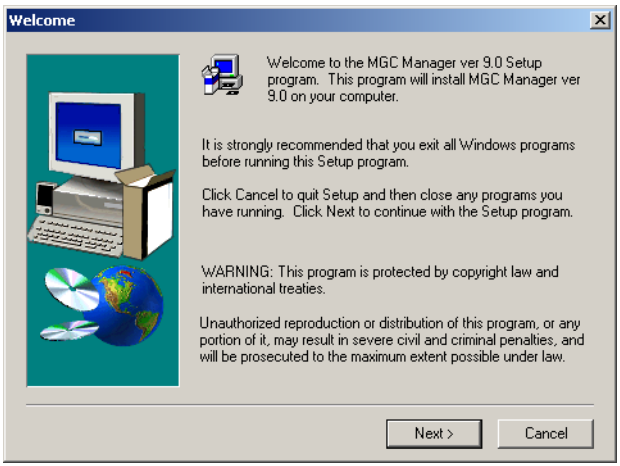


3. Type **D:\SETUP** (where D is the name of the CD drive) and click **OK**.

The installation wizard starts and the *Software License Agreement* window opens.

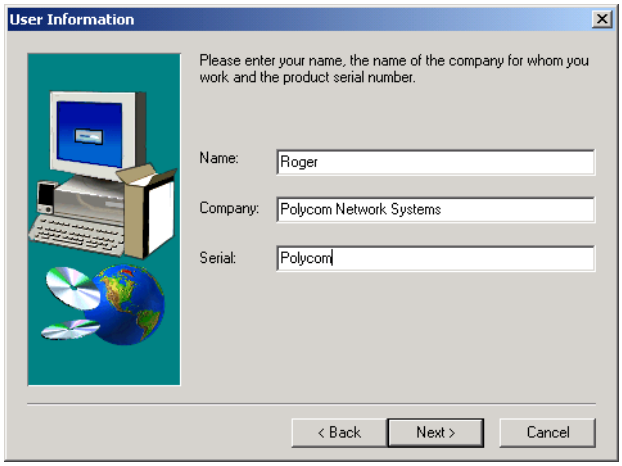
4. Click **Yes** to accept the software license terms.

   The *Welcome* screen opens.



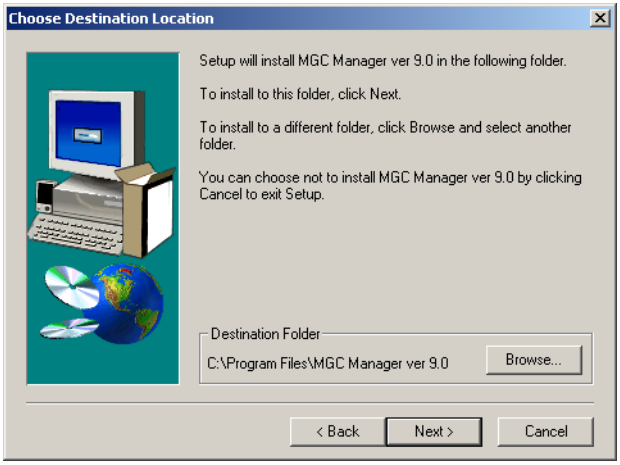
5. Read the notices and then click **Next**.

The *User Information* screen opens.



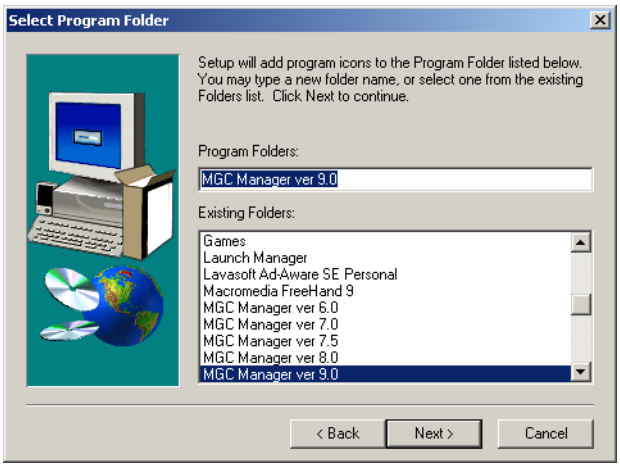
6. Type your name and the name of your company in the appropriate text boxes.
   For a standard installation, enter Polycom in the *Serial* box.
   Click **Next**.

   The *Choose Destination Location* screen opens.



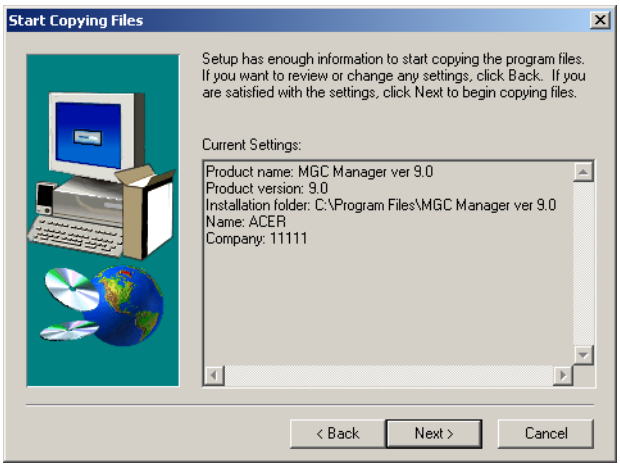
7. Select the directory in which to install the MGC Manager software. To accept the default directory, click **Next**.
   To change the directory, click **Browse**, choose the directory in which to install the software, and then click **Next**.

   The *Select Program Folder* screen opens.



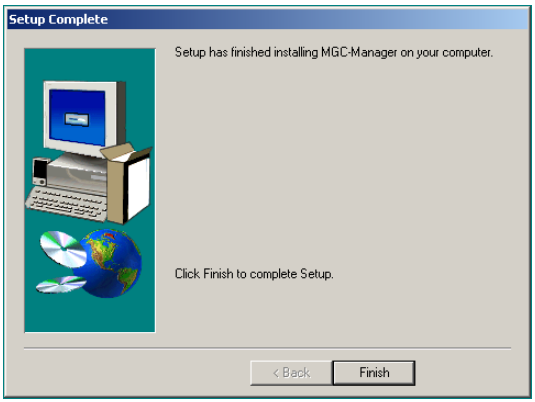
8. Select the Program folder in which to install the MGC Manager's icons. To accept the default folder, click **Next**.

   The *Start Copying Files* screen opens.



9. To change an installation setting, click **Back** until the appropriate screen appears. Click **Next** to start copying the files to your hard disk.

   When the installation procedure has finished, the *Setup Complete* screen opens.



10. Click **Finish**.
    The MGC Manager software is now installed on your computer.

First Entry IP Configuration

During the hardware installation process, a network IP address should have been assigned to the MCU. The IP address must be properly assigned to the MCU in order for the MGC Manager to connect to it. For more information about First IP Configuration on the MCU, refer the MGC Hardware and Installation Guide, Chapter 2.

Another method to connect to the MCU and modify its IP configuration is via a telephone line with a modem or directly via a serial connection. For details, see "Appendix B: PPP Setup".

MCU Definition

The MGC Manager can connect to several MGC unit simultaneously. The first time you run the MGC Manager application, or when a new MCU is added to your configuration, you must define the MCU's connection parameters to enable the communication between the MGC Manager and the MGC unit.

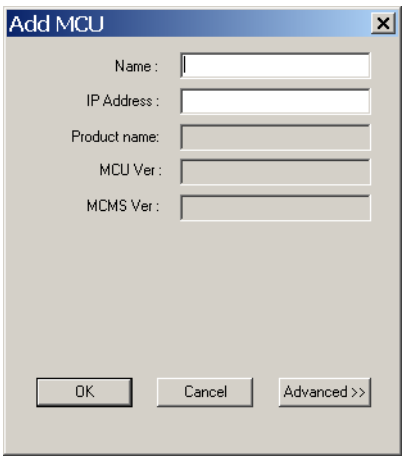
The MGC unit must be installed and its IP address properly configured before defining its connection parameters in the MGC Manager application.

To define an MGC unit in the MGC Manager application:

When opening the MGC Manager application, the *Reservations in AccordDB* window opens automatically. Click on any area of the *MGC Manager* window to move the *Reservations in Accord DB* window to the back.

1. In the MGC Manager *Browser* pane, right-click the *MCUs Network* icon, and then click **New MCU**.

The *Add MCU* dialog box opens.



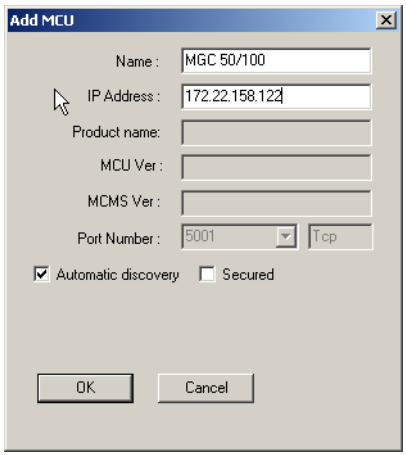
2. In the *Name* box, enter the name of the MCU. Specify a name that clearly identifies the MCU.
3. In the *IP Address* box type the IP Address of the MCU.

The IP address must be identical to the one configured in the MCU during first IP Configuration. For more details, see the MGC-25 Getting Started Guide, MGC+50/100 Getting Started Guide and MGC-50/100 Hardware and Installation Manual.

4. If you are not using a secured (TLS or SSL) connection between the MGC Manager and the MCU, and if you let the system automatically select the port for communication and data transactions between them, you can use the system defaults and end the MCU definition.

   Click **OK**.
5. To override the automatic port selection and manually define the port number between the MCU and the MGC Manager, click the **Advanced** button.

The *Port Number* field, and the *Automatic Discovery* and *Secured* check boxes, appear in the *Add MCU* dialog box.



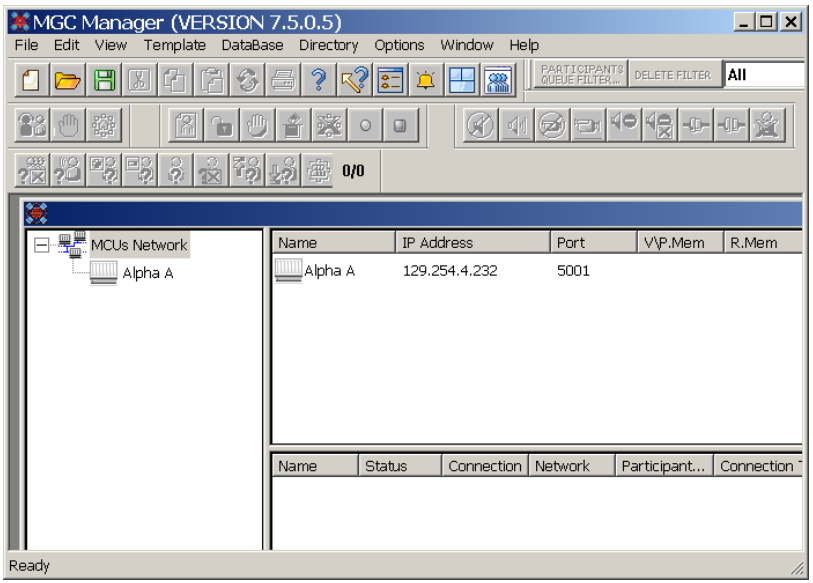
The *Port Number* field identifies the MCU port to which the MGC Manager initially connects. If the Automatic Discovery option is enabled, then after initially connecting to the MCU, the system checks the system configuration file (system.cfg) for the preferred port settings. The preferred port is defined in the GENERAL section of the system.cfg file, in the PREFERRED_PORT flag. If the preferred port differs from the currently connected port, then the system disconnects and reconnects using the preferred port and replaces the Port Number with the preferred port.

6. To manually define the *Port Number*, clear the **Automatic Discovery** check box.
7. In the *Port Number* field, select the listening port number from the drop down list. The default port number is 5001. The Internet Assigned Numbers Authority (IANA) has assigned port number 1205 to MCUs In new installations, it is recommended to select the IANA port (1205). If you are upgrading an existing installation and you do not wish to change the firewall configuration, use the default setting (5001).

To define a secured connection between the MGC Manager and the MCU, refer to "Defining a Secured Connection to the MCU" on page 2-10.

8. Click **OK**.

The *Add MCU* dialog box closes. A new icon with the specified MCU name appears in the *Browser* pane, below the *MCUs Network* icon.



9. To connect to an MCU, see the MGC Manager User's Guide, Volume I, Chapter 3, “Connecting to an MCU”.

Defining a Secured Connection to the MCU

TLS and SSL are used to provide a secure environment for connections between the MGC Manager, WebCommander and API applications and the MCU. TLS is the successor to the SSL and is a formal IETF standard.

The MCU supports TLS, SSL version 3 or SSL version 2 secured connections based on the client’s capabilities.

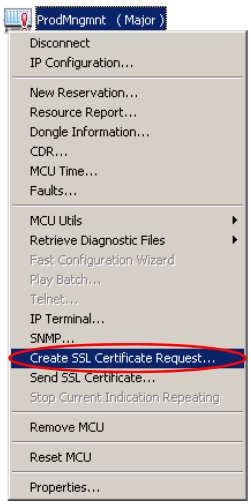
The External DB Application does not support the TLS protocol, and the MCU will continue to support their connection over the SSL v2.

A TLS or SSL Certificate is required to enable security for the MCU’s connection to external applications. TLS and SSL use a third party, that is the Certificate Authority, to identify HTTP transactions and secure them using the HTTPS protocol.

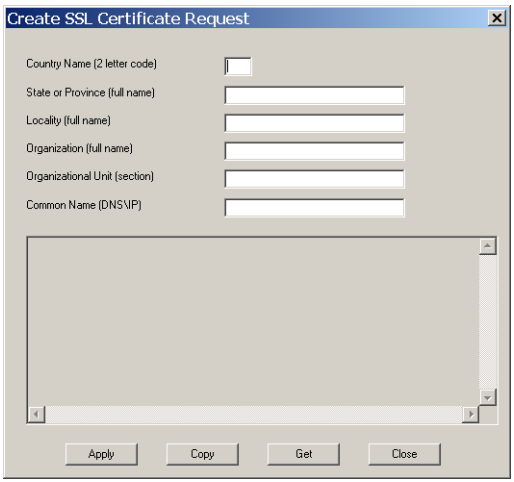
The TLS or SSL certificate must be obtained on first connection to the MCU, once the MCU is defined in the MGC Manager application.

To obtain the TLS or SSL certificate:

1. Connect to the MCU.
2. Right-click the unit's icon or name, and then click **Create SSL Certificate Request**. Use this option for both TLS and SSL requests.



The *Create SSL Certificate Request* dialog box opens, where you can enter data for the request and apply.

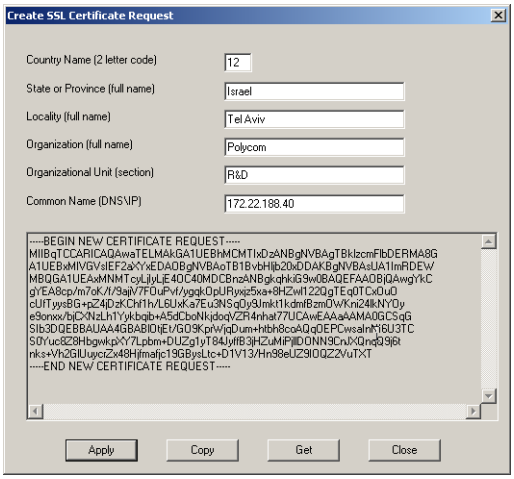


3. Enter information for all the following fields, as they are mandatory for the request:

Table 2-1: SSL/TLS Certificate Request - Required Information

Field	Description
Country	Enter any 2 letter code for the country name.
State or Province	Enter the full name of the state or province.
Locality	Enter the full name of the town/city/location.
Organization	Enter the full name of your organization for which the certificate will be issued.
Organizational Unit	Enter the full name of the unit (group or division) for which the certificate will be issued.
Common Name (DNS/IP)	Enter the DNS or the IP address of the MCU.

4. Click **Apply**.
   The new certificate request appears in the details box.

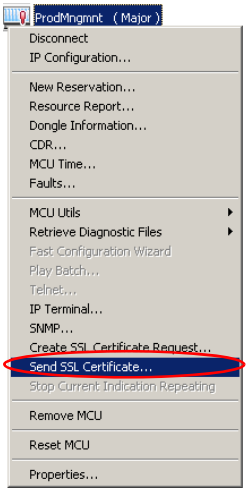


5. Click **Copy**, then click **Close.**
   For a previously defined MCU for which SSL or TLS has been obtained before, click **Get** to get the latest certificate request from the MCU.

6. In the browser, access your preferred certificate authority (for example, http://www.thawte.com and select from the *quick login* box: **Certificate Status**), paste the certificate request from MCU and submit.
   The authority issues the TLS/SSL certificate, and sends the certificate by text to you by E-mail.

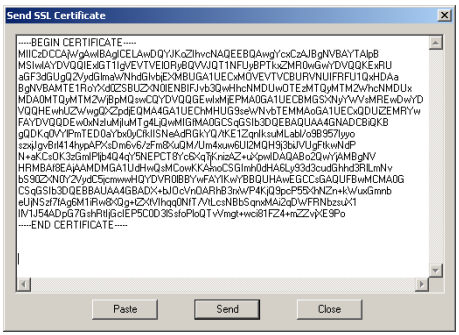
7. When the E-mail with the certificate arrives from the authority, select the text and click **Copy**.

8. Back in the MGC Manager application, right-click the MCU's icon and click **Send SSL Certificate**. Use this option for both TLS and SSL requests.



The *Send SSL Certificate* dialog box opens.

9. Paste the certificate's text in the *Send SSL Certificate* window.



10. Click **Send**.
    The MCU validates the certificate.
    - If the certificate is not valid, an error message appears.
    - If the certificate matches the private key, and the task is completed, a confirmation message indicating that the certificate was created successfully is displayed.

11. Reset the MCU.
    The system has access to the TLS or SSL-secured port 443.

    If the preferred port or preferred secured port differs from the currently connected port, then the system disconnects and reconnects using the preferred port or the preferred secured port, and replaces the Port Number with the preferred port or preferred secured port.

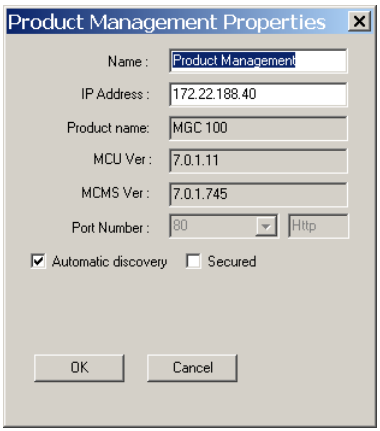
To enable a Mandatory and Secure connection to the MCU:

1. Before connecting the MCU, right-click the *MCU* icon and click **MCU Utils**, then click **Edit "system.cfg"**.
   The *SysConfig* dialog box opens.
2. In the GENERAL section, set the following flags:
   - SECURED_PORT_MANDATORY_FOR_API=YES
   - SECURED_PORT_MANDATORY_FOR_FILE=YES
   - PREFERRED_SECURED_PORT=443
3. Click **OK** and then reset the MCU.
4. Right-click the *MCU* icon and then click **Properties**.

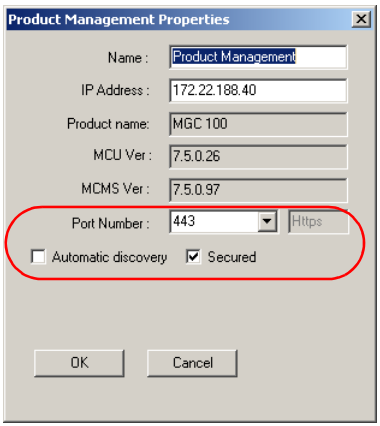
Do not connect to the MCU. When you right-click the MCU, the MCU should be disconnected and the icon appear grey.

The *Properties* dialog box opens.

5. Click **Advanced**.
   The *Port Number* field, and the *Automatic Discovery* and *Secured* check boxes, appear in the *Properties* dialog box.



6. Clear the **Automatic Discovery** check box.
7. In the *Port Number* box that is enabled, enter port **443**.
8. Select the **Secured** check box to enable mandatory security.



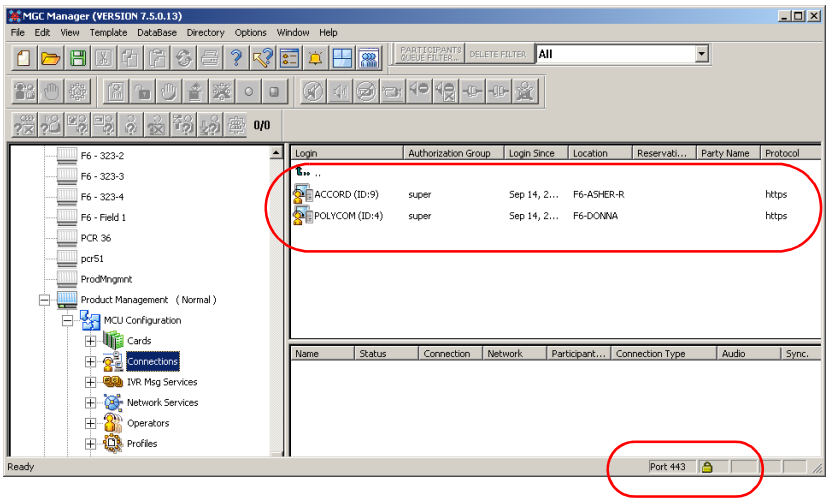
9. Click **OK**.

10. **Connect** to the MCU.
    When reconnected, the MCU uses the secured port.

After reconnecting, it is highly recommended to change the login password.

Viewing the MCU Connection Type in the MGC Manager Application

When mandatory security is enabled, on first connection after the reset, the MCU will automatically use only the preferred TLS/SSL-secured port 443, and the HTTPS protocol. The HTTPS protocol is indicated in the *Connections* list *Protocol* column under the *MCU Configuration* icon. Port 443 and the *Secured* (the lock) icon are indicated in the MGC Manager window's status bar.



MGC Configuration - Setting the MCU Date and Time

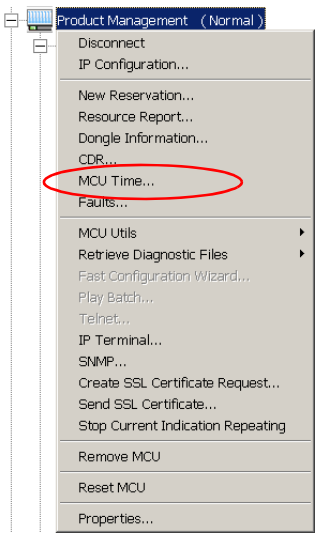
The first time you install the MCU, if you are moving the MCU to a different location, or if the MCU is located in a different time zone from the MGC Manager, you have to set the MCU date and time to synchronize the MGC Manager.

The time format used in the MGC Manager is taken from the Operating System installed on the PC running the MGC Manager. This allows 12-hour AM/PM and 24-hour formats to be used.

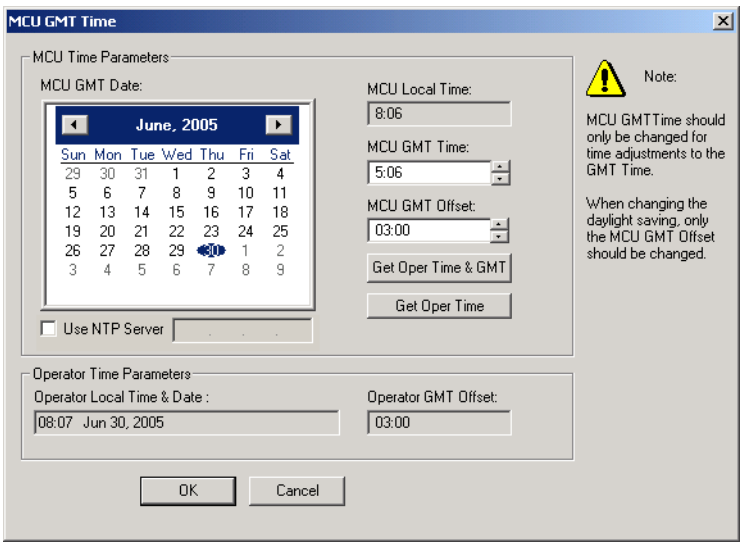
You can set the MCU time manually, or automatically either by updating it according to the MGC Manager application or synchronizing it with an external NTP server. The synchronization with an external NTP server is available only for MCUs with XPEK operating system and it enables accurate time calculation that is essential for cascaded or recurring conferences.

To set the MCU date and time:

1. Connect to the MCU.
2. Once connected, right-click the MCU icon, and then click **MCU Time**.



The *MCU GMT Time* dialog box opens.



The *Use NTP Server* check box and field is only displayed in XPEK Systems. You cannot set the MCU's time or connect to the NTP server, when there are On Going conferences on the bridge.

3. The following fields are available:

Table 2-2: MCU GMT Time Options

Field	Description
MCU GMT Date	From the calendar, first select the month/year and then click the day of the month.
MCU Local Time	Displays the MCU's current local time settings. The local time is calculated according to the MCU GMT Time and the MCU GMT Offset.
MCU GMT Time	Displays the MCU's current GMT time settings. To manually modify the GMT Time, click on the hours or minutes section of the time and either use the scroll arrows to change the value, or enter the new value.

Table 2-2: MCU GMT Time Options

Field	Description
MCU GMT Offset	Displays the currently defined time zone difference. To manually modify the GMT Offset, click on the scroll arrows to change the value, or enter the new value. **Note**: GMT offset can be set in minutes, for example: 5 hours and 45 minutes.
Get Oper Time&GMT	Click this button to automatically update the MCU's Date, Time and time zone to match the MGC Manager's date, time and time zone settings.
Get Oper Time	Click this button to automatically update the MCU's Time and Date to match the MGC Manager's time and date settings (without GMT offset).
Use NTP Server	This field is only applicable to XPEK systems. Select this check box to synchronize the time with an NTP server. Enter the IP address of the required NTP server.
Operator Local Time and Date	Displays the local date and time as set in the MGC Manager (this time is taken from the Windows operating system).
Operator GMT Offset	The time zone difference as set in the MGC Manager (this time is taken from the Windows operating system).

To set the time on the MCU using an NTP Server:

1. In the *MCU GMT Offset* box, enter the time difference between the MCU Local Time and MCU GMT Time.
2. Select the **Use NTP Server** check box, and enter the IP address of the NTP server.
3. Click **OK**.
   NTP Server synchronization may take up to an hour. All time-related settings, such as the scheduled Starting Time of Reservations, are adjusted.

To set the time on the MCU automatically, using the MGC Manager time settings:

1. **C**lick the **Get Oper Time&GMT** button or **Get Oper Time** button.
2. Click **OK**.

To set the time on the MCU Manually:

1. In the *MCU GMT Time* box, enter the appropriate MCU GMT time by either clicking on the scroll arrows to change the value, or retyping the new value.
2. Set the *MCU GMT Offset* (hours), by clicking the scroll arrows to change the value, or retyping the new value.
3. Click **OK**.

Modifying the MCU Local Time for Daylight Savings

To modify the *MCU Local Time* for daylight savings:

1. In the *MCU Time* dialog box, change the *MCU GMT Offset.*

   The MCU local time will be changed accordingly. For example, if the *Local MCU Time* shows 11:00 and the *MCU GMT Offset* is set to 2, changing the *MCU GMT Offset* to 1 will change the *MCU Local Time* to 10:00. The *MCU GMT Time* will remain unchanged.
2. Click **OK**.

MGC Unit Software Installation

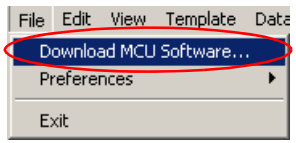
When upgrading the software from a previous version, you need to download the new MCU version to the MCU unit. This process may also be required when replacing or upgrading the control unit of the MCU.

A pre-download check is performed to ensure a successful software installation.

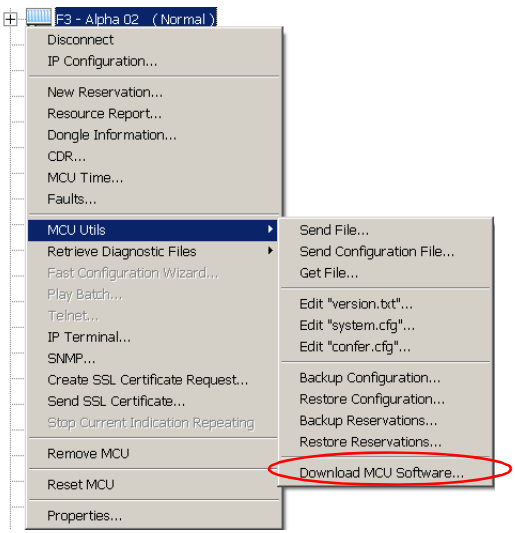
Before you upgrade the MGC unit software, it is important to backup all reservations in the MCU. This is to safeguard against reservations being lost. For more details, see Chapter 5, “Backing up Reservations” on page 5-112.

To install the MCU software:

1. Select the MCU to which you want to download software.
2. On the *File* menu, click **Download MCU Software.**



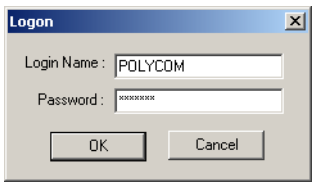
Alternatively, right-click the *MCU* icon, click **MCU Utils**, and then click **Download MCU Software**.



A message is displayed reminding you that you must have a valid dongle attached to the MCU.

3. Click **OK**.

   The *Logon* dialog box opens.

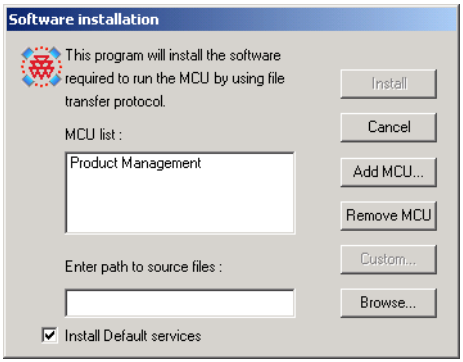


   The *Login Name* and *Password* of the current logged in operator are entered by default. If required, enter another login name and password.

4. Click **OK** to login or **Cancel** to continue without logging in.

   If you have selected *Cancel*, a message is displayed indicating that connection will be established without login. Click **YES** to continue.

   The *Software Installation* dialog box opens, with the selected MCU displayed in the *MCU List* box.



5. Select the **Install Default Services** check box to download the default IVR Service and Entry Queue Service. The default IVR Service is in English and is named **IVR90**. The default Entry Queue Service is in English and is named **EQ90**. You can manually install the default English IVR Service and Entry Queue Service or the English and Spanish IVR and Entry Queue Services. For more information, see "Manual Installation of the Default Message Services" on page 2-30.

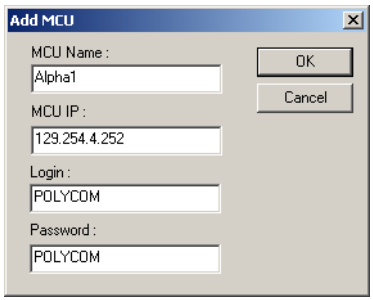
6. You can download software to all MCUs listed in the *MCU List* in one operation.

   Make sure that all MCUs to update appear in the *MCU List*.

   To add an MCU to the list:

   a. Click the **Add MCU** button.

      The *Add MCU* dialog box opens.



   b. In the *MCU Name* box, type the name of the MCU.

   c. In the *MCU IP* box type the IP address of the MCU.

   d. The *Login* and *Password* fields are filled with the login name and password of the logged in operator.

   e. Click **OK**.

      The *Add MCU* dialog box closes and the name of the MCU is added to the *MCU list*.

   To remove an MCU from the list:

   a. In the *MCU List*, click the MCU to remove.

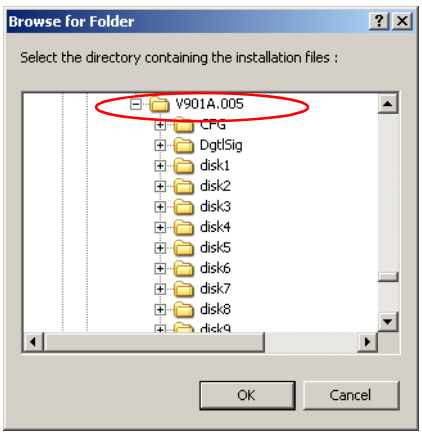
   b. Click the **Remove MCU** button.

      The MCU Name is removed from the *MCU List*.

7. In the *Enter path to source files* box, type the full path to the folder containing the software version. Alternatively, click the **Browse** button and use the standard Windows techniques to select the **Folder** containing the software.

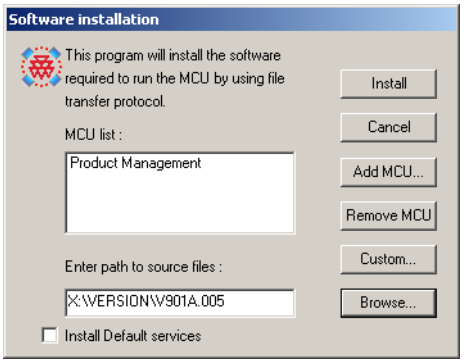
This folder is named Vaaa.bbb, where aaa is the MGC Manager version number, and bbb is the MCU version number.

You need to select the folder containing the latest version number, and not the sub-folder labeled Disk 1.



8. Click **OK**.

   The software version's path is displayed in the *Enter path to source files* box.



9. To install only selected files, do the following:
   a. Click the **Custom** button.

      The *Custom* dialog box opens listing the files that can be installed on the MCU. All the files are checked (selected). Only checked files are copied to the MCU.
   b. To change the selection of all files, click **Toggle All**.
   c. Select the check box of a file to select or clear its selection.
   d. When you are finished selecting the files you want to install, click **OK**.

      The *Custom* dialog box closes and you are returned to the *Software Installation* dialog box.
10. Click the **Install** button to start the installation procedure.

    A pre-download check is performed to ensure a successful software installation. If no problem is detected, the installation procedure is completed. If the pre-download check detects a problem, the installation procedure is halted, and the following error messages and possible solutions are displayed:

Table 2-3: Software Pre-download Checks

Pre-download test	Error Message	Solution
Verifying that a dongle is installed	"You must have a valid dongle attached to the MCU before downloading MCU software version 5.02 and later."	Verify that the dongle is installed on the MCU. Contact the Polycom support team to have a dongle shipped.
Verifying the software version suits the MGC type MGC-50/100 vs. MGC-25	"Software is not supported on this MGC type."	Download the appropriate version of the software from the CD or the Polycom Resource Center.

Table 2-3: Software Pre-download Checks (Continued)

Pre-download test	Error Message	Solution
Verifying that the installed dongle version enables the use of the new software version	"Dongle doesn't support the version. Please upgrade the dongle before downloading the version."	Contact Polycom's Resource Center and download the upgrade file for the dongle.
Verifying that there is sufficient space on the MCU's hard disk	"There is not enough space on your hard disk to install the version. A minimum of 130 MB required."	Contact the Polycom support team.

- After you have successfully installed the latest software version, it may be necessary to restore the backed up files. For more information on backing up and restoring reservations, see Chapter 5, "Reservations Backup and Restore" on page 5-112.
- When you upgrade the MCU's software, the existing card configuration files are automatically restored.
- If you are upgrading from version 5.x or 6.x, after the completion of the upgrade process, you must manually update the existing Entry Queue Services by adding the voice message files prompting for the conference Numeric ID, otherwise the participants are placed on hold and cannot move to the target conferences.

11. If you have installed the Default Services during the MCU Software installation and you do not need to manually install additional Message Services (such as the Spanish IVR Message Service), reset the MCU at the end of the MCU software installation process.

Dongle Information

The MGC-50/100 is shipped with a serial dongle installed on COM1 of the rear panel. The MGC-25 is shipped with a serial dongle installed on parallel port of the rear panel.

To verify if you have a dongle your are required to inspect the rear panel of the MCU as shown in Figure 3.

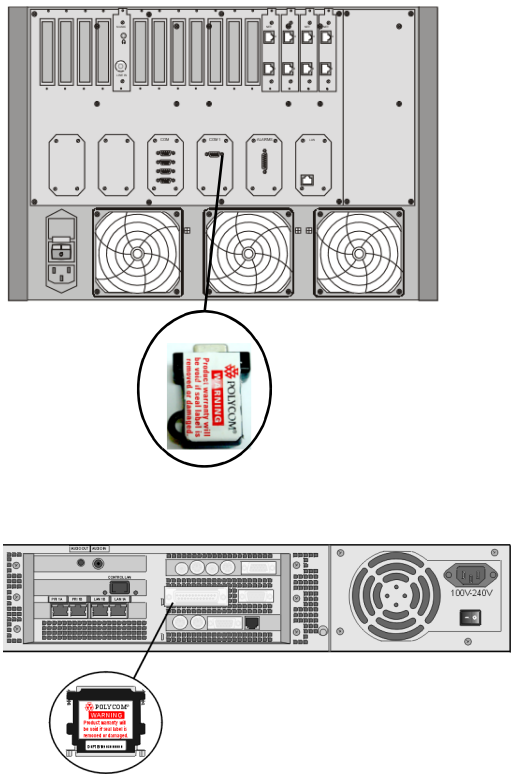


Figure 3: MCU-100 & MCU-25 rear panels and their dongles

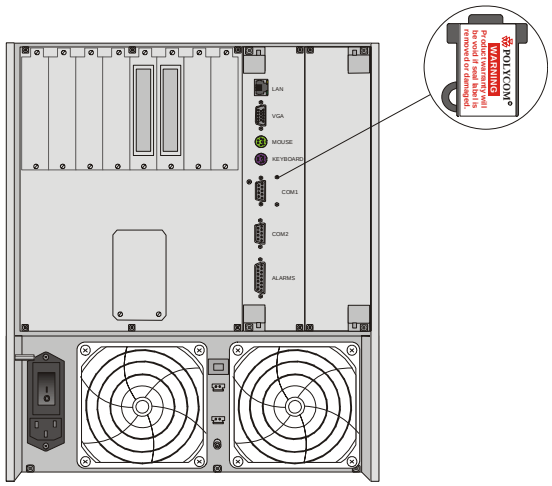


Figure 4: MCU+ 50 rear panel and dongle location

The dongle on the MGC+ 100 is located in the identical location. On both the MGC+ 50/100, an additional bracket is installed together with the dongle. For more information on the installation and removal of the dongle on the MGC+ 50/100, refer to the MGC+ Hardware and Installation Manual.

The Dongle was introduced on the MCU and MGC Manager in version 5.02. Each dongle installed on the MCU is backward compatible with current or previous MGC Manager versions.

Only customers with an active Polycom Premier Family Maintenance Agreement are entitled to upgrade a version for free.

When upgrading the MGC Manager version, you are required to upgrade your Dongle. For details of the dongle upgrade procedure, refer to the Release Notes of the relevant version.

Manual Installation of the Default Message Services

The MGC software kit is shipped with the voice messages required for the default Entry Queue Service and the default IVR Message Service. These messages can be automatically installed on the MCU during the software installation. You can also manually install the default Message Services at the end of the installation process.

The MGC software and documentation CD contains two IVR Service folders:

- English
- English and Spanish

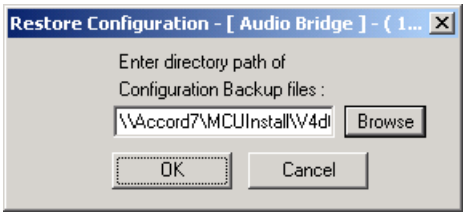
The Automatic installation of Message services during MCU software update automatically installs the English only Message services. The manual installation process enables you to install the English and Spanish Message Services as well as the English only. When you install the English and Spanish IVR Services, two separate IVR Services are created on the MCU and the English IVR Service is automatically set as the default IVR Service.

To restore the Default IVR Service:

The default Message Services are installed using the *Restore Configuration* utility.

Restoring the IVR Services overwrites existing IVR Services.

1. Right-click the *MCU* icon, click **MCU Utils**, and then click **Restore Configuration**.
   The *Restore Configuration* dialog box opens.

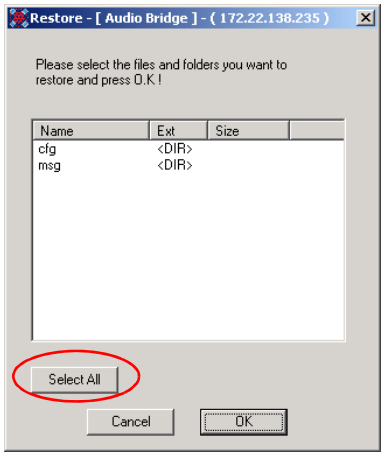


2. Enter the path to the folder containing the configuration files to be installed, or click the **Browse** button to locate them.

If you have selected Browse, the *Browse for Folder* dialog box opens, enabling you to select the source folder.

3. From the version 8.0x software folder, select **English V90 IVR** or **English and Spanish V90 IVR** folder, according to the required Message Service, and click **OK**.
   The system returns to the *Restore* dialog box.
4. Click **OK** to continue.

   The *Restore* dialog box is displayed.



   The system lists the configuration folder (*CFG* box) and the audio files (*Msg* box) used in the IVR Service.
5. Click the **Select All** button.
6. Click **OK** to install the default Message Services on the MCU.
7. At the end of the Restore process, a message is displayed indicating that the MCU must be reset to be able to use the new Message Services.
8. Click **OK** and reset the MCU.

After the completion of the upgrade process, you must manually update the Existing Entry Queue Services by adding the voice message files prompting for the conference Numeric ID, otherwise the participants are placed on hold and cannot move to the target conferences.

Command Line Launch

The MGC Manager can be launched by other applications using the Command Line Instruction.

When accessing the MGC Manager from an external application, the application must read the ".exe" file name stored in the Windows registry. After reading the file and version name, the IP address, MCU name, user login name and password are added.

Windows Registry Access

The Windows Registry uses the following format:

HKEY_LOCAL_MACHINE \ SOFTWARE \ POLYCOM \ MGC_MANAGER \ Versions\VerX.Y

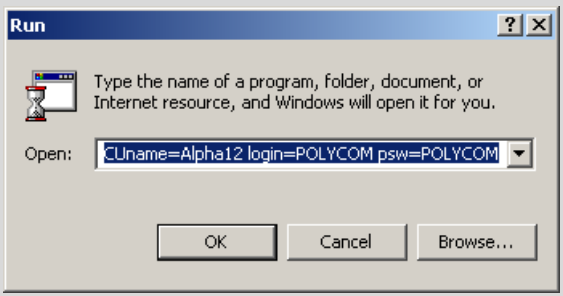
MGC Manager launch format requires the full path and name of the specific MGC Manager version, including IP, MCU name, User login and password. For example:

c:\ProgramFiles\MGCManager\OperWS.exe ip=172.22.168.135 MCUname=Alpha12 login=POLYCOM psw=POLYCOM

Spaces (character) are forbidden between the argument name, the '=' character and the version value.

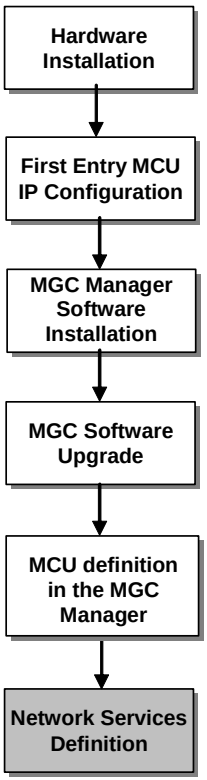
Activate the application and connect. When the MGC Manager window opens, a single MCU is displayed.

The MGC Manager can be activated using the Windows *Start* menu as illustrated in the *Run* window:



3

Defining Network Services



Providers of communication services such as telephone carriers use different communication protocols, lines, equipment and configurations. This can be true even in different regions of the same country.

The MGC unit is designed to work with different service providers/ communication lines. In particular, the MGC unit can be connected to any public or private network that supplies ISDN lines, ISDN leased lines, T1–CAS lines, ATM connections or IP connections. These include long distance carrier services and local area services. In addition, the MGC unit may be connected to a serial network using the MPI serial network interface card.

To enable the MCU to connect participants using any of the following networks: ISDN, PSTN, T1-CAS, ISDN-NFAS, ISDN-Leased Lines, IP, serial connection (MPI) and ATM, the network parameters must be defined in the Network Services. You must also set up the network parameters whenever you:

- Connect the MGC unit to a switch in a new site
- Add a new switch to an existing site
- Add ISDN/T1–CAS lines to the system
- Connect the MGC to an additional LAN zone
- Change the network properties

Only MGC Manager operators with Superuser rights can perform MGC Manager configuration tasks. In addition, the user must have Superuser rights on the computer on which the MGC Manager application is running, or any other permission than enables the application to access the Registry (read/ write) and read/write files on the C: drive (root directory), under the Windows directory folder.

ISDN Network Service

The Net-2/4/8 Network card installed in the MCU interfaces between the MGC unit and the ISDN switch. The Network Service is used to define the properties of the switch and the ISDN lines running from the switch to the ISDN Network card. Each group of ISDN lines having the same characteristics and originating from the same ISDN switch, will be assigned to the same Network Service. The ISDN Network Service is also used for connections via PSTN, leased lines and NFAS configuration of ISDN lines.

T1–CAS Network Service

The Net-2/4/8 Network card installed in the MCU interfaces between the MGC unit and T1–CAS lines. The T1–CAS Network Service is used to define the properties of the switch and the T1–CAS lines running from the switch to the Net-2/4/8 Network card.

IP (H.323 and SIP) Network Service

The IP Network Service defines the properties of the IP network and the IP cards (installed in the MCU) used for connecting IP (H.323 and SIP) endpoints to the conference. Several of the network components are used by both H.323 and SIP endpoints to connect to the conference, and the same IP card is used for H.323 and SIP connections.

ATM Network Service

The ATM Network card installed in the MCU interfaces between the MGC unit and the ATM Network (FVC), usually via a UNI address router (V-Gate). The Network Service is used to define the properties of the ATM switch and the V-Gate to which the MGC unit is connected.

MPI Serial Network Service

The MGC unit may be connected to endpoints over a serial connection using the V.35, RS-449 and RS-530 serial standards. The MPI-8 Network Interface module together with the MPI box interfaces between the serial equipment and the MGC unit. The MPI Network Service is used to define the properties of the serial connections between the MGC unit and the data communication equipment.

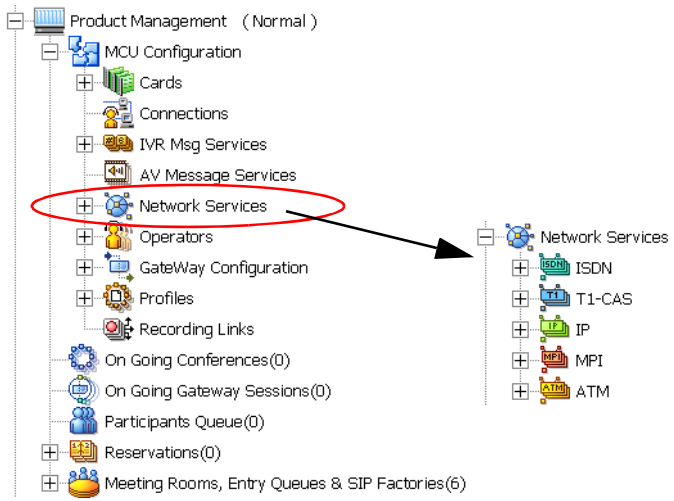
Defining an ISDN Network Service

The MCU may be connected to ISDN lines provided by different carriers. Each carrier has unique characteristics, and may have different pricing programs. To use these lines, together with the carrier's special programs, you need to first obtain the relevant information from the carrier and then define their parameters in the MGC Manager application.

To define a New ISDN Network Service connection:

1. Connect the MGC Manager to the MCU. For more information, see the MGC Manager User's Guide, Volume I, Chapter 3, "Connecting to an MCU".
2. In the *Browser* pane, expand the *MCU* tree.
3. Expand the *MCU Configuration* tree.
4. Expand the *Network Services* tree.

   The list of *Network Services* is displayed.



5. Right-click the *Network Services - ISDN* icon, and then click **New Network Service**.

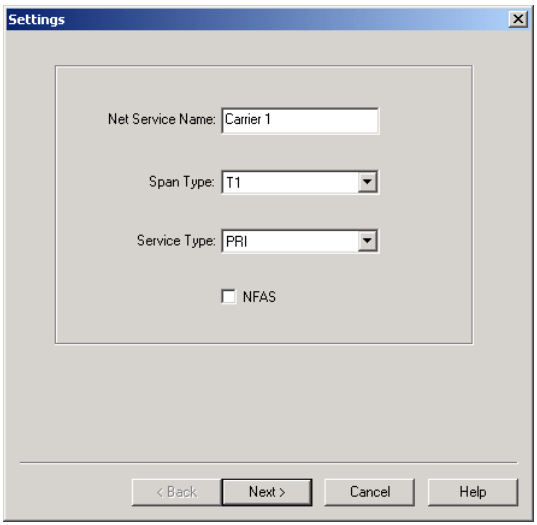
The *New Network Services* configuration wizard opens. The wizard displays a series of dialog boxes.

— To display the next dialog box, click on **Next**.

— To display the previous dialog box, click **Back**.

Settings Dialog Box

The first dialog box displayed by the wizard is used to identify the network service to the system.



6. Define the *Settings* parameters as follows:

Table 3-1: Settings Dialog Box Options

Field	Description
Net Service Name	Specify the service provider's (carrier) name or any other name you choose, using up to 20 characters. The *Network Service Name* identifies the service to the system.

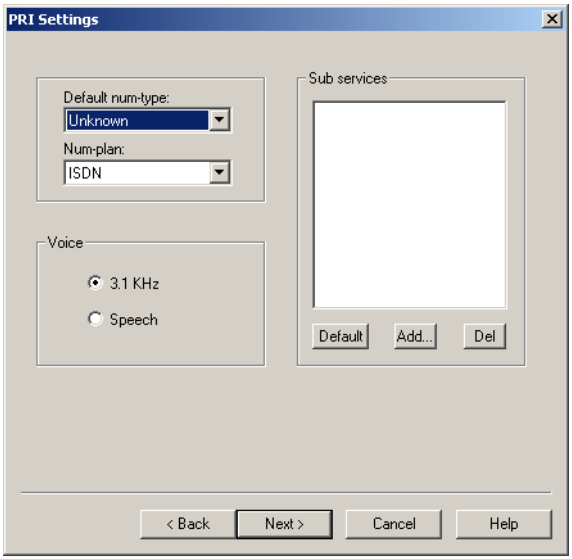
Table 3-1: Settings Dialog Box Options

Field	Description
Span Type	Spans are ISDN lines supplied by the service provider to the MCU. You can define each span as a separate Network Service, or you can define all the spans from the same carrier under the same Network Service. Select the span type from the drop-down list; select either **T1** (usually in the U.S., has 23 B channels + 1 D channel), or **E1** (usually in Europe, has 30 B channels + 1 D channel). The MCU may contain several network cards. A Net-E1/Net-T1 card may be connected to two spans; both spans must be of the same span type. A Net-2/4/8 card may be connected to 2, 4 or 8 spans respectively with both spans types connected to it.
Service Type	Select the service type from the drop-down list. The following options are available: • PRI (Primary Rate Interface) - default selection for all ISDN lines that are not leased lines • Leased-24 - leased line applicable to T1 lines • Leased-30 or Leased-31 - leased line applicable to E1 lines. For a detailed description of the ISDN Leased lines Network Service definition, see "Defining ISDN Leased Lines" on page 3-19.
*NFAS (*Non-Facility Associated Signaling)	Select the **NFAS** check box to define a network service using ISDN-NFAS lines. For more information on this option, see "Defining ISDN Non-Facility Associated Signaling (NFAS)" on page 3-24.

7. Click **Next**.
   The *PRI Settings* dialog box opens.

PRI Settings Dialog Box

The the *PRI Settings* dialog box enables you to define the properties of the PRI Service Type.



If you do not need to define a sub-service, you can use the defaults, and just click **Next** to display the subsequent dialog box.

8. Define the *PRI Settings* properties as follows:

Table 3-2: PRI Settings Dialog Box Options

Field	Description
Default num-type	The num-type defines how the system handles the dialing digits. For example, if you type eight dialing digits, the *num-type* defines whether this number is national or international. If the PRI lines are connected to the MCU via a network switch, the selection of the Num Type is used to route the call to a specific PRI line. If you want the network to interpret the dialing digits for routing the call, select **Unknown**.

Table 3-2: PRI Settings Dialog Box Options

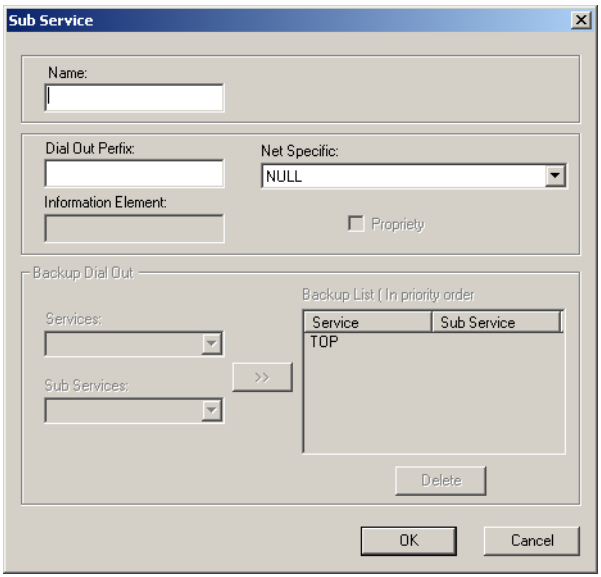
Field	Description
Num-plan	Set the type of signaling (Number Plan) that the MGC unit will use for this service—for example, ISDN or telex. Enter the number plan according to information given by the service provider. For video conferencing purposes, select **ISDN**.
Voice	Indicate the frequency of the data being sent. For practical purposes, the *Voice* option is set to **3.1 KHz** as it is the more widely used frequency. However, it is important to make sure that the system receiving the voice data is set to the same frequency as that of the data being sent.
Sub Services	Some service providers (carriers) may have several service programs that can be used. They may also use a backup service provider in case of malfunction in the ISDN network. You may define several service programs as sub-services and set one of them as the default. If the PRI lines are connected to the MCU via a network switch, the sub-service may be used to route the calls to a certain service provider. The *Sub-Service* list displays the list of currently defined sub services. To select the service program to be used for the PRI line channels, click the **Add** button. The *Sub-Service* dialog box opens. To remove a service program from the list, highlight it in the list box and click the **Del** button. The selected sub-service is removed from the list. To set a service program as the default, highlight it in the list box and click the **Default** button. The selected sub-service becomes the default service program for the current service provider. The word "default" appears in parentheses next to the sub-service's name. To edit the parameters of a sub-service, double-click its name in the sub-services list. The *Sub-Service* dialog box opens.

9. If you are not defining a sub-service or if you have completed the sub-service definition, click **Next** to continue.
   The *Span Definition* dialog box opens.

Defining Sub-Services

10. This step is required only if your ISDN network includes a sub-service, otherwise, skip these steps.

    In the *PRI Settings* dialog box, in the *Sub Services* section, click the **Add** button to add the sub-service, or double-clicked the Sub Service name to edit its parameters. The *Sub Service* dialog box opens.



a. Fill in the *Sub Service* dialog box as follows:

Table 3-3: Sub Service Dialog Box Options

Field	Description
Name	Type the name of the sub-service using up to 20 characters. This name identifies the sub-service.
Dial-out Prefix	Type the prefix that your PBX needs to dial out in order to use this service program. Leave this field blank if a dial-out prefix is not required.

Table 3-3: Sub Service Dialog Box Options

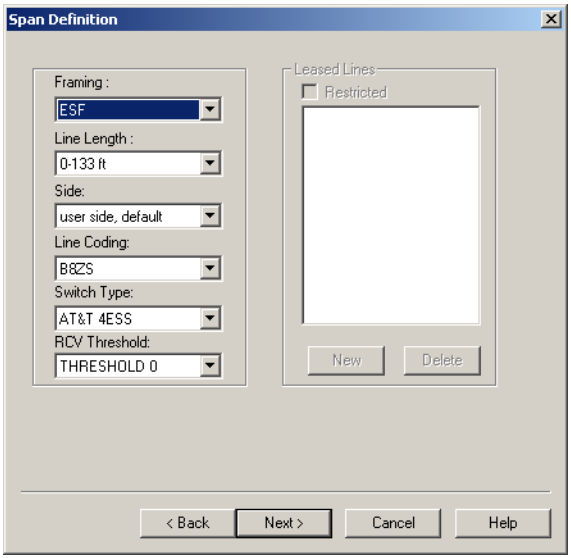
Field	Description
Information Element	For future release.
Net Specific	Select the desired service program from the drop-down list. The service programs are listed according to the service providers. If no special specification is required, select the **NULL** option.
Backup Dial-Out	For future release.

b. Click **OK**.
The *Sub Service* dialog box closes and you are returned to the *PRI Settings* dialog box.

c. Click **Next**.
The *Span Definition* dialog box opens.

Span Definition Dialog Box

The *Span Definition* dialog box is used to define the PRI span technical properties. The default values displayed for the Span's technical parameters are appropriate for most ISDN networks, therefore, you can skip their definition by clicking Next to move to the subsequent window. If you do not know the technical properties of your span, try these values first.



The *Leased Lines* section of this dialog box is disabled, unless you have specified Leased Lines as the *Service Type* in the *Settings* tab. For more details about Leased Lines definition, see "Defining ISDN Leased Lines" on page 3-19.

11. Define the *Span Definition* properties as follows:

Table 3-4: Span Definition Dialog Box Options

Field	Description
Framing	Framing refers to the frame format used by the carrier for the network interface. Select the appropriate option from the drop-down list.

Table 3-4: Span Definition Dialog Box Options

Field	Description
Framing (cont.)	If a span type of T1 is specified in the *Settings* dialog box, the following Framing values are available: • ESF (Extended Super Frame format of 24 frames, which provides enhanced performance). This is the system default • ESF ZBTSI • SF SLC96 • SF If a span type of E1 is specified in the *Settings* dialog box, the following framing values are available: • CRC4 Si = FEBE (default) • CRC4 Si = 1 • BASIC, noCRC4
Line Length	Indicates the distance between the MCU and the PBX. Select the desired option from the drop-down list. If T1 is specified as the span type in the *Settings* dialog box, the following *Line Length* values are available: • 0-133 ft. (0.0 dB) • 133-266 ft. (-7.5 dB) • 266-399 ft. (-15.0 dB) • 399-533 ft. (-22.5 dB) • 533-655 ft. (-30.0 dB) If E1 is specified as the span type in the *Settings* dialog box, the *Line Length* value is 0 by default.

Table 3-4: Span Definition Dialog Box Options

Field	Description
Side	Select the desired option from the drop-down list. The following options are available: • User side (default) • Network side • Symmetric side **Note:** If the PBX is configured on the network side, then the MGC unit must be configured as the user side, and vice versa, or both must be configured symmetrically.
Line Coding	Indicates how the bits are sent on a PRI line. Select the desired option from the drop-down list. If T1 is specified as the span type in the *Settings* dialog box, the following *Line Coding* values are available: • B8ZS (default) - Bipolar 8-Zero Substitution • B7ZS • AMI - Alternate Mark Inversion with zero code suppression The difference between these modes is the way eight consecutive zeros enabling information synchronization are encoded. If E1 is specified as the span type in the *Settings* dialog box, the following *Line Coding* values are available: • HDB3 (default) - Fours zeros are replaced by a code • AMI - Alternate Mark Inversion with zero code suppression

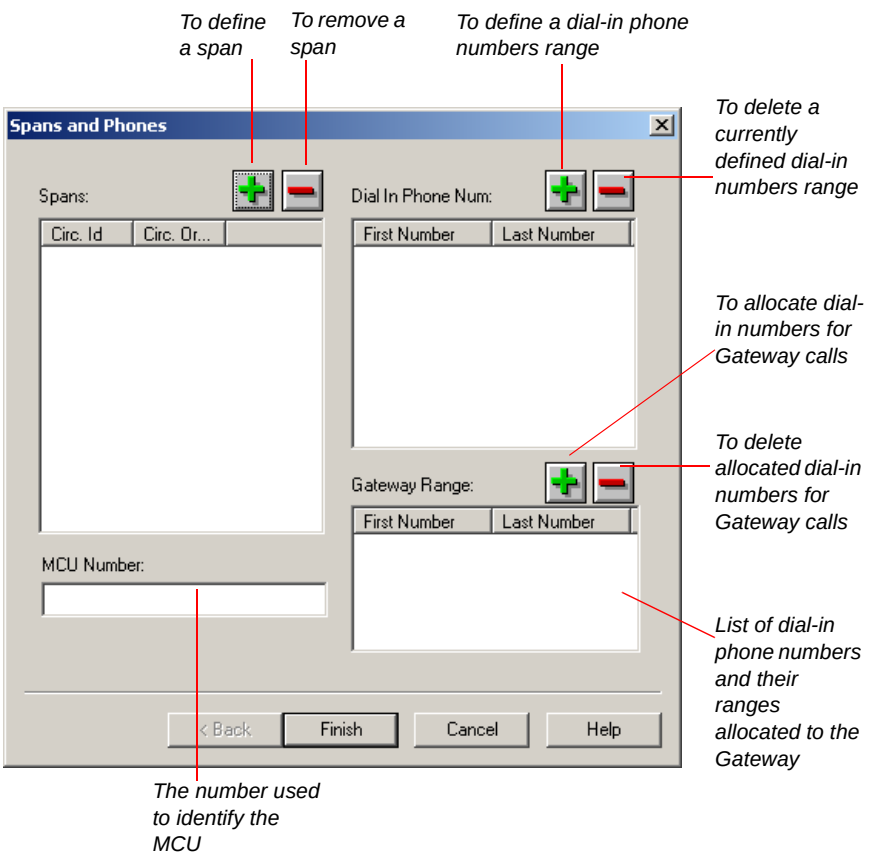
Table 3-4: Span Definition Dialog Box Options

Field	Description
Switch Type	Select the desired brand and revision level of equipment installed in the telephone company's central office. The following *Switch Types* are available for T1: • AT&T 4ESS • AT&T 5ESS • Northern Telecom DMS-100 • Northern Telecom DMS-250 • Ericsson MD110 U.S. • Siemens U.S. • NI-1 • NI-2 The following *Switch Types* are available for E1: • Ericsson MD110 International • Euro ISDN
RCV Threshold	RCV Threshold refers to the minimum detectable signal in a T1 or E1 span on the Net-2/4/8 card FALC component. This option is used to increase the signal on E1 or T1 spans when the system detects a very low signal. Select the desired threshold values from the list. The following values are available: • THRESHOLD 0 (by default) • THRESHOLD 1 • THRESHOLD 2 • THRESHOLD 3 **Note:** When you modify the threshold values a warning is displayed, advising you to obtain authorization from system support. Click **OK** to confirm the modification.
Leased Lines	The Leased Lines list is enabled when you select **Leased** as the Service Type in the *Settings* dialog box. For more information on how to configure the leased line connection, see "Defining ISDN Leased Lines" on page 3-19.

12. Click **Next** to continue.
    The *Spans and Phones* dialog box opens.

Spans and Phones Dialog Box

This dialog box is used to assign circuit identification numbers and the dial-in phone number ranges to be used in dial-in conferences. Circuit orders are automatically assigned to spans. The dial-in phone numbers are allocated to the MCU by your service provider (carrier) and should be obtained from the service provider. You specify the range of dial-in numbers in the *Spans and Phones* dialog box by entering the first and last numbers in the range. You can define several ranges for the same span.



13. Define the *Spans and Phones* parameters as follows:

Table 3-5: Spans and Phone Dialog Box Options

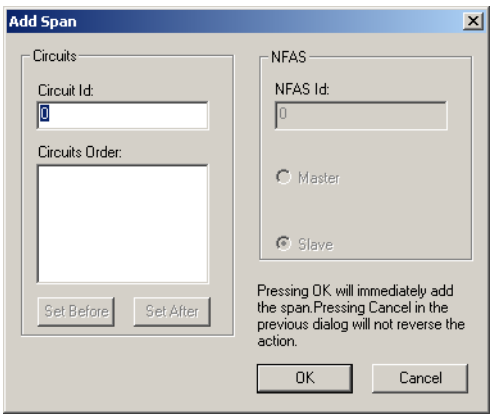
Field	Description
Span	Displays the existing definitions of circuit identification numbers and circuit orders. If only one service provider is used, define all the PRI lines here. For each span that is connected to the MCU and is included in this Network Service, click the Plus button to define the new spans. The Add Span dialog box opens. For more details see Table 3-6 on page 3-16.
Dial In Phone Num	Lists the phone numbers that will be used for dialing in, as allocated to the MCU by the service provider. To define additional dial-in number ranges see "Defining Dial-In Numbers" on page 3-17.
MCU Number	Type a number that will identify the MCU when calling the participants in dial-out conferences. This number should be obtained from your system administrator. The MCU Number is also used in conferences when the Meet Me Per MCU option is selected as the connection type for participants.
Gateway Range	Displays the dial-in numbers allocated to Gateway calls. Click the Plus button to allocate dial-in ranges to the gateway. The *Gateway Phone Numbers* dialog box opens. For more details see "Defining the Gateway Range" on page 3-18.

If you have selected the *NFAS* option in the *Settings* dialog box, an additional field is displayed in the Spans list. See "Defining ISDN Non-Facility Associated Signaling (NFAS)" on page 3-24.

Defining Spans

14. To assign circuit identification numbers and orders:
    a. In the *Spans* pane of the *Span and Phone* dialog box, click the **Plus** button.

The *Add Span* dialog box opens.



b. Define the *Circuit ID* parameters:

Table 3-6: Add Span Dialog Box Options

Field	Description
Circuit ID	The Circuit Identification is a logical number used to identify the span to the MGC Manager. This number is later used to assign the span to the network card. Enter any positive integer from 0 to 65535, to be used as the circuit identification number in the MGC Manager. **Note:** If other services are already defined, make sure to use numbers other than those already assigned to the existing services.
Circuit Order	The Circuit Order determines the order in which the MCU uses the spans to dial out. The Circuit Order is assigned automatically by the system according to the order in which the spans are added. In dial-out connections, when the operator calls the participant, the MGC unit allocates ports from the spans starting with the span having the lowest number and the lowest port number within that span.

c. Click **OK**.

The *Add Span* dialog box closes and you are returned to the *Spans and Phones* dialog box.

To delete a circuit identification entry:

- In the *Spans* pane, click the Circuit Identification entry you want to delete and then click the **Minus** button.

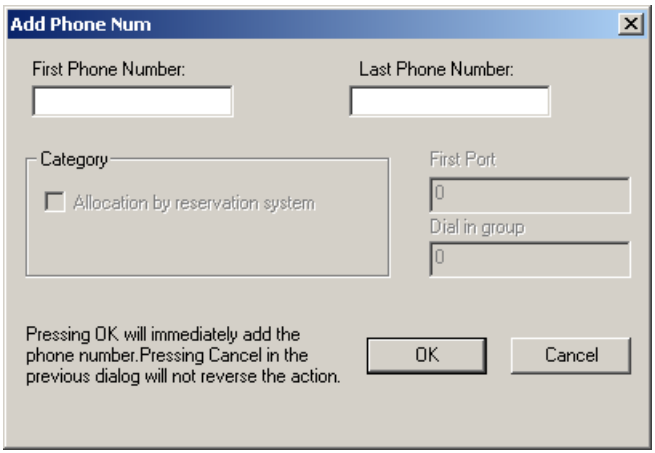
  The entry is deleted.

Defining Dial-In Numbers

15. You specify the range of dial-in numbers by entering the first and last numbers in the range. You can define several ranges for the same span. To define the dial-in numbers range:

    a. In the *Spans and Phones* dialog box, in the *Dial In Phone Numbers* section, click the **Plus** button.

    The *Add Phone Num* dialog box opens.



    b. In the *First Phone Number* box, enter the first number in the range of dial-in numbers.

    c. In the *Last Phone Number* box, enter the last number in the range of dial-in numbers.

    d. Click **OK**.

The dialog box closes. You are returned to the *Spans and Phones* dialog box. The number range appears in the *Dial-In Phone Numbers* list.

e. Repeat steps a-d for each number range you need to enter.

To delete a dial-in number entry:

- In the *Dial In Phone Number* section, click the entry to delete and then click the **Minus** button.
- Click **Yes** when prompted to confirm the deletion.

  The entry is deleted.

Sorting the dial-in number list:

You can change the order in which dial-in phone number entries are displayed by doing the following:

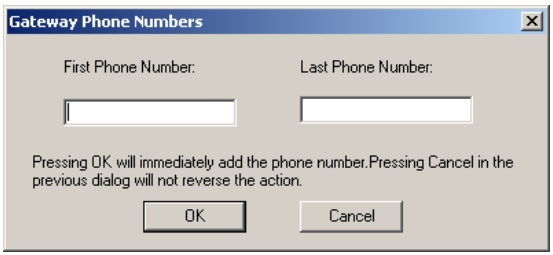
- Click the *First Number* heading to sort the list in ascending order according to the First Number value of the entries.
- Click the *Last Number* heading to sort the list in ascending order according to the Last Number value of the entries.

Defining the Gateway Range

16. The dial-in numbers to be used for Gateway connections are allocated to the MCU by your service providers. The range of dial-in numbers allocated to Gateway calls must differ from the dial-in number ranges allocated to multipoint conferencing. To define the Gateway dial-in numbers range:

    a. In the *Spans and Phones* dialog box, in the *Gateway Range* section, click the **Plus** button.

    The *Gateway Phone Numbers* dialog box opens.



b. In the *First Phone Number* box, enter the first number in the range of gateway dial-in numbers.

c. In the *Last Phone Number* box, enter the last number in the range of gateway dial-in numbers.

d. Click **OK**.
The dialog box closes. You are returned to the *Spans and Phones* dialog box. The number range appears in the *Gateway Range* list.

Completing the ISDN Network Service Definition

Once you have finished filling in all the Wizards screens, click the **Finish** button in the *Spans and Phones* dialog box.

The data you have specified will be validated, after which the ISDN Network Service will be added to the list of ISDN network services of the MCU.

Defining ISDN Leased Lines

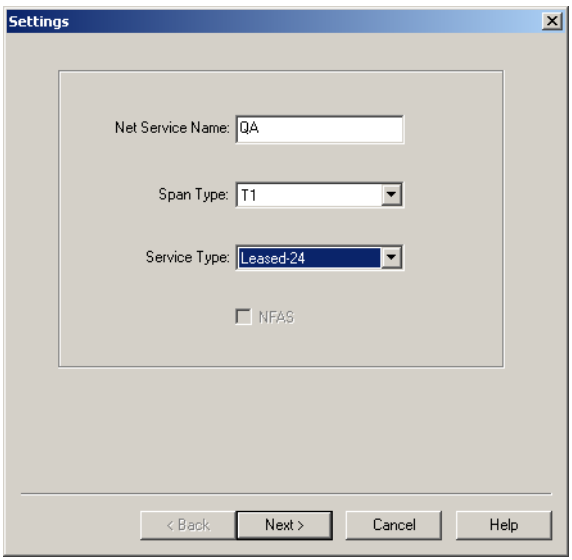
With Leased lines two or more ports are dedicated to one endpoint, depending on the required Line Rate. Each port provides a line rate of 64 Kbps. When using Line Rates of 128 Kbps, two ports will be assigned to the endpoint with leased lines. The endpoint connects directly to the conference, once the connection is initiated.

1. Expanded the *MCU Configuration* tree.

1. Expanded the *Network Services* tree.

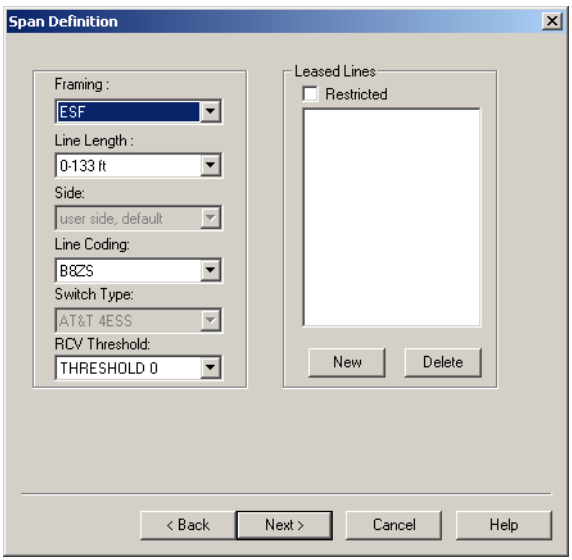
2. Right-click the *Network Services – ISDN* icon, and then click **New Network Service.**

The *Network Service* wizard displays the *Settings* dialog box.



3. Define the *Net Service Name* and *Span Type* as you would for a standard line. For details, see “Settings Dialog Box” on page 3-4.
4. In the *Service Type* list, select **Leased-24** for T1, or **Leased-30**/ **Leased-31** for E1.
5. Click **Next** to continue.

The *Span Definition* dialog box opens.



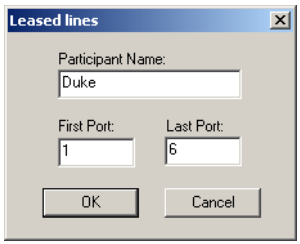
6. Define the applicable span technical properties in the left pane of the dialog box. For details, see "Span Definition Dialog Box" on page 3-10.

   The *Leased Lines* pane of the *Span Definition* dialog box is used to configure leased lines. The Leased Lines pane is active only if you have selected one of the leased lines options in the *Service Type* field in the *Settings* dialog box.

   To add lines:

   a. In the *Span Definition* dialog box, *Leased Line* pane, click the **New** button.

      The *Leased Lines* dialog box opens:



Leased lines are communication lines that are dedicated to specific participants. In the *Leased Lines* dialog box, you select the participants that will be assigned to this line. The number of ports allocated to each participant determines the line rate to be used in multiples of 64 Kbps, and it depends on the endpoint capabilities. For example, if the participant's capabilities allow a line rate of 384 Kbps (6B), the participant will be assigned six (ports).

b. In the *Participant Name* box, enter the participant name.

c. In the *First Port* box, enter the sequential number of the first port (channel) in the range of channels to be assigned to this participant.

d. In the *Last Port* box, enter the sequential number of the last port (channel) in the range of ports (channels) to be assigned to this participant.

For example, if the line rate to be assigned to this participant is 384Kbps, assign 6 ports. If this is the first participant you are defining, you may define the range by indicating the first port as number 1 and the last port as number 6. However, if this participant is not the first participant to be defined, the first port number will have to be the next available sequential number. For example, if the last port defined for a participant is 16, the first port number to be assigned to this participant is 17.

e. Click **OK**.

The participant's name is added to the *Leased Lines* list.

f. Repeat steps a to f to define additional participants using this leased line.

To modify a participant's configuration:

- In the *Leased Lines* list, double-click the participant name. The *Leased Lines* dialog box opens.
- Define the participant's parameters as described in steps 7.b to 7.f.

To delete a participant's configuration:

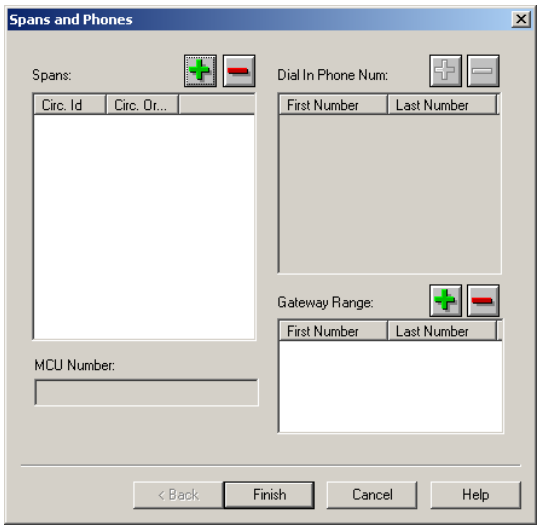
- In the *Leased Lines* list, highlight the participant name, and then click the **Delete** button.

  The participant is removed from the *Leased Lines* list.

7. Select the **Restricted** check box if the endpoints support a line rate of 56 Kbps per channel, instead of 64 Kbps.

8. Click **Next** to continue.

   The *Spans and Phones* dialog box opens.



   When defining leased lines, the *Dial In Phone Num* pane is disabled, as there is no need to define dial-in phone numbers. The participants are connected directly.

   You can connect more than one PRI leased line per Network Service. The span definition is identical to the standard T1 definition. For details, see "Spans and Phones Dialog Box" on page 3-14.

   The leased line is always open to the MCU and no dialing is required. For this reason the *MCU Number* field is disabled.

   For definition of the *Gateway Range* see the "Spans and Phones Dialog Box" on page 3-14.

9. Click **Finish** to complete the Network Service definition.

Defining ISDN Non-Facility Associated Signaling (NFAS)

Non-Facility Associated Signaling (NFAS) only applies to T1 lines and can be configured in two different ways, depending on the ISDN network cards installed in your MCU.

Each T1 span has 23 B channels for transferring audio, video, or data and one D channel. The D channel acts as a signaling channel, and controls the call activity.

In systems using NFAS, when you have a Net-2/4/8 card installed in your system, only one D channel is used. The other spans share the D channel, and this enables each additional PRI line to use the D channel as a B channel for audio, video, or data.

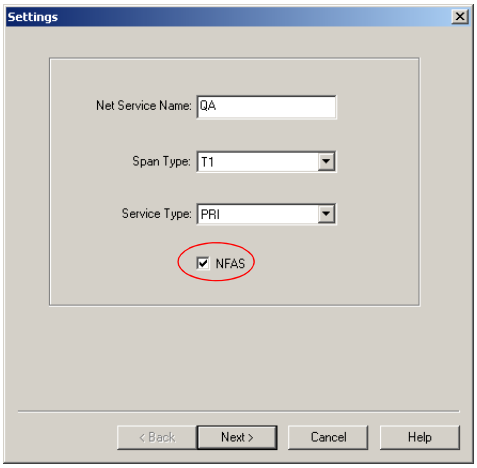
The span containing the D channel is called the *Master.* The remaining spans, which share this D channel are called *Slaves,* and the number of B channels on each *Slave* line is increased to 24.

The Net-8 card has certain limitations in that you cannot aggregate PRI lines from another Net-8 card. This means that the maximum number of *Slave* spans that can share a *Master* span is seven, allowing for eight spans in total.

If you are using a Net-T1 card, several PRI lines on different cards may be aggregated to create one span. In such a case, one D channel controls the call activity for all the aggregated PRI lines - the *Master.* The remaining D channels are used to transfer call data (video and audio data), hence increasing the number of B channels (from 23 to 24 channels for each *Slave* PRI line) that can be used for video conferencing. You can, however, aggregate *Slave* spans from different Net-T1 cards to share with one *Master.* Theoretically, you can have up to 10 Net-T1 cards having 19 *Slaves* sharing with a *Master* (20 spans in total). However, it is not practical to have so many Net-T1 cards connected to an MCU at any given time.

To define an NFAS Network Service:

1. In the *Settings* dialog box select the **NFAS** check box.
2. Define the remaining settings parameters as described for standard PRI lines. For details, see "Settings Dialog Box" on page 3-4.

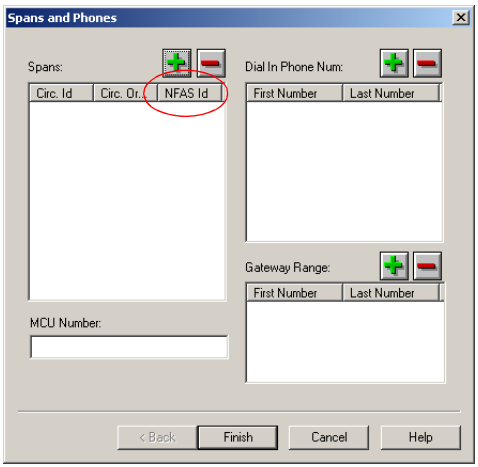


3. Select **Next**.
   The *PRI Settings* dialog box opens.

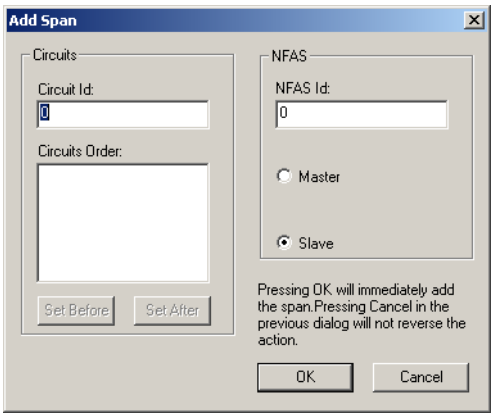
   Define the service provider's parameters as for standard PRI lines. For details, see "PRI Settings Dialog Box" on page 3-6.
4. Select **Next**.
   The *Span Definition* dialog box opens.

   Define the technical span parameters as for standard PRI lines. For details, see "Span Definition Dialog Box" on page 3-10.
5. Select **Next**.

The *Spans and Phones* dialog box opens, displaying the *NFAS ID* field in the *Spans* pane.



6. In the *Spans* pane, click the **Plus** button. The *Add Span* dialog box opens.



7. Enter *Circuit ID* numbers for each span, as per PRI lines.

The Circuit Order is assigned automatically by the system according to the order in which the spans are added.
You can change the span order (if there are several spans defined in the system) using the **Set Before** or **Set After** buttons. These buttons are enabled when the *NFAS* option was enabled in the *Settings* dialog box and you define several PRI spans to be used as part of the NFAS service.
To do so:

- Click the name of a circuit in the Circuits Order list, which is to be adjacent to the circuit you are defining.
  The circuit's entry is highlighted.
- To insert the new circuit, do one of the following:
- Click **Set Before** to insert the new circuit before the highlighted entry.
- Click **Set After** to insert the new circuit after the highlighted entry.

8. In the *NFAS ID* box, enter the NFAS ID number for the span that you are defining.
9. Select the **Master** or **Slave** option, which is applicable to the span that you are defining.
   - *Master* - The D-channel of the first PRI line that will be used to control the data flow for all the PRI lines bundled as NFAS.
   - *Slave* - The PRI line that is used for data transfer (audio and video information), increasing the line rate that can be used to run conferences.

- There are certain limitations when using a **Net-8** card. The first number should be that of the *Master*, and is always 0. The order in which you define the remaining PRI lines (the *Slaves*) determines the order in which the lines will be used for running conferences. The NFAS ID number of the first *Slave* is 1. The ID numbers for each successive PRI line that is added as a *Slave* is sequentially increased by 1.
- If you are using a **Net-T1** card, the NFAS ID number that you allocate to the *Master* and *Slave* PRI lines is not important. It is however recommended that you enter 0 for the *Master* and increase this number by one sequentially, for every additional *Slave* that you define.
- The ID numbers assigned to each span must be identical to the ID numbers configured on the switch in order for the system to recognize the data flow on each channel.

10. Click **OK**.
    The *Add Span* dialog box closes and you are returned to the *Spans and Phones* dialog box.
11. To define additional NFAS spans, repeat steps 3 to 7.
12. Define the dial-in phone ranges as described in “Defining Dial-In Numbers” on page 3-17.
13. Click **Finish** to complete the Network Service definition.

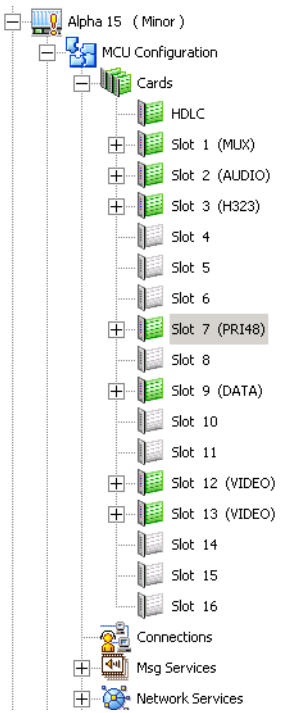
Assigning the ISDN Network Service to the NET-T1/NET-E1 Card

To connect the MCU to the ISDN network, you need to configure the Network Interface Module in conjunction with the ISDN Network Services defined in the MGC Manager.

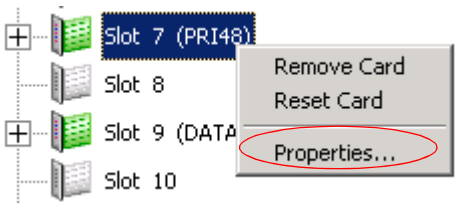
The label on the Network functional module indicates the card type.

To assign the ISDN Network Service to the Network Interface module (Net-T1/Net-E1 Card):

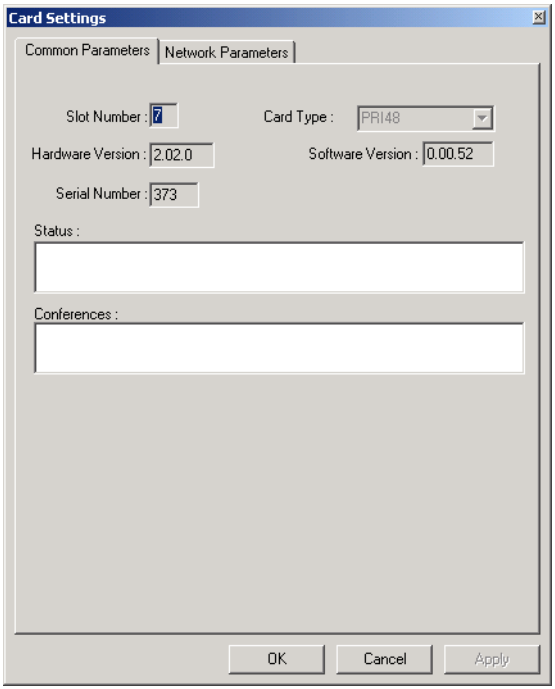
1. Expand the *MCU* tree.
2. Expand the *MCU Configuration* tree.
3. Expand the *Cards* tree.
   The *Cards* list is displayed below the *Cards* icon.



4. In the *Browser* pane, right-click the slot containing the Net-E1/T1 card, indicated by PRI48 and PRI64, and then click **Properties**. Alternatively, double-click the slot containing the card.



The *Card Settings – Common Parameters* dialog box opens.



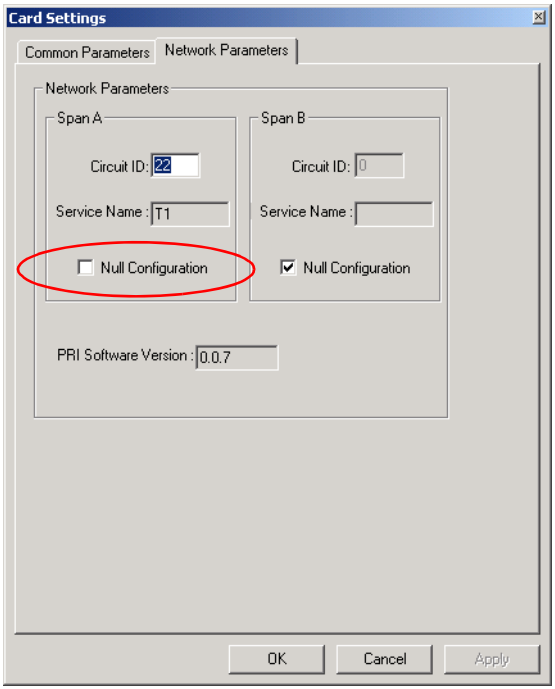
The *Common Parameters* describe the basic card settings; Slot Number, Card Type, Hardware Version Number, Software Version Number, and Serial number. For more information, see Chapter 4, “Viewing the Common Card Parameters” on page 4-10.
These settings are for viewing purposes only and cannot be modified in this tab.

The *Status* box displays all error messages relating to the card.

The *Conference* box displays the names of conferences that are currently being run by this card.

5. Click the **Network Parameters** tab.

   The *Card Settings - Network Parameters* dialog box opens, displaying the settings that are specific to the Net-T1/Net-E1 *Network Interface* module.



The Net-T1/Net-E1 ISDN Network Interface module supports up to two PRI connections. Both of these connections must be of the same type; either T1 or E1. One Net-T1/Net-E1 Network Interface module in each system serves as the "master clock," which synchronizes the system clock with the network clock. A second Net-T1/Net-E1 Network Interface module provides a backup clock, which is used if the master clock fails. For more information see Chapter 5, "Clocking" on page 5-139.

For the system to recognize the PRI line that connects to the Net-T1/Net-E1 Network Interface card you have to assign the PRI line's circuit ID as defined in the ISDN Network Services to the Net-T1/Net-E1 Network Interface module.

6. Fill in the *Span A* section as follows:

   a. Clear the **Null Configuration** check box to indicate that a PRI line is connected to the Network Interface Module.

   b. In the *Circuit ID* box, enter the circuit ID as defined in the *Network Service-Span and Phones* dialog box. According to the selected Circuit ID, an ISDN Network service is assigned to the network card. Each span can be assigned a different ISDN Network Service.

   c. Click **Apply**.

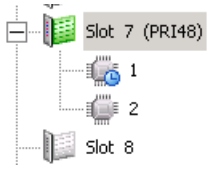
   The name of the network service appears in the *Service Name* box.

7. Click **OK**.

To configure the Net-T1/Net-E1 ISDN network span as primary or backup clock:

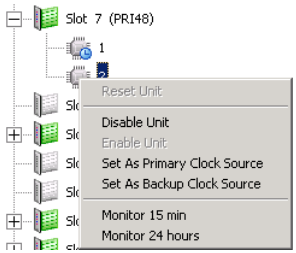
1. In the *Browser* pane, click the slot containing the ISDN Network Interface module (PRI) to configure in the *Status* pane, or click the plus [+] icon next to the *Card* icon to expand its units tree.

   If you clicked the slot, the module's units and configuration are displayed in the *Status* pane. If you expanded the units tree, the units are displayed in the *Browser* pane.



Id	Config	Occupied	Faulty	Disabled	Ports State	Net Service	Percent Occ
..							
1	T1 PRI	No	No	No		11	
2		No	Yes	No			

2. Right-click the unit you want to configure. Depending on the card clock source assignment (if primary or backup) the following options appear.



3. Click the desired option.

Table 3-7: Network Interface Unit (ISDN) - Configuration Options

Option	Description
Set as Primary Clock Source	Sets this unit as the primary clock source. For further information, see Chapter 5, "Clocking" on page 5-139.
Cancel Primary Clock Source	Stops this unit from acting as the primary clock source. For further information, see Chapter 5, "Clocking" on page 5-139.
Set As Backup Clock Source	Sets this unit as the backup clock source. For further information, see Chapter 5, "Clocking" on page 5-139.
Cancel Backup Clock Source	Stops this unit from acting as the backup clock source. For further information, see Chapter 5, "Clocking" on page 5-139.

After setting the network clock, a *Warning* message box opens, advising you to reset your MCU.

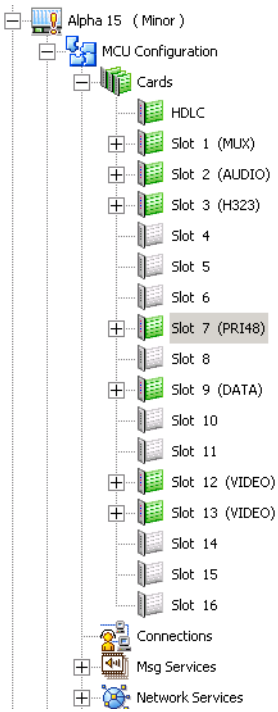
The configuration changes take effect only after the next MCU reset or startup, and are shown in the *Configured Clock* column in the *Status* pane.

Assigning the ISDN Network Service to the Net-2/Net-4/Net-8 Card

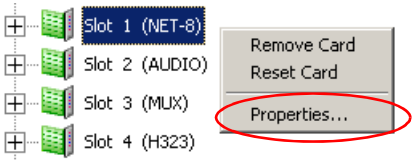
In order to connect the MCU to the ISDN network switch, you need to assign the ISDN Network Service to the appropriate span of the Net-2/Net-4/Net-8 Network Interface module. In addition, you may define which span in the network interface card will be used as the primary clock and which one as the backup clock to synchronize with the network clock.

To assign the ISDN Network Service to the Net-2/Net-4/Net-8 Network Interface module:

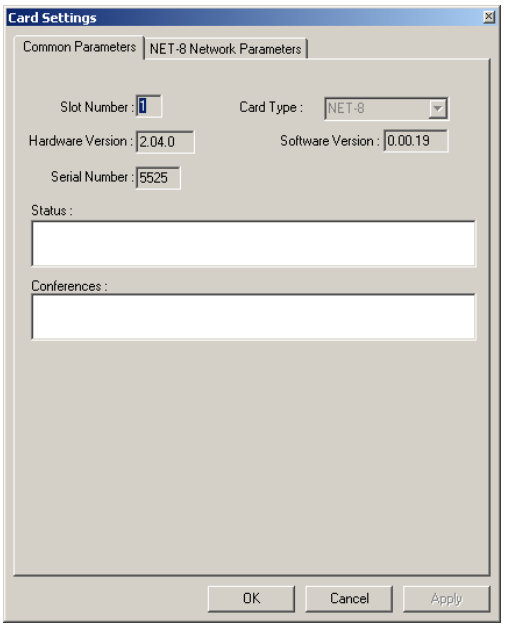
1. Expand the *MCU* tree.
2. Expand the *MCU Configuration* tree.
3. Expand the *Cards* tree.
   The *Cards* list is displayed below the *Cards* icon.



4. In the *Browser* pane, right-click the slot containing the Net-2/4/8 card, and then click **Properties**.
Alternatively, double-click the slot containing the card.



The *Card Settings – Common Parameters* dialog box opens.



The *Common Parameters* describe the basic card settings: Slot Number, Card Type, Hardware Version Number, Software Version Number, and Serial number. For more information, see Chapter 4, "Viewing the Common Card Parameters" on page 4-10.

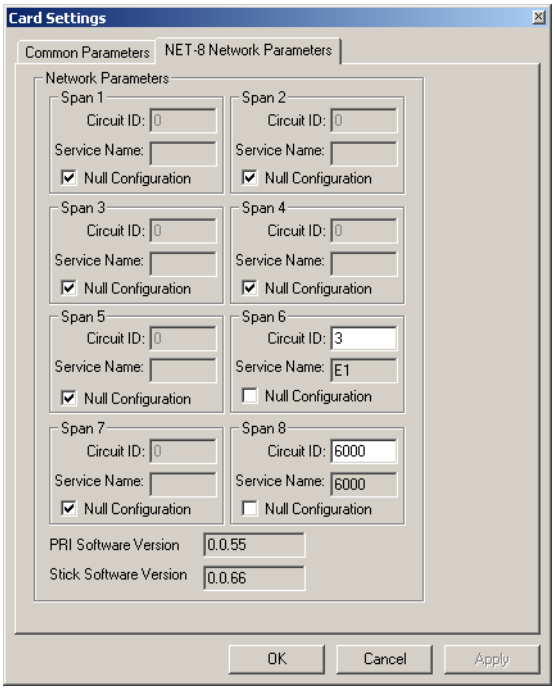
The *Status* box displays all the error messages related to the card.

The *Conferences* box displays the names of conferences which are currently active.

These settings are for viewing purposes only and cannot be modified in this tab.

5. Click the **Net-8 Network Parameters** tab.

   The *Card Settings - NET-8 Network Parameters* dialog box opens, displaying the settings that are specific to the Net-2/Net-4/Net-8 Network Interface module.

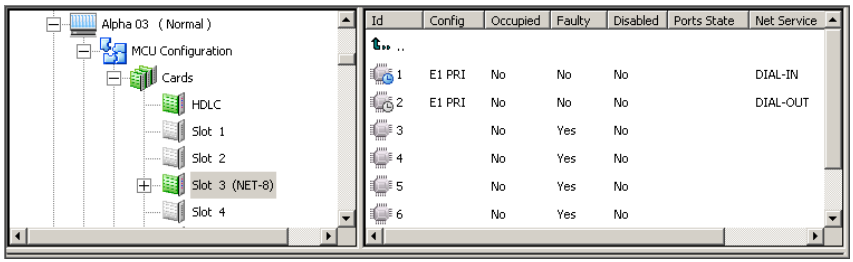


The Net-2/Net-4/Net-8 Network Interface module supports up to eight PRI connections depending on the card model installed in the MCU. These connections may be either T1 or E1. Any of these spans may be set as the “master clock,” which synchronizes the system clock to the network clock, or “backup clock, which is used if the master clock fails. For the system to recognize the PRI lines that connect to the Network card you must assign the *Circuit ID* of the PRI line defined in Network Service to the appropriate span in the *Card Settings - Net-8 Network Parameters*. Not all spans may currently be in use. In such a case, only the spans being used are configured. Different Network Services may be defined for each of the spans being used. Alternatively, the same Network Service may be used for all the spans. In such a case, different circuit IDs must be defined for each span in the Network service.

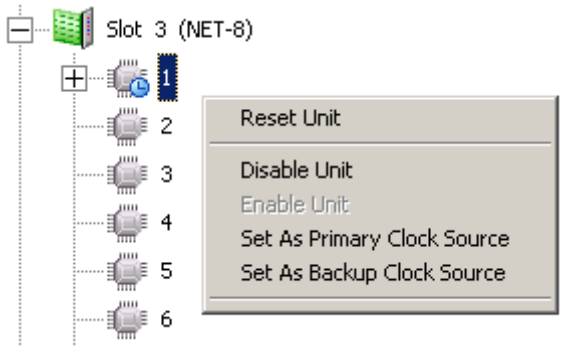
6. To assign a *Circuit ID* to the appropriate span:
   a. In the *Span n* box (where *n* is the span number on the Net-2/Net-4/Net-8 module to which the PRI line is connected), clear the **Null Configuration** check box to enable the span.
   b. In the *Circuit ID* box, enter the circuit ID as defined in the *Network Service-Span and Phones* dialog box. According to the selected *Circuit ID*, the Network Service is assigned to the network card. Each span can be assigned a different Network Service.
   c. Click **Apply**.
   The name of the network service appears in the *Service Name* box.
7. Click **OK**.

To configure a Net-2/Net-4/Net-8 span as primary or backup clock:

1. In the *Browser* pane, click the slot containing the Net-2/Net-4/Net-8 ISDN Network Interface module (PRI) to configure in the *Status* pane, or click the plus [+] icon next to the *Card* icon to expand its units tree. If you clicked the slot, the module's units and configuration are displayed in the *Status* pane.If you expanded the units tree, the units are displayed in the *Browser* pane. Each unit represents a span in the Network Interface Module.



2. Right-click the unit (span) to configure.
   A menu appears.



3. Click one of the following options to set up the clock source for the system.

Table 3-8: Net-2/Net-4/Net-8 Unit Configuration Options

Option	Description
Set as Primary Clock Source	Sets this unit as the primary clock source. For further information, see Chapter 5, “Clocking” on page 5-139.
Cancel Primary Clock Source	Stops this unit from acting as the primary clock source. For further information, see Chapter 5, “Clocking” on page 5-139.
Set As Backup Clock Source	Sets this unit as the backup clock source. For further information, see Chapter 5, “Clocking” on page 5-139.
Cancel Backup Clock Source	Stops this unit from acting as the backup clock source. For further information, see Chapter 5, “Clocking” on page 5-139.

After setting the clock source, a *Warning* message box opens, instructing you to reset your MCU.

The configuration changes take effect only after the next MCU reset or start up, and they are shown in the *Configured Clock* column in the *Status* pane.

Defining a T1-CAS Network Service

Channel Associated Signaling (CAS), is a method of signaling performed on a traffic channel rather than on a dedicated signaling channel (as in ISDN).

T1-CAS Network Service allows connection of Audio Only participants and is intended for VoicePlus configurations or MCUs running Audio Only conferences using T1-CAS lines.

T1-CAS participants may take part in a video conference as Audio Only participants if the MCU is configured accordingly.

T1-CAS is supported only with Audio+ 12/24, Audio+24/48 and Audio+48/96.

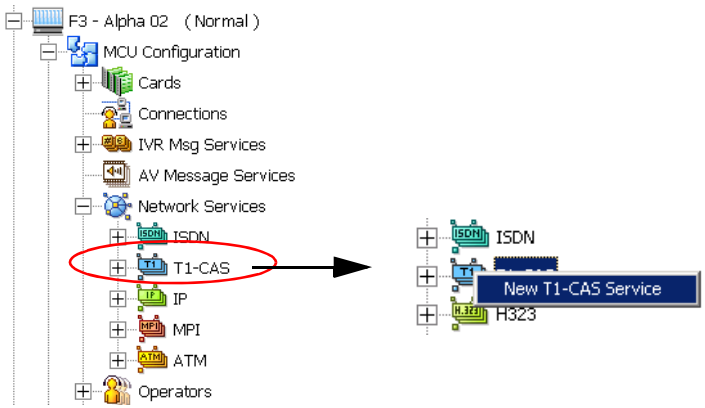
To configure the MCU to work with T1-CAS:

To enable participant connection over T1-CAS lines the following components must be configured:

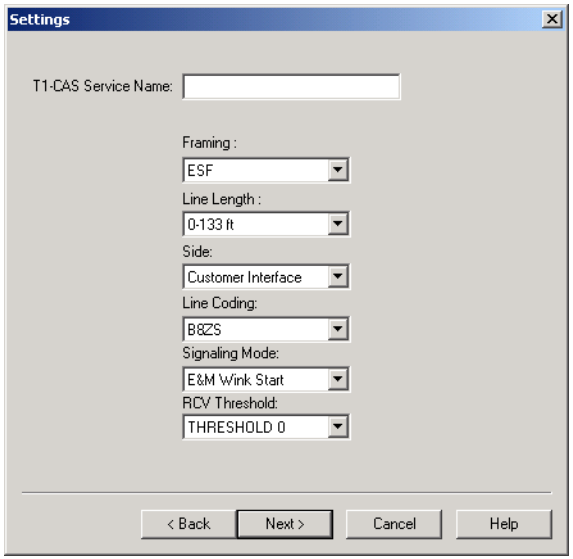
- Set the appropriate flags in the "system.cfg" file. For more details, Chapter 5, "Section NET8_PARAMETERS" on page 5-96 and Chapter 5, "Section T1-CAS-PARAMETERS" on page 5-94.
- Define a T1-CAS Network Service.
- Assign the T1-CAS Network Service to the Net-2/4/8 card.
- Set a T1-CAS Span as the network clock source.

Defining a new T1-CAS Network Service

1. In the *Browser* pane, expand the MCU tree, and then expand the *MCU Configuration* tree.
2. Expand the *Network Services* tree.
3. Right-click the *Network Services - T1-CAS* icon, and then click **New T1-CAS Service**.



The *New Network Services* configuration wizard opens.



4. Define the following parameters:

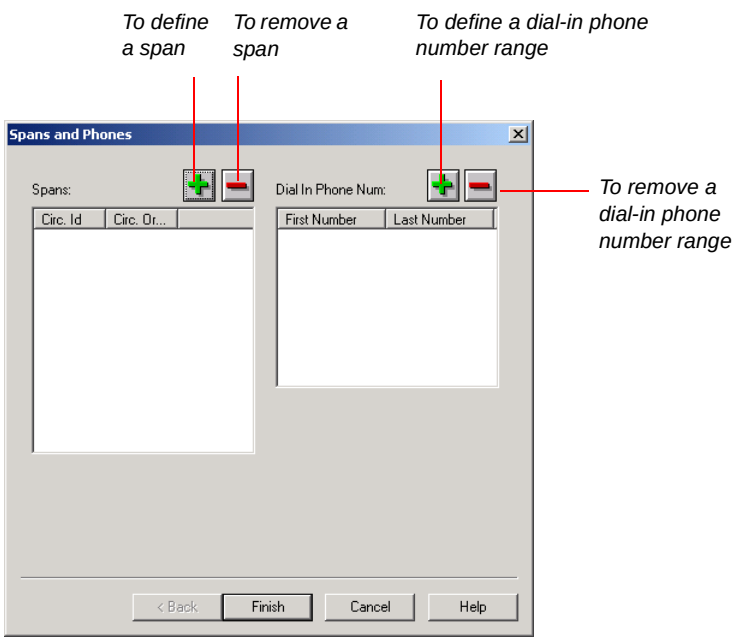
Table 3-9: Settings Dialog Box Options

Field	Description
T1-CAS Service Name	Specify the service name using up to 20 characters. The *Network Service Name* identifies the service to the system.
Framing	Framing refers to the frame format used by the carrier for the network interface. Select the appropriate option from the drop-down list. • ESF (Extended Super Frame). This is the system default. • ESF ZBTSI • SF SLC96 • SF
Line Length	Indicates the distance between the MCU and the PBX. Select the desired option from the list: • 0-133 ft. (0.0 dB) • 133-266 ft. (-7.5 dB) • 266-399 ft. (-15.0 dB) • 399-533 ft. (-22.5 dB) • 533-655 ft. (-30.0 dB)
Side	Select the desired option from the list: • Customer Interface (default) • Network Interface **Note:** If the PBX is configured on the network side, the MGC unit must be configured as the customer side, and vice versa.
Line Coding	Indicates how the bits are sent on a PRI line. Select the desired option from the list. • B8ZS - Bipolar 8-Zero Substitution (default) • B7ZS • AMI - Alternate Mark Inversion with zero code suppression
Signaling Mode	• Select the **E&M Wink Start** option.

Table 3-9: Settings Dialog Box Options

Field	Description
RCV Threshold	This option is used to increase the signal on T1 spans when the system detects a very low signal. Select the desired threshold values from the list: • THRESHOLD 0 (default) • THRESHOLD 1 • THRESHOLD 2 • THRESHOLD 3 **Note:** When you modify the threshold values a warning box is displayed, advising you that you need to obtain authorization from the system support.

5. Click **Next** to continue.
The *Spans and Phones* dialog box opens.



This dialog box is used to assign circuit identification numbers and the dial-in phone number range to be used in dial-in conferences.

Circuit orders are automatically assigned to spans. The dial-in phone numbers are allocated to the MCU by the service provider (carrier).

Gateway Sessions are not supported with T1-CAS lines.

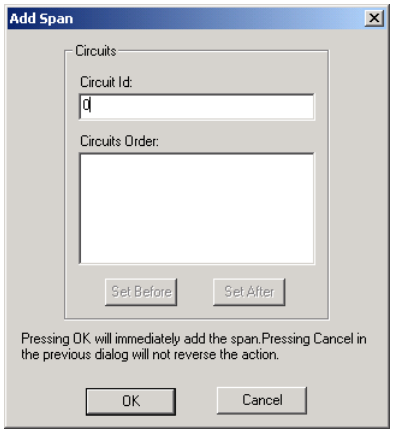
6. Define the *Spans and Phones* parameters as follows:

Table 3-10: Span and Phone Dialog Box Options

Field	Description
Spans	Displays the existing definitions of circuit identification numbers and circuit orders. Click the plus button to define the new spans.
Dial In Phone Num	Lists the phone numbers that will be used for dialing in, as allocated to the MCU by the service provider. Click the plus button to define a new dial-in phone range.

7. To assign circuit identification numbers and orders:
   a. In the *Spans and Phones* dialog box, in the *Spans* section, click the **Plus** button.

      The *Add Span* dialog box opens.



b. Define the *Circuit Id*.

Table 3-11: Add Span Dialog Box Options

Field	Description
Circuit ID	The Circuit Identification is a logical number used to identify the span to the MGC Manager. This number is later used to assign the span to the network card. Type any positive integer from 0 to 65535, to be used as the circuit identification number in the MGC Manager. **Note:** If other services are already defined, make sure to use numbers other than those already assigned to the existing services.
Circuits Order	The Circuit Order determines the order in which an MCU uses the spans to dial out. The Circuit Order is assigned automatically by the system according to the order in which the spans are added. In dial-out connections the MGC allocates ports from the spans starting with the span having the lowest number and the lowest port number within that span.

c. Once you have defined all the identification numbers click **OK**.

The *Add Span* dialog box closes and you are returned to the *Spans and Phones* dialog box.

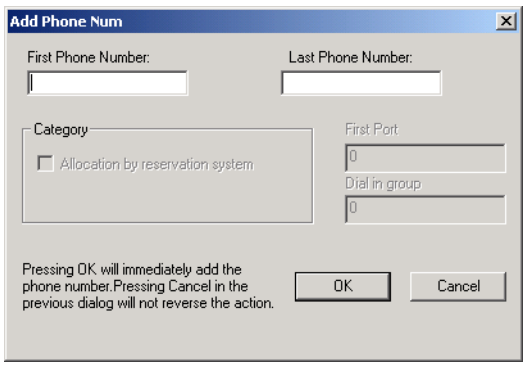
To delete a circuit identification entry:

— In the *Spans* pane, click the Circuit Identification entry, and then click the **Minus** button.
The entry is deleted.

8. To define the dial-in phone number range:

a. In the *Dial-in Phones* pane of the *Spans and Phones* dialog box, click the **Plus** button.

The *Add Phone Num* dialog box opens.



b. Enter the first number and the last number in the phone numbers range and click OK.

The phone numbers range is added to the *Dial-in Phones* pane of the *Spans and Phones* dialog box.

Completing the T1-CAS Network Service Definition

9. Once you have finished filling in all the Wizards screens, in the *Spans and Phones* dialog box, click the **Finish** button.

   The data you have specified will be validated, after which the T1-CAS Network Service will be added to the list of T1-CAS network services of the MCU.

Assigning the T1-CAS Network Service to the Net-2/Net-4/Net-8 Card

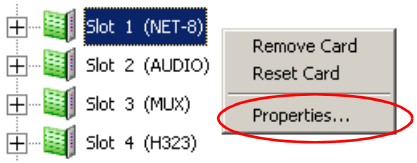
In order to connect the MCU to the network switch, you need to assign the T1-CAS Network Service to the appropriate span of the Net-2/Net-4/Net-8 Network Interface module.

It is not possible to mix an ISDN Network Service and a T1-CAS Network Service on the same Net-2/Net-4/Net-8 Network Interface module. Therefore, the Net-2/Net-4/Net-8 card can only be used with either ISDN or T1-CAS Network Service. Before you assign the T1-CAS Network Service to the card, you must set the following 'system.cfg' flag: in the NET8_PARAMETERS section, set NET8_DEFAULT_TYPE = to T1-CAS.

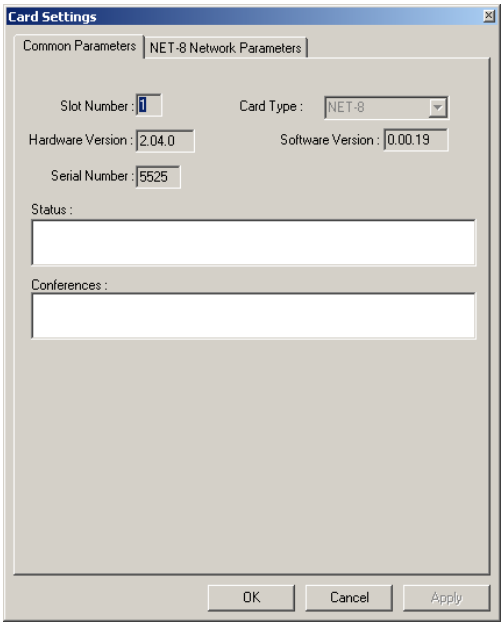
In addition, you may define which span in the network interface card is used as the primary clock and which one as the backup clock in order to synchronize with the network clock.

To assign the T1-CAS Network Service to the Net-2/Net-4/Net-8 Network Interface module:

1. In the *Browser* pane, right-click the slot containing the Net-2/4/8 card, and then click **Properties**. Alternatively, double-click the slot containing the card.



The *Card Settings – Common Parameters* dialog box opens.



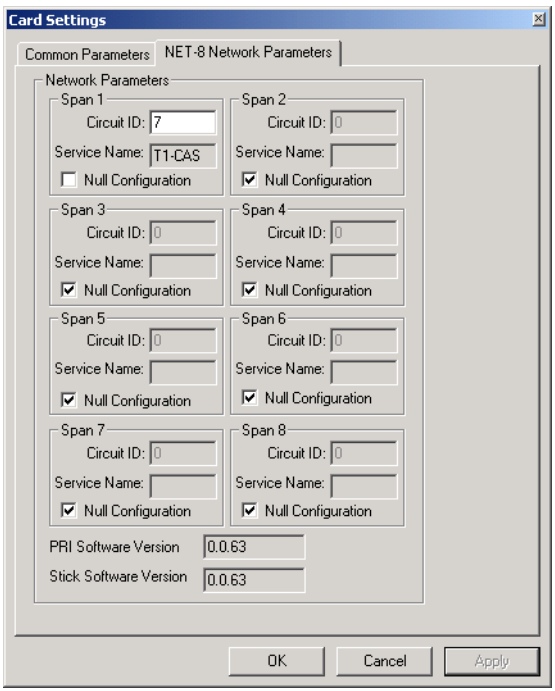
The *Common Parameters* describe the basic card settings.

The *Status* box displays all the error messages related to the card.

The *Conferences* box displays the names of conferences which are currently active.

2. Click the **Net-8 Network Parameters** tab.

The *Card Settings NET-8 Network Parameters* dialog box opens.



The Net-2/Net-4/Net-8 Network Interface module supports 2/4/8 T1-CAS spans depending on the card model. Any of these spans may be set as the "master clock," which synchronizes the system clock to the network clock, or "backup clock, which is used if the master clock fails. Only the spans being used are configured. The same Network Service may be used for all the spans. In such a case, different circuit IDs must be defined for each span in the Network Service.

- It is not possible to mix an ISDN and a T1-CAS Network Service on the same Net-2/Net-4/Net-8 Network Interface module. If an ISDN and a T1-CAS Network Service are mixed on the same Network card an error message is displayed.
- Net-T1 module does not support a T1-CAS Network Service.

3. To assign a *Circuit ID* to the appropriate span:

   a. In the *Span "n"* box, clear the **Null Configuration** check box to enable the span.

b. In the *Circuit ID* box, enter the circuit ID as defined in the *Network Service–Spans and Phones* dialog box. According to the selected *Circuit ID*, the Network Service is assigned to the network card. Each span can be assigned a different Network Service.

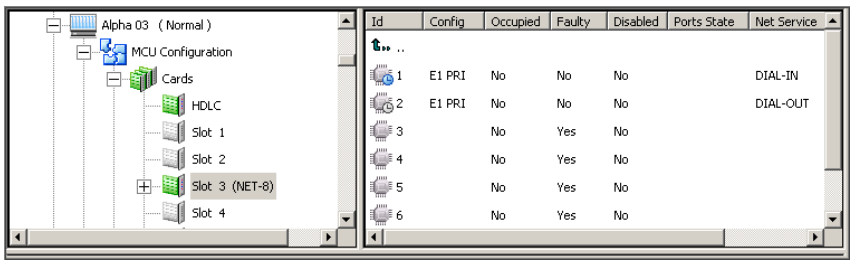
c. Click **Apply**.
The name of the network service appears in the *Service Name* box.

4. Click **OK**.

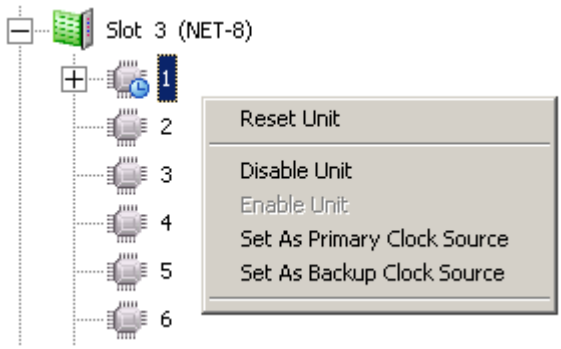
To configure a Net-2/Net-4/Net-8 span as primary or backup clock:

1. In the *Browser* pane, click the slot containing the Net-2/Net-4/Net-8 ISDN Network Interface module (PRI) to configure in the *Status* pane, or click the plus [+] icon next to the *Card* icon to expand its units tree.

   If you clicked the slot, the module's units and configuration are displayed in the *Status* pane.If you expanded the units tree, the units are displayed in the *Browser* pane. Each unit represents a span in the Network Interface Module.



2. Right-click the unit (span) to configure.
A menu appears.



3. Click one of the following options to set up the clock source for the system.

Table 3-12: Net-2/Net-4/Net-8 Unit Configuration Options

Option	Description
Set as Primary Clock Source	Sets this unit as the primary clock source. For further information, see Chapter 5, “Clocking” on page 5-139.
Cancel Primary Clock Source	Stops this unit from acting as the primary clock source. For further information, see Chapter 5, “Clocking” on page 5-139.
Set As Backup Clock Source	Sets this unit as the backup clock source. For further information, see Chapter 5, “Clocking” on page 5-139.
Cancel Backup Clock Source	Stops this unit from acting as the backup clock source. For further information, see Chapter 5, “Clocking” on page 5-139.

After setting the clock source, a *Warning* message box opens, instructing you to reset your MCU.

The configuration changes take effect only after the next MCU reset or start up, and they are shown in the *Configured Clock* column in the *Status* pane.

Defining an IP Network Service

The IP Network Service defines the properties of the IP network used for connecting IP endpoints to the conference and the IP cards (installed in the MCU) to which the network is connected. Several of the network components are used by both H.323 and SIP endpoints to connect to the conference, and the same IP card is used for H.323 and SIP connections. Therefore one IP Network Service can be defined for both H.323 and SIP environments as well as an H.323-only or a SIP-only network service.

This section covers the following topics:

- IP Network Service components ("Appendix E: IP Network Components" on page E-1)
- Defining an IP Network Service (page 3-54)
- Assignment of network services to the IP/IP+ card (page 3-93)
- Designating the IP Network Service as Default (page 3-97)

H.323

H.323 is a standard for audio, video, and data communications across IP-based (LAN) networks, including the Internet.

The H.323 network includes four main components: H.323 endpoints, gateway, gatekeeper, and MCU with an IP card. The gateway and MCU may be in one unit or two separate units.

The RAS (Registration Admission Status) signalling protocol is used to communicate between endpoints and the gatekeeper.

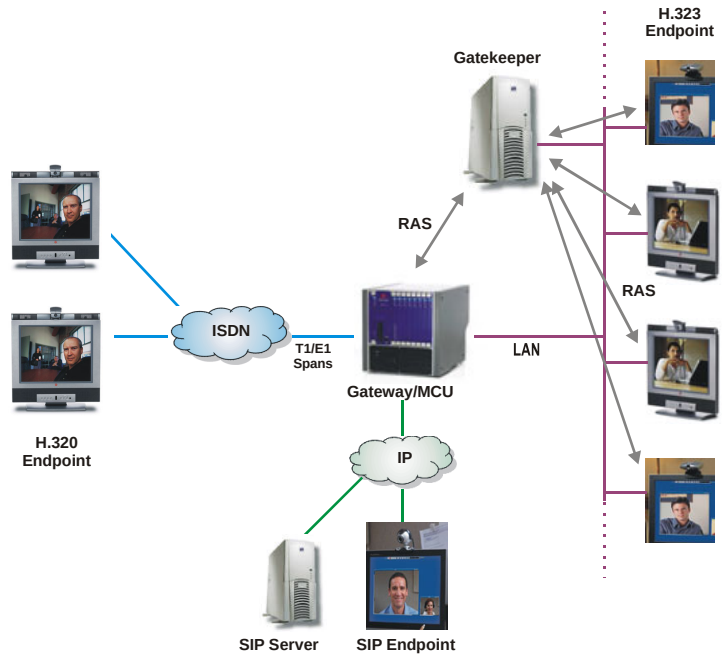


Figure 3-1: Typical H.323 Configuration

SIP

Session Initiation Protocol (SIP) is an application-layer protocol designed to work over IP networks that can establish, modify, and terminate multimedia sessions (conferences).

The SIP network includes the following components: SIP endpoints, DNS, SIP Server, and MCU with an IP card.

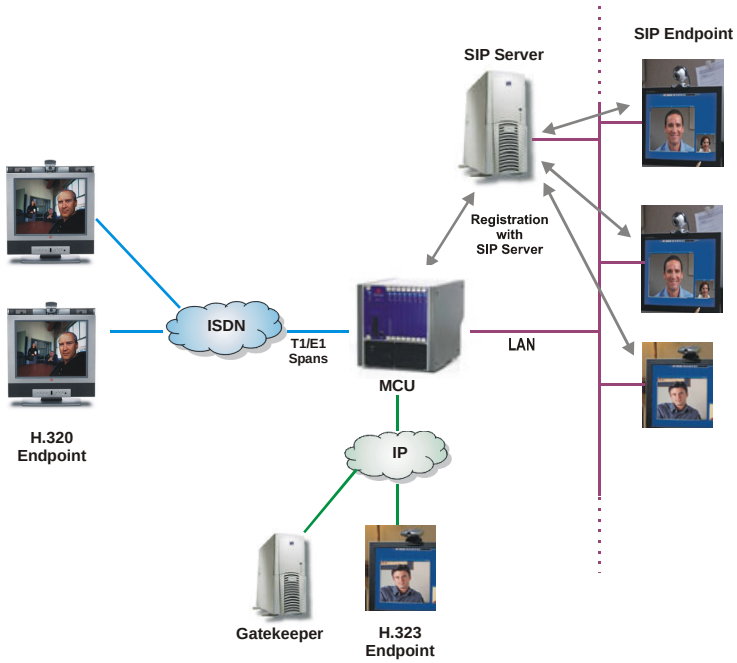


Figure 3-2: Typical SIP Configuration

For a detailed description of the IP network components, see Appendix E: IP Network Components.

Defining an IP Network Service

Conferencing with H.323 and SIP endpoints requires the presence of various components in the IP environment. Several components are common to both H.323 and SIP connections and others are unique to H.323 or SIP.

The following table lists the components required for conferencing using IP endpoints, indicating their relevancy to H.323 and SIP:

Table 3-13: IP Network List of Components and Logical Entities

Name	H.323	SIP
MCU with IP card(s)	Required	Required
Subnet Mask	Required	Required
DHCP	Optional	Optional
DNS	Optional	Optional
Host Name	Required	Required
Default Router	Required	Required
Static Routes	Optional	Optional
NAT Traversal	Optional	Optional
Gateway	Optional	Optional
Gatekeepers	Optional (recommended)	N/A
H.323 endpoints	Required	N/A
SIP endpoints (User Agents)	N/A	Required
SIP Servers—general	N/A	Optional
Registrar	N/A	Optional (recommended)

The MCU's IP cards can be used to connect both H.323 and SIP participants to conferences. Therefore, you can define one IP Network Service that includes both H.323 and SIP entities (including the MCU's IP cards) that

belong to the same subnetwork. H.323 entities are serviced by the same gatekeeper, while SIP entities are serviced by the same SIP server. You can also define an H.323-only Network Service that includes only H.323 entities and a SIP-only Network Service that includes only SIP entities.

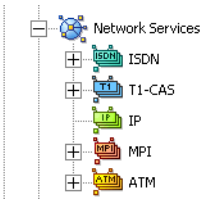
Following is a summary table for the IP Network Service components configuration combinations:

Table 3-14: IP Network Service Configuration by Protocol Type

Network Service	Both H.323 & SIP	H.323 Only	SIP Only
Dialog Box			
Settings	+	+	+
DNS	+	+	+
H.323	+	+	–
SIP	+	–	+
Security	+	–	+
Span	+	+	+

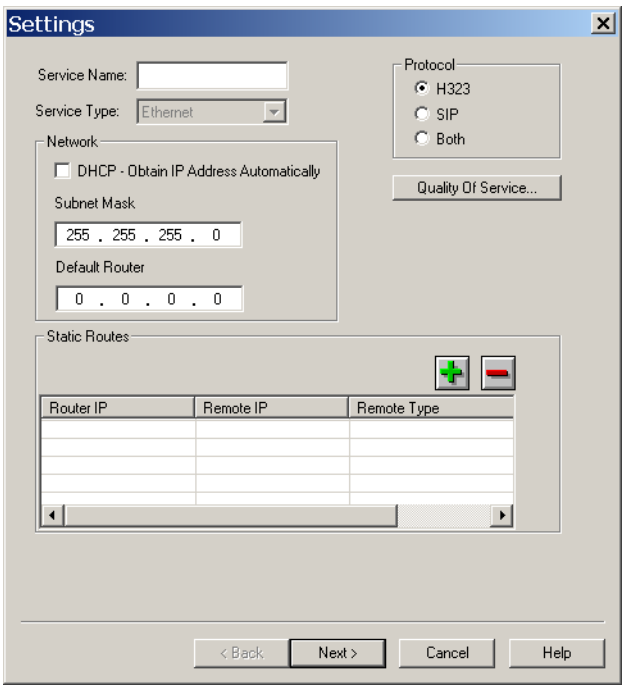
To define an IP Network Service:

1. In the *Browser* pane, expand the *MCU* tree.
2. Expand the *MCU Configuration* tree.
3. Expand the *Network Services* tree.
   A list of Network Service types is displayed.



4. Right-click the *Network Services – IP* icon, and then click **New IP Service.**

The *Setting* dialog box opens.



5. Define the following fields:

Table 3-15: Settings Dialog Box Options

Field	Description
Service Name	Specify the service name using up to 20 characters. The *Network Service Name* identifies the service to the system. To designate a SIP-CX enabled IP Network Service, this name will be used for the system.cfg flag settings.
Service Type	IP services use an Ethernet network, which is a LAN standard. The *Service Type* cannot be changed.

Table 3-15: Settings Dialog Box Options

Field	Description
Protocol	Select: • **H.323:** For an H.323-only Network Service. Only H.323 participants can connect to the MCU using this service. • **SIP:** For a SIP-only Network Service. Only SIP participants can connect to the MCU using this service. • **Both:** For an integrated IP Service. Both H.323 and SIP participants can connect to the MCU using this service.
Network	
DHCP-Obtain IP Address Automatically	Select this check box to use a DHCP server for automatic assignment and tracking of IP addresses to the conference devices (for a definition of DHCP, see "DHCP" on page E-3). Selecting this option retrieves the IP addresses necessary for registration with the DNS and H.323 gatekeeper, and for automatic configuration of the SIP server. This option is useful when your network includes many components whose IP addresses have to be defined. When this option is selected, each IP card is assigned an IP address for the session by the DHCP. With this assigned IP address, the IP card registers with the gatekeeper using its alias and the IP address received from the DHCP. Usually, the DHCP will recognize the MAC address of the IP card and will try to assign the same IP address to the card (unless the card was inactive for several days.) It is recommended to use this option if you have several IP cards to configure as this automatic configuration minimizes the probability of configuration errors. When the DHCP server is used, the IP address of the card appears as 0.0.0.0.

Table 3-15: Settings Dialog Box Options

Field	Description
DHCP-Obtain IP Address Automatically (cont.)	Although the IP address allocated to the cards rarely changes, you may prefer not to select this check box if you need to: • Establish a static IP address, for example, when working with a firewall and you need to translate an internal IP address, that must be static, with an external one. • When dialing in directly to the card, using the card's IP address.
Subnet Mask	Enter the subnet mask of the MCU's IP card. If the DHCP is used, the subnet mask is automatically retrieved from the DHCP server and cannot be modified. For more details, see "Subnet Mask" on page E-2. The detected number appears in the card's *Properties-Settings-IP Network Parameters* dialog box. For more details, see the MGC Administrator's Guide, Chapter 4.
Default Router	Enter the IP address of the default router. If the DHCP is used, the IP address of the default router is automatically retrieved from the DHCP server and cannot be modified. The default router is used whenever the defined static routers (see Static Routes table below) are not able to route the packet to its destination. Another use of the default router is when host access is restricted to one default router. If there are several routers that are used, add their IP addresses to the *Static Routes* table.

Table 3-15: Settings Dialog Box Options

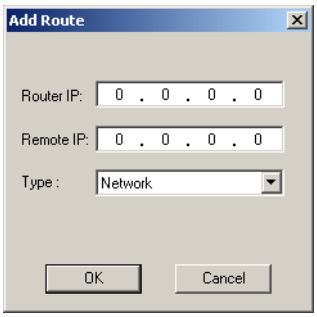
Field	Description
Static Routes	
Routes Table	Displays the list of static routes currently defined in the system. Up to five routers can be defined in addition to the Default router. The order in which the routers appear in this list determines the order in which the system will look for the endpoints on the various networks, if not found on the local LAN. If the system cannot route the packet to the required IP address using one of the defined static routes, the default router is used. If the address is in the local subnet, no router is used. To add a router to the *Static Routes* table, click the **plus** [+] button. For more details see "Defining Static Routes" on page 3-60. To delete a router from the *Static Routes* table select the router to remove, and then click the minus (-) button. You can define one router with different destinations.
Quality Of Service	
Quality Of Service	Data transmission in IP networks is based on best effort. Quality of Service (QoS) is an effort to guarantee in advance the quality of the transmission, especially for video and multimedia information, by allocating higher priority to transmitted media packets. The QoS parameters are based on required priority for video conferencing. To change the defaults click the **Quality of Service** button. For more information see "Defining Quality of Service" on page 3-61.

Defining Static Routes

6. To define a static route:

   a. Click the **plus** [+] button.

   The *Add Route* dialog box opens.



   Two router types can be defined: *Network* and *Host*. A *Host* router provides a direct connection to a specific host (an endpoint) located in another subnetwork. A *Network* router provides a connection to a segment of another network.

   b. Define the following fields:

Table 3-16: Add Router Dialog Box Options

Field	Description
Router IP	Enter the IP address of the router and its subnetwork.
Remote IP	The IP address of the packet destination. The destination determines the entity to be reached outside the local network. The *Type* determines whether this entity is a specific component (Host) or a subnetwork (Network). • If *Host* is selected in the *Type* field, enter the IP address of the endpoint. • If *Network* is selected in the *Type* field, enter the components of the IP address indicating the segment of the other network. For example, entering 128.4.0.0 refers to a network segment whose first two components are 128 and 4.

Table 3-16: Add Router Dialog Box Options (Continued)

Field	Description
Type	Select the type of router connection: • **Network** – defines a connection to a router segment in another network. • **Host** – defines a direct connection to an endpoint found on another network.

c. Click **OK**.
The system returns to the *Settings* dialog box, displaying the added static route.

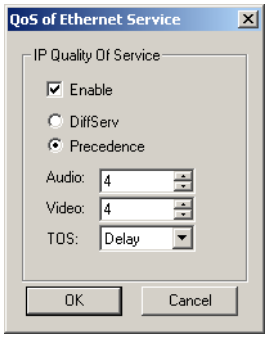
Defining Quality of Service

QoS can be measured and guaranteed in average delay between packets, the variation in delay, and the transmission error rate. Currently, two QoS methods are supported: DiffServ and Precedence. These methods differ in the way the packet's priority is encoded in the packet header.

7. To define Quality of Service parameters:

   a. Click the **Quality of Service** button.

   The *QoS of Ethernet Service* dialog box opens.



b. Define the following fields:

Table 3-17: QoS of Ethernet Service Dialog Box Options

Field	Description
Enable	Select the **Enable** check box to implement QoS for marking outgoing IP packets, either according to the DiffServ standard or the IP Precedence mechanism. If the **Enable** check box is cleared, QoS is not implemented.
DiffServ and Precedence	DiffServ and Precedence are two methods for encoding the packet's priority. The priority set here for audio and video packets should match the priority set in the router. • Select **DiffServ** when the network router uses DiffServ for priority encoding. When the MCU implements DiffServ, it prioritizes the IP packets according to the *QOS PARAMS section* flags, set in the system configuration (system.cfg) file. (The default priority is 4 for audio and video packets). **Note**: If you select DiffServ but your router does not support this standard, IP packets queue on the same communication links with data packets. This non-prioritized queueing greatly increases the latency and jitter in their delivery. • Select **Precedence** when the network router uses Precedence for priority encoding, or when you are not sure which method is used by the router. **Note**: If you are not sure which QoS policy your router supports, select Precedence combined with *None* in the TOS field. Precedence is the default mode as it is capable of providing priority services to all types of routers, as well as being currently the most common mechanism.

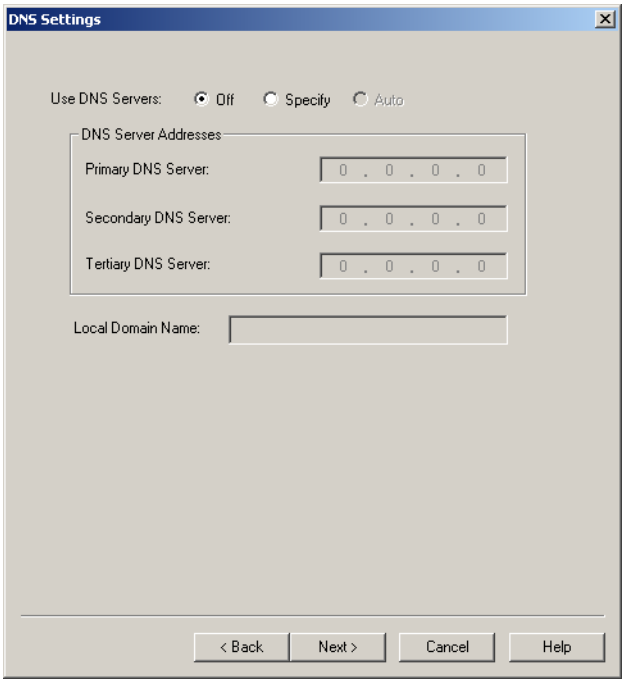
Table 3-17: QoS of Ethernet Service Dialog Box Options (Continued)

Field	Description
Audio and Video	You can prioritize audio and video IP packets to ensure that all participants in the conference hear and see each other clearly. Select the desired priority. The scale is from 0 to 5, where 0 is the lowest priority and 5 is the highest. The recommended priority for both audio and video is 4 to ensure that the delay for both packets is the same and audio and the video packets are synchronized and to avoid lip sync.
TOS	Type of Service (TOS) defines optimization tagging for routing the conferences audio and video packets. Routers that support the Precedence mechanism can implement classification by TOS optimization tags when transferring IP packets. • **Delay** – The recommended default for video conferencing; prioritized audio and video packets tagged with this definition are delivered with minimal delay (the throughput of IP packets minimizes the queue sequence and the delay between packets). • **None** – No optimization definition is applied. This is a compatibility mode in which routing is based on Precedence priority settings only. Select **None** if you do not know which standard your router supports.

c. Click **OK** to apply your settings and return to the *Settings* dialog box.

8. Click **Next.**

   The *DNS Settings* dialog box opens.



   This dialog box is used to define the DNS Server IP address and the local domain name.

   For H.323 conferencing, DNS is used if gatekeeper discovery using the gatekeeper host name and NAT auto-discovery are applied. Using NAT Traversal, the DNS is queried for the NAT server IP address used for allocating the public (external) IP addresses to the cards for the conferencing session.

   For SIP conferencing, domain names are required and therefore it is recommended to enter the details of the DNS server and the local domain name. The DNS is also used if SIP Server discovery is applied. The system decides whether to use the DHCP or the DNS server for auto-discovery with preference to the DNS server.

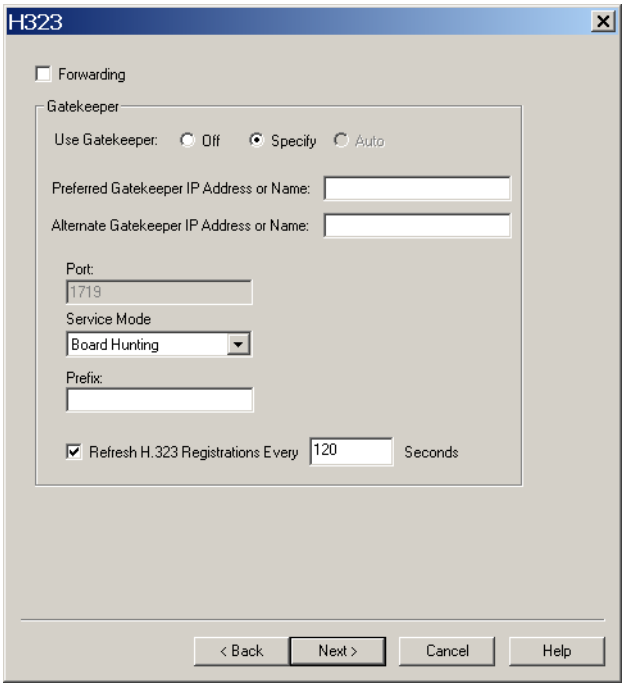
9. Define the following parameters:

Table 3-18: DNS Settings Dialog Box Options

Field	Description
Use DNS Servers	• **Off** – DNS servers are not used in the network. • **Specify** – Select this option to enter the IP address of the DNS servers. • **Auto** – Select this option to automatically detect the primary DNS address, provided the DNS Server is defined in the DHCP and if the *DHCP - obtain IP Address Automatically* check box was selected in the **Settings** tab.
DNS Server Addresses	
Primary DNS Server IP Address	If *Specify* was selected, this field is mandatory. Enter the IP address of the primary DNS server.
Secondary/Tertiary DNS Server IP Address	If *Specify* was selected, enter the IP address(es) of the next DNS server in line to resolve domain names as a fallback for the primary DNS server. These fields are optional.
DNS Name	
Local Domain Name	Enter the domain name where the MCU is installed. The name of the domain includes the host part of URL or URI (the part of the host's address that appears after the at sign (@), or in a URL the part following the *www.* prefix), for example, *polycom.com*. This field is used both for SIP proxy registration purposes and DNS resolution and therefore it is required if you are using DNS servers in this service.

10. Click **Next.**

    The *H.323* dialog box opens.



This dialog box is skipped when defining a SIP-only Network Service.

11. Define the following parameters:

    The following table describes the gatekeeper modes that can be configured with each of the listed gatekeepers.

Table 3-19: H.323 Dialog Box Parameters

Field	Description
Forwarding	Select this check box to enable Forwarding. Forwarding enables the MCU to indicate the IP address of another card for handling the incoming call when the first card is busy. The advantage of Forwarding is that it can be used when no gatekeeper is involved, or when a special Service Mode, such as Basic, is used. **Note**: It is not recommended to use Forwarding when using either Board Hunting or Pseudo Gatekeeper modes.
Gatekeeper	
Use Gatekeeper	• **Off** – select this option if a gatekeeper is not present in your network. In this case, conferencing uses the IP addresses of the endpoints and the MCU IP cards for dial-in and dial-out connections. • **Specify** – to manually define the IP address of the preferred and alternate gatekeepers. • **Auto** – to retrieve the IP address of the preferred and alternate gatekeepers from the DHCP, if they are defined in the DHCP.
Preferred Gatekeeper IP Address or Name	If you have selected *Specify* in the *Use Gatekeeper* option, enter either the gatekeeper's host name (if the DNS server is enabled and the gatekeeper is registered with the DNS, it translates this name into an IP address), or IP address. When *Auto* is selected, this field is disabled and the gatekeeper's name or IP address are taken from the DHCP.
Alternate Gatekeeper IP Address or Name	An alternate gatekeeper is a fallback gatekeeper in case the preferred gatekeeper is not functioning properly. Enter the host name or IP address of the alternate gatekeeper. If this box is left empty, but DHCP is enabled, or when *Auto* is selected, the alternate gatekeeper's details are automatically retrieved from the DHCP.

Table 3-19: H.323 Dialog Box Parameters (Continued)

Field	Description
Port	Port 1719 is the most common port that gatekeepers listen to and transmit through.
Service Mode	Each card registers with the gatekeeper with its IP address and/or alias. The gatekeeper routes calls to the card with available resources. If there is no gatekeeper, calls that approach an IP card with unavailable resources get a reject response, unless *Forwarding* is enabled. • **Basic** [Least recommended] – Each IP card in the MCU registers independently with the gatekeeper. The H.323 endpoint dials directly to this card, using the cards alias as registered with the gatekeeper. The call is routed once only to the MCU. If the card can accommodate the call, the call is accepted. If the card cannot accommodate the call, the call is rejected with no further effort on behalf of the gatekeeper or the operator. In this mode, using a prefix for dialing to the gatekeeper is not required as there is no pooling of resources. • **Board Hunting** – In this mode, the Network Service is registered with the gatekeeper and is associated with a prefix. In addition, all the IP network cards that belong to the same Network Service register with the gatekeeper with the same Network Service prefix. The same prefix is also defined in the IP Network Service in the MGC Manager. When an IP call reaches the gatekeeper (using the Network Service Prefix), the gatekeeper identifies the Network Service according to the prefix, and looks for the first available IP card on the MCU according to the cards registered with the gatekeeper for that Network Service.

Table 3-19: H.323 Dialog Box Parameters (Continued)

Field	Description
Service mode (cont.)	To use the *Board Hunting* mode and route calls to an available IP card, the dialed string must begin with the IP Service prefix. When this format is used for dial-in, the prefix can be followed by a conference/ Meeting Room numeric ID or name. When using a gateway call, the prefix can be followed by a gateway session profile or by another format that can be read by the gateway. The dialing format depends on the call type as follows: • Conference (multipoint): [H.323 prefix service] [Conference/Meeting Room numeric ID/name] • Gateway session (point to point): [H.323 service prefix] [gateway service prefix] [gateway delimiter] [gateway information] **Notes**: • This mode is dependent on the gatekeeper's implementation as the gatekeeper may not allow multiple registrations from different IP addresses. • Board Hunting is the default mode. It is not recommended to use Board Hunting with Forwarding. If both are selected, Forwarding overrides Board Hunting settings. • **Register as a Gateway** – Select this mode when using a Cisco gatekeeper. In this mode the gatekeeper is defined as a gateway. A gateway prefix is usually manually registered with the gatekeeper and the IP cards use the same prefix to register with the gateway. With a Cisco gatekeeper that supports this mode, the MCU is registered as an H.320-gateway and it requires the dialing string to start with the prefix as with Board Hunting.

Table 3-19: H.323 Dialog Box Parameters (Continued)

Field	Description
Service Mode (cont.)	**Note**: In current Cisco implementations when there is more than one IP card in use, the gatekeeper selects one of the boards that are registered with the dialed string. Thus the system does not automatically forward the calls to an available card. To overcome this problem, combine *Register as a Gateway* with *Forwarding.* However, this method only works for defined dial-in participants. • **PseudoGatekeeper** – Each IP card acts and is defined as a gatekeeper allowing Board Hunting to be performed. In PseudoGatekeeper mode, the IP cards are manually registered with the gatekeeper as neighboring gatekeepers. When the gatekeeper receives an Admission Request (ARQ) message from a participant looking for the conference alias, the gatekeeper will forward the request to all “neighboring gatekeepers” (IP cards) simultaneously. The first card that has enough resources to handle the call accepts the request. **Note**: Gatekeepers often send a multicast LRQ message hoping that there is a gatekeeper that can help with the translation. Multicast LRQ messages are not handled by the MCU IP cards within the Pseudo Gatekeeper mode. • **PseudoGatekeeper-AVF** – Applicable to the Avaya environment only.
Prefix	Enter a number to be used by H.323 participants to dial to the MCU as part of the dial-in string. Usually, one Network Service is defined for all IP cards to let the system automatically manage the resources allocated to conferences. When one Network Service is defined per card, the MGC Manager operator must manage the conferencing resources since there is no automatic pooling.

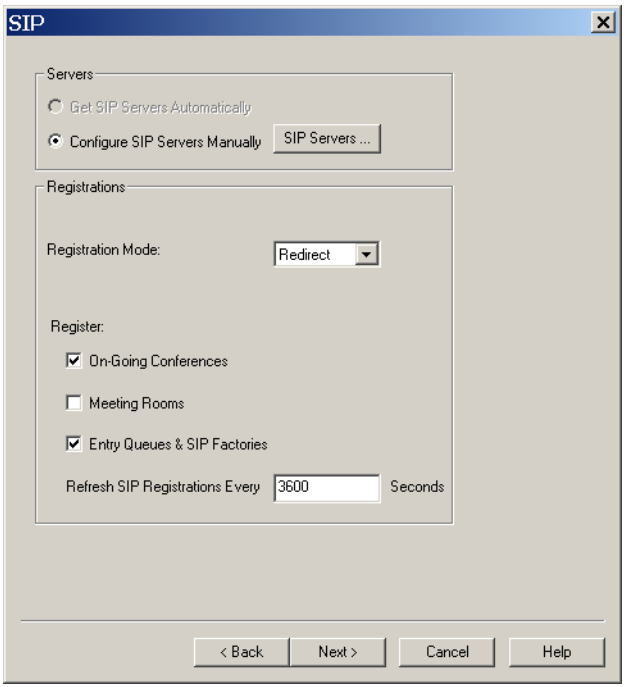
Table 3-19: H.323 Dialog Box Parameters (Continued)

Field	Description
Prefix (cont')	**Notes**: • When PathNavigator is used, this prefix automatically registers with the gatekeeper. When another gatekeeper is used, this prefix must also be defined in the gatekeeper. • When a firewall is used, two IP Network Services are usually defined; one for the card that is connected to the external network and the other one that includes all the remaining cards (those connected to the internal network).
Refresh H.323 Registrations Every n Seconds	Enter the frequency in which the system informs the gatekeeper that it is active by re-sending the IP address and aliases of the IP cards to the gatekeeper. (The conference details are not registered.) If the IP card does not register within the defined time interval, the gatekeeper will not refer calls to this IP card until it re-registers. If timeout is set to 0, re-registration is disabled. **Note:** It is recommended to use default settings.

Table 3-20: Gatekeeper Interoperability

Gatekeeper Modes/ Types	Basic	Board Hunting	Pseudo Gatekeeper	Register as Gateway
Radvision MGK-100	+	+	+	+
Radvision ECS	+	+	+	+
VCON MXM	+	+	+	+
Cisco MCM	-	-	-	+
PathNavigator/SE200	+	+	+	+
	Shading indicates the preferred configuration mode			

12. Click **Next** to continue to the *SIP* dialog box.



This dialog box is skipped when defining an H.323-only Network Service.

13. Define the following parameters:

Table 3-21: SIP Dialog Box Options

Field	Description
Servers	
Get SIP Servers Automatically	Select this option to automatically retrieve the IP address of the SIP servers. This option is enabled if a DHCP or a DNS server is enabled and the local domain name is defined (as it is required for locating the SIP proxy). If both are enabled, DNS resolution precedes DHCP as it provides the most current information.
Configure SIP Servers Manually	Select this option to manually configure the SIP servers. After selecting this option click the **SIP Servers** button to access the manual configuration window. For detailed information see "Defining SIP Servers" on page 3-77.
Registrations	
Registration Mode	The Registration Mode determines how the proxy will direct the incoming SIP call to the MCU's IP card that has enough resources to handle the call. The selection is done according to the method supported by the proxy. If all three methods are supported, the selection is done according to the required working method. • **Redirect** – The conference registers with the proxy using the IP address of a specific IP card. The proxy directs the incoming call to the registered card. If the card has no available resources, the MCU returns to the proxy the IP address of the card that does have enough resources and the proxy redirects the incoming call to that IP card. • **Forking** – Each IP card is registered in the proxy with all the conferences. The proxy directs the incoming call to all cards simultaneously. The MCU ensures that only the card that has enough resources answers the call.

Table 3-21: SIP Dialog Box Options (Continued)

Field	Description
Registration Mode (cont.)	• **Polling** – Each IP card is registered in the proxy with all the conferences and each card is assigned a priority per conference. The proxy directs the incoming call to one of the registered cards. If the card does not have enough resources, the call is rejected and the proxy redirects the call to the next card according to the card's priority. Usually, the load is distributed between the cards by registering the first conference with the first card, the second with the second card, and so on.
Register OnGoing Conferences/ Meeting Rooms/ Entry Queues & SIP Factories	Select the conferencing types and methods to register with the proxy. In SIP conferencing, the Entry Queues, SIP Factories, Meeting Rooms and conferences register with the SIP proxy. The endpoint calls the Entry Queue, SIP Factory, Meeting Room or the conference directly and not the card (as with H.323 conferencing, where the cards are registered with the gatekeeper and the dialing can be done directly to the card). Registering all the conferences with the proxy loads the proxy and the MCU as the registration is refreshed constantly (every x seconds). Therefore, it recommended to register only the Entry Queues and SIP Factories, and define all the conferences and Meeting Rooms as Entry Queue Access. All the incoming calls are routed to the Entry Queue by the proxy and from the Entry Queue to the conferences by the MCU. Reservations are not registered. **Note:** To use SIP Factories, the **Entry Queues & SIP Factories** check box *must* be selected. For more information about SIP Factories, see the MGC Manager User's Guide, Volume II, Chapter 3, "SIP Factories".

Table 3-21: SIP Dialog Box Options (Continued)

Field	Description
Refresh SIP Registrations Every n Seconds	Enter the frequency in which the system informs the SIP proxy that it is active by re-sending the details of all conference types to the server. If the various conferences and Entry Queues do not register within the defined time interval, the SIP server will not refer calls to this conference/Entry Queue until it re-registers. If timeout is set to 0, re-registration is disabled. The default value is 3600 seconds (60 minutes).

To decide which registration mode is the most appropriate, the following table lists the trade-off of each type relative to parameters such as processing load, speed, and more.

Table 3-22: Registration Modes—Pros and Cons

Factor/Mode	Redirect	Polling	Forking
Connection speed: How long it will take for an incoming call to establish its connection to the conference	2	3 The slowest connection.	1 The fastest connection.
IP card and MCU load: The amount of processing required by the MCU to complete the connection according to selected method	1 Lower load. The request is sent only to one IP card.	2 The request is sent to one card after the other.	3 Highest load. The request is sent to all cards simul-taneously.
Network load	1 Least load.	2	3 Highest Load.
Proxy dependence: How common is this mode to proxies	1 Supported by most proxies.	3 Not supported by all proxies.	3 Not supported by all proxies.

Table 3-22: Registration Modes—Pros and Cons (Continued)

Factor/Mode	Redirect	Polling	Forking
Success rate: With which method the incoming call will be successful connecting to the conference	3 If there is a problem with the IP card, it may not be able to send the IP address of the next card.	2	1 Highest connections rate.
	Shading indicates best score	1= highest score	

The following table lists the supported SIP Proxies and their Registration modes:

Table 3-23: Supported SIP Proxies and their Registration Modes

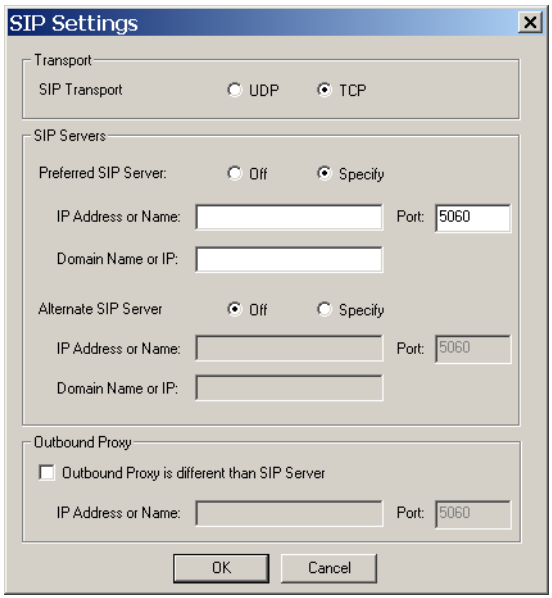
SIP Proxy	Registration Mode	Comment
Microsoft LCS 2003/2005	• Redirect	Each IP card must be configured in the Static Routes table of the LCS.
Cisco	• Forking • Redirect	
Alcatel	• Redirect • Forking	
IPTEL	• Redirect • Forking	
Nextone	• Redirect	

Defining SIP Servers

14. To configure the SIP servers manually:

    a. Click the **SIP Servers** button.

    The *SIP Settings* dialog box opens.



It is important to know which protocol the SIP proxy uses, as there are proxies that can work with only one type of protocol. The SIP transport type must reflect the correct protocol in order to communicate.

b. Define the following parameters:

Table 3-24: SIP Settings Dialog Box Options

Field	Description
Transport	
SIP Transport Type	Select the protocol that is used for signaling between the MCU and the SIP proxy or the endpoints according to the protocol supported by the SIP proxy: • **UDP** – Select this option to use UDP for signaling. • **TCP** – Select this option to use TCP for signalling. If the SIP proxy supports both protocols, select the one that is most suitable. If the selected protocol is TCP and the endpoint that is behind the proxy supports UDP, the proxy knows how to send and receive the signaling from the endpoint in UDP, even if it is defined as TCP. Transferring the signaling directly to this endpoint will fail as its protocol its different from the selected protocol.
SIP Servers	
Preferred SIP Server	• **Off** – No SIP server is used. The only dial-out option is when conference participants are defined by their IP addresses. • **Specify** – Select this option to manually define the SIP server that is used for SIP communication. This is the SIP server the MCU approaches for all its dial out needs.
IP Address or Name	If you have selected *Specify*, enter either the IP address of the preferred SIP server or its host name (if a DNS server is used).
Port	Enter the number of the TCP or UDP port used for listening. The port number must match the port number configured in the SIP server. The default port is 5060.

Table 3-24: SIP Settings Dialog Box Options (Continued)

Field	Description
Domain Name or IP	Conferences and Entry Queues can be registered in the proxy in the format *user@host*. For example, EQ1@polycom.com, where EQ1 is the user part and polycom.com is the host part. When dialing to a conference or Entry Queue, the SIP server expects to receive the host either as domain name or as an IP address. The domain name is used for identifying the SIP server in the appropriate domain according to the host part in the dialed string. For example, when the call to EQ1@polycom.com reaches its the outbound proxy, this proxy looks for the SIP server in the polycom.com domain to which it will forward the call. When this call arrives to the SIP server in polycom.com, the server looks for the registered user (EQ1) and forwards the call to this Entry Queue or conference.
Alternate SIP Server	• **Off** – No SIP server will be used in case of failure of the preferred SIP server. • **Specify** – Select this option to manually define the SIP server that will be used in case of failure of the preferred SIP server.
IP Address or Name	If you have selected *Specify*, enter either the IP address of the SIP server that will be used in case of failure of the preferred SIP server, or its domain name (if a DNS server is used).
Port	Enter the number of the TCP or UDP port used for listening. The port number has to match the port number configured in the SIP server.
Domain Name or IP	Same as for the Preferred SIP Server. Enter the domain name or IP address to identify the host and the registered Entry Queue/conference in the dialed string of the call.

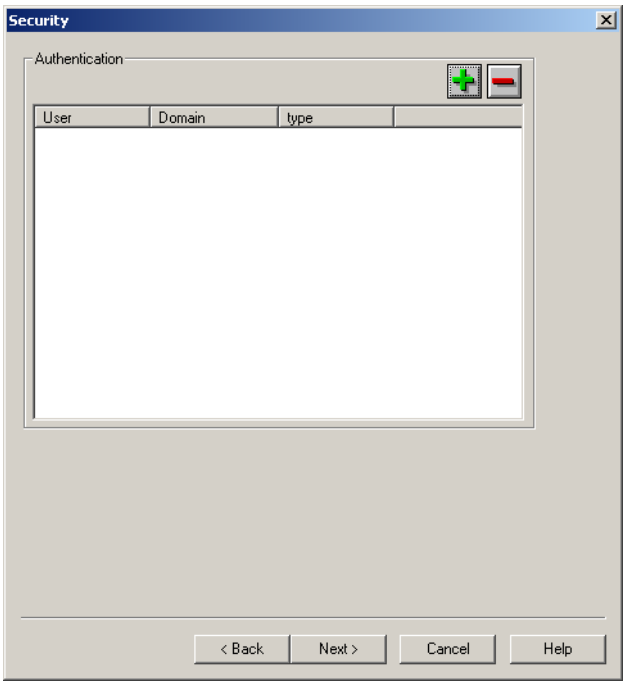
Table 3-24: SIP Settings Dialog Box Options (Continued)

Field	Description
Outbound Proxy	
Outbound Proxy is different than SIP Server	Select this check box if the outbound proxy is installed on a different computer than the one the SIP server is installed on. Usually these two entities reside on the same machine (both identification and forwarding the users to their destination). But in the instance that they are not and the entity that deals with identifying and registering users is on a different machine, select this check box.
IP Address or Name	If you have selected *Outbound Proxy is different than SIP Server*, enter either the IP address of the outbound proxy or its host name (if a DNS server is used).
Port	Enter the port number the outbound proxy is listening to. The default port is 5060.

c. Click **OK** to apply the manual server settings and return to the *SIP* dialog box.

15. Click **Next.**

The *Security* dialog box opens.



The *Security* dialog box lists the authenticated entities registered with the preferred proxy.

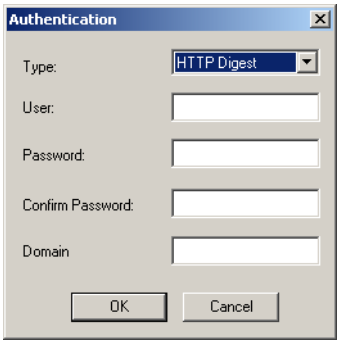
Authentication is the method used by the SIP proxy to validate the identity of the MCU and its Entry Queues and Meeting Rooms. When registering with the proxy, the MCU must provide the user name and password as configured and predefined in the SIP proxy.

Up to three entities can be defined in this dialog box. You can define the Entry Queues, Meeting Rooms, the IP cards or any combination of these entities

With Microsoft LCS 2003, each Entry Queue and conference must be registered individually and marked as Trusted.
With Microsoft LCS 2005, you can register the IP card and mark it as Trusted, hence all the conferences and Entry Queues are automatically registered as Trusted.

a. To add authenticated users to this list, click the **plus** [+] button.

The *Authentication* dialog box opens.



b. Define the authentication parameters of the Entry Queue or Meeting Room as registered with the SIP proxy.

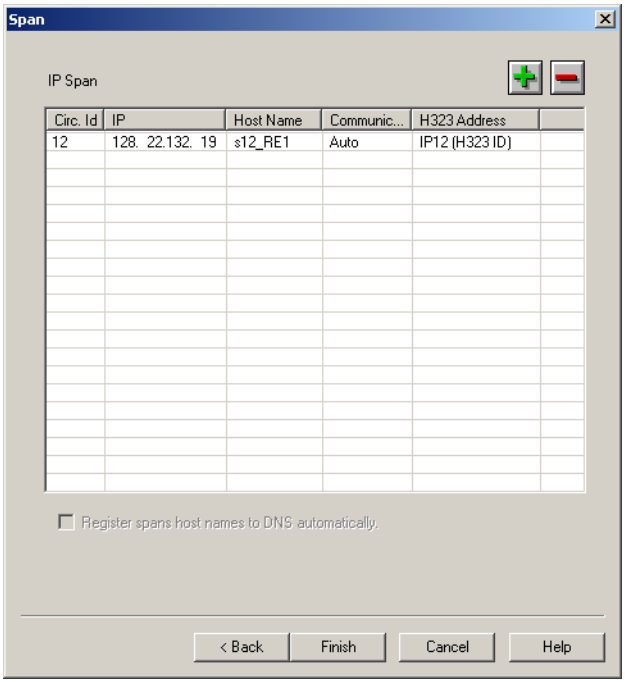
Table 3-25: Authentication Dialog Box Options

Field	Description
Type	HTTP Digest is currently the only supported authentication method. It uses basic encryption—using this authentication method the user's password is never sent in readable format. This type of authentication can be applied only if the entities (Entry Queue, Meeting Room or IP card) are entered in the proxy's users tables.
User	Enter the MCU conference, Entry Queue or Meeting Room name as registered with the proxy.
Password	Enter the conference, Entry Queue or Meeting Room password as defined in the proxy.
Confirm Password	Re-enter the password.
Domain	If the call is routed via several proxies, the user name and password are relevant to a specific domain. Enter the domain name of the SIP proxy that the user (MCU conference) is registered with.

c. Click **OK** to add this user (UA) to the authenticated users list, and return to the *Security* dialog box.

16. Click **Next**.

The *Span* dialog box opens.



This dialog box lists the currently defined spans to be used with the defined Network Service. This dialog box is used to define the cards to which the network, whose properties are defined in the Network Service, is connected. In this dialog box you define the IP cards that can be used to handle incoming and outgoing calls from/to the gatekeeper and/or SIP server.

A span defines the card's parameters and network settings; it is set separately for each IP card as each IP card has a unique IP address and can also have different capabilities than other installed IP cards.

The Circuit ID is the connection between the span and the card; it identifies the specific span with a numeric identification, which you use

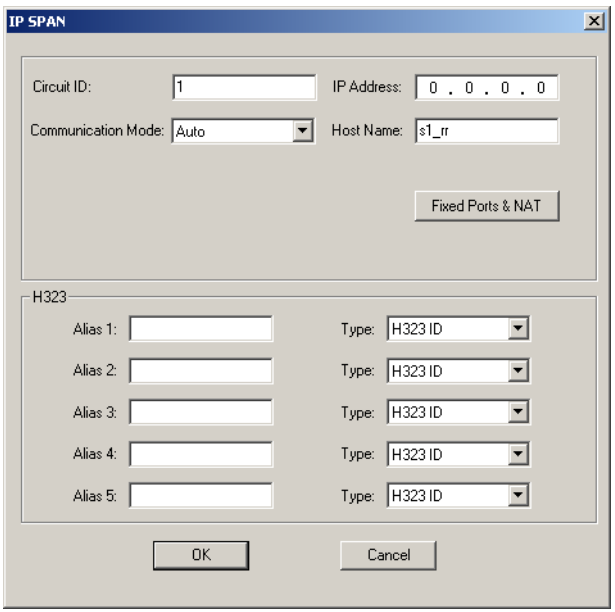
afterwards when assigning the Network Service to the IP card (for details see “Assigning Network Services to the IP/IP+ Cards” on page 3-93).

To delete an existing span, select it and click the minus (-) button.

Adding a Span

a. To add a span click the **plus** [+] button.

The *IP SPAN* dialog box opens.



This dialog box is used to define the IP card to which the IP network is connected and that should be used with this Network Service.

The IP+ cards and IP48, hardware version 4.41 and higher, can be used for both SIP and H.323 conferencing. The IP cards (IP12/24) can only be used for H.323 conferencing.

b. Define the following fields:

Table 3-26: IP SPAN Dialog Box Options

Field	Description
Circuit ID	The circuit identification is a number used to identify the card's span, it can be any whole number between 0 to 65535. This number is assigned to a specific IP address. Therefore, when defining several spans (different cards) each should be assigned a different Circuit ID number. The circuit ID must be unique per MCU. The Circuit ID is used later to assign this Network Service to the IP card (see "Assigning Network Services to the IP/IP+ Cards" on page 3-93).
IP Address	The IP address of the IP network interface card installed in the MCU. Each card has a specific IP address. This address is assigned to the Circuit ID. If the DHCP option is selected for this Network Service, this field is disabled, and shows the address 0.0.0.0, as the IP address will be retrieved from the DHCP.
Communication Mode	Indicates the data transmission rate and duplex mode. When set to *Auto* the system synchronizes the data transmission rate according to the network. You can also force the router to connect to the IP card installed in the MCU at the following data transmission rates according to the network's capabilities: • 10 Mb Half Duplex • 10 Mb Full Duplex • 100 Mb Half Duplex • 100 Mb Full Duplex **Full Duplex** refers to the transmission of data in two directions simultaneously. **Half Duplex** refers to the transfer of data in only one direction at a time.

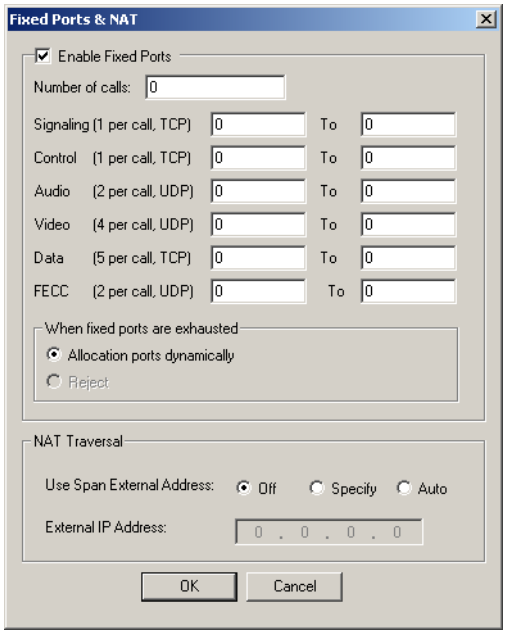
Table 3-26: IP SPAN Dialog Box Options (Continued)

Field	Description
Host Name	The name of the computer on the domain network, and that will be added to the local domain name to identify the card by its host name, for example: IP1. If the local domain name is polycom.com, the card name will be IP1.polycom.com. A default host name is suggested by the system.
Fixed Ports & NAT	Click this button to configure the firewall ports and NAT traversal. For details on this option, see “Fixed Ports & NAT Dialog Box Options” on page 3-88.
H.323	
Alias	The alias by which the IP card is identified within the network. An alias must be entered when working with a gatekeeper. Up to five aliases can be defined for each IP card.
Type	The type defines the format in which the card alias is sent to the gatekeeper. Each alias can be of a different type: • H.323 ID (alphanumeric ID) • E.164 (digits 0-9, * #) • URL ID (URL style address) • Transport ID (IP address: port number) • Email ID (email address format) • Party Number (identical to the E.164 format) **Note**: Although all types are supported, the type of alias to be used depends on your gatekeeper’s capabilities.

c. Click the **Fixed Ports & NAT** button to configure the NAT for each span—as each mapped IP should be personally known to the firewall—and the fixed signaling and media ports. Selecting Fixed Ports allows you to define the ports that are allocated in the firewall to multimedia (audio, video and data) conference calls. These ports are used for the capabilities exchange messages sent between the endpoint and the MCU during the establishment of the connection

between them. If these ports are not defined in the system, ports are randomly allocated, which can result in the firewall allocating a wider range of ports and thus be vulnerable to unauthorized network access.

NAT (Network Address Translation) Traversal is a mechanism used translate the internal IP address into a public IP address. In this dialog box you define the external IP address that will be used for the translation of the internal addresses. For more information, see "NAT Traversal" on page E-5.



d. (Optional) Define the following fields.

Table 3-27: Fixed Ports & NAT Dialog Box Options

Field	Description
Enable Fixed Ports	
Enable Fixed Ports	Select this check box to enable the configuration of firewall ports used for softening, control and media and definition of the number of concurrent calls in the IP network service. If you are defining a service for local calls that do not require configuring the firewall to accept calls from external entities, leave this check box clear.
Number of calls	Enter the Number of Calls based on the predicted number of simultaneous incoming video calls that require fixed port allocation and are handled by the network and MCU, up to the maximum that can be handled by the IP card (dependent on card type). If you exceed the maximum number of calls configured for the card an error message appears listing the call range that can be entered.
Port Range Definitions	The following general instructions apply to the *Signaling*, *Control*, *Audio*, *Video*, *data* and *FECC* fields. Individual field definitions follow the general instructions. Define the port ranges for each of the channels; enter the first port for each channel and the system automatically fills in the end of the assigned port range. The IANA recommended port range is 49152 to 65535. The network administrator configures the server and allocates firewall ports based on network requirements. In case of a firewall, the network administrator calculates the number of ports that should be allocated to video calls according to the number of ports required for each media channel (13 in total) and the volume of incoming traffic via the firewall (the number of simultaneous calls).

Table 3-27: Fixed Ports & NAT Dialog Box Options (Continued)

Field	Description
Port Range Definitions (cont.)	*For example:* If each call is allocated 13 ports (Signaling - 1, Control - 1, Audio - 2, Video - 4, and Data - 5, for a total of 13 ports), and 6 simultaneous calls are to be handled by the network, the total number of ports that is required is 78 (6 x 13). If the first allocated port is 1025, then the last port will be 2003 (1025 + 78 = 2003). In this example port number 1037 has not been allocated, as the starting range for audio and video port allocation has to be an even number. If an odd number is entered an error message appears to remind you of this requirement. **Note:** You can allocate the same port number to different channels provided the numbers are in two different protocols; one is in TCP and the other is in UDP. For example you can allocate port numbers 2000-2009 to the Signaling channel in TCP and ports 2000 -2002 to the Audio channel in UDP.
Signaling [TCP]	Define the ports used for transferring call setup messages. After you enter the beginning of the range, the system automatically fills in the end of the assigned range. If the signaling port is set to 49181, and one signaling port is allocated per call, and your total number of calls is 6, then the last number allocated by the system will be 49186 (inclusive numbering, using the port numbers 49181, 49182, 49183, 49184, 49185 and 49186 = 6).
Control [TCP]	Define the ports used for control messages (setup, maintenance, and teardown of sessions). After you enter the beginning of the range, the system automatically fills in the end of the assigned range.

Table 3-27: Fixed Ports & NAT Dialog Box Options (Continued)

Field	Description
Audio [UDP], Video [UDP]	Define the ports used for audio and video channels. After you enter the beginning of the range, the system automatically fills in the end of the assigned range. If the first audio port is 49182, and the number of audio ports per call is two, the total number of required ports for six simultaneous calls is 12. Therefore, the last port number in the range is 49193.
Data [TCP]	Define the ports used for transferring data packets: file transfer, whiteboard, and application sharing. The recommended port range is 49152 to 65535. After you enter the beginning of the range, the system automatically fills in the end of the assigned range.
FECC [UDP]	Define the ports used for FECC. After you enter the beginning of the range, the system automatically fills in the end of the assigned range.
When fixed ports are exhausted	
Allocation ports dynamically	Select this option to allocate any of the available ports in the firewall to calls that exceed the number of predicted simultaneous calls. These ports may not be secured.
Reject	Set the system to reject any request to open additional ports and the call will be rejected. If the volume of simultaneous calls exceeds the specified number of calls and there are no available ports in the firewall to handle the call, it is rejected by the network server.

Table 3-27: Fixed Ports & NAT Dialog Box Options (Continued)

Field	Description
NAT Traversal	
Use Span External Address	Define the method in which the public IP address is mapped to the IP card's internal address: **Off** – No external IP address will be used. Select this option for local calls, there is no need to use the public IP address to identify the source and destination for the messaging. **Specify** – Select this option to manually define the IP card's public IP address. **Auto** – The IP card's public IP address is automatically retrieved from the HTML Answer of the external server. http://videovideo.polycom.austin.com. The automatically retrieved IP address appears in the **IP Card Settings-IP-Network Parameters** tab.
External IP address	If you selected *Specify,* enter the IP card's public IP address.

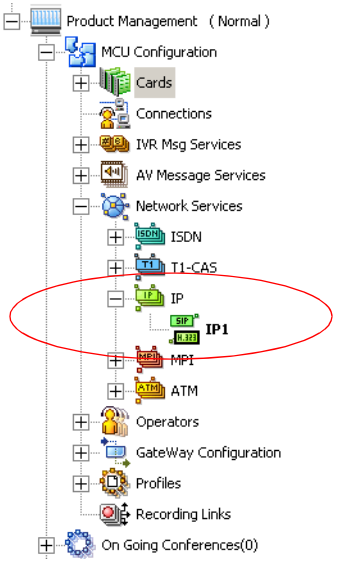
Notes: For a complete port configuration you define both the fixed ports (signaling, media, etc.) and the relevant reserved ports. Make sure that the following IANA registered ports reserved for system services have been opened as part of your firewall's definitions:

- Port # 1720 – H.323 standard signaling port
- Port # 1719 – H.323 gatekeeper port
- Port # 1503 – T.120 port for incoming connections
- Port # 5060 –SIP standard signaling port

Entering a well-known port that the IANA has reserved for other applications in your configuration is not allowed as it would result in system service failure. It is highly recommended to use ports from the dynamic range defined by IANA.

17. Click **OK** to return to the *Span* dialog box.
    The new span is added to the *Spans* table.

18. In the *Spans* dialog box, click **Finish** to complete the IP Network Service definition.
The new network service is added to the IP Network Services list.



The following icons are used to indicate the IP Network Service type:

Table 3-28: IP Network Service Icons

Icon	Description
	The Network Service supports both SIP and H.323 connections.
	The Network Service supports only H.323 connections.
	The Network Service supports only SIP connections.

Assigning Network Services to the IP/IP+ Cards

For each IP card installed in the MCU, you need to define which Network Service is used, thereby defining the network properties connected to that card.

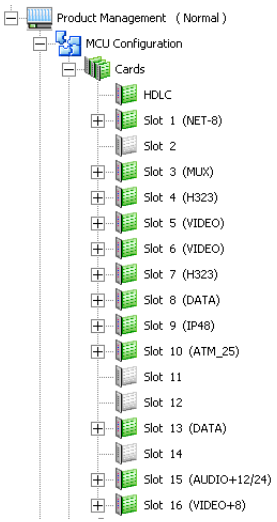
Usually, one Network Service is used for all IP cards, enabling the MCU to automatically manage the conferencing resources.

The association between the network properties and the IP cards is done in two stages. In the first stage, while defining the IP Network Service, you add all the IP cards that can use this Network Service (they are all using the same IP network entities such as gatekeeper, DNS, SIP server or DHCP). In the second stage, you define for each IP card which Network Service it uses to manage conferencing calls.

For SIP conferences, or conferences that include SIP participants, IP+ cards from version 4.23 or higher are required. For H.323-only conferences, IP (12 or 24) cards are sufficient.

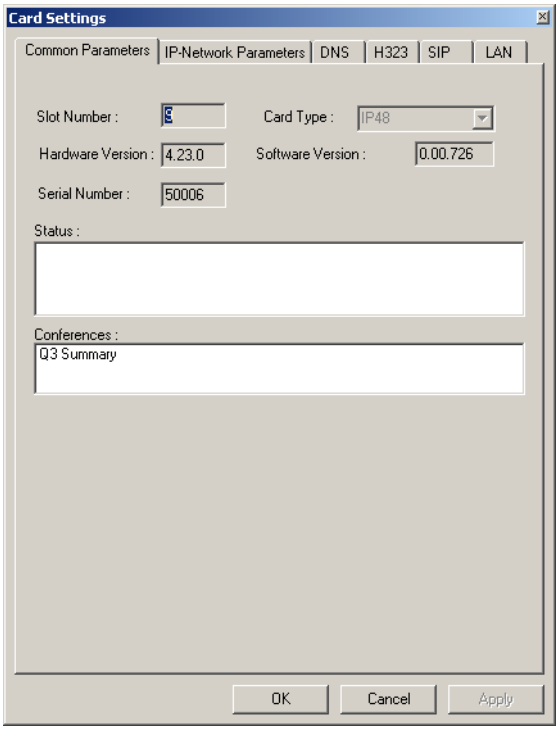
To assign IP service settings to the IP card:

1. In the *Browser* area, expand the *MCU* tree.
2. Expand the *MCU Configuration* tree.
3. Expand the *Cards* tree.



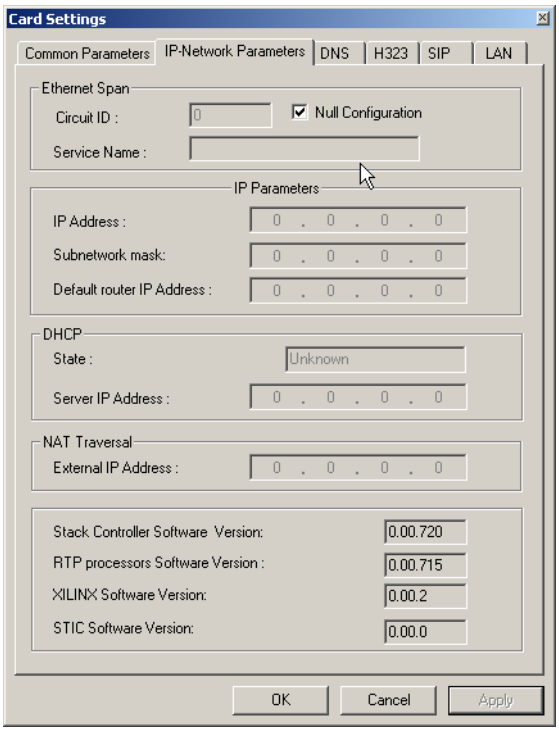
4. Double-click the IP card.
   Alternatively, right-click the IP card icon, and then click **Properties**.

   The *Card Settings-Common Parameters* dialog box opens.



   The **Common Parameters** tab is for viewing purposes only.

5. Click the **IP-Network Parameters** tab.



6. In the **IP-Network Parameters** tab clear the **Null Configuration** check box to enable assignment of the IP Network Service.
7. In the **Circuit ID** box enter the circuit ID that was defined for this card in the *IP Network Service—Spans* dialog box. For additional information on circuit IDs see "IP SPAN Dialog Box Options" on page 3-85.
8. Click **Apply**.

   The name of the IP Network Service is displayed in the *Service Name* field.

Working with Microsoft LCS

Ongoing conferences with Microsoft Office Communicator participants can span over several IP+ cards. Once the an IP+ card is full, the MCU forwards the call to the next IP+ card without involving the endpoint or the LCS server in the process.

In version 7.5, when the MCU was configured to work in Microsoft SIP-CX environment, all IP+48 cards were configured to connect up to 24 IP participants (H.323, standard SIP and Office Communicator SIP-CX participants) per card (instead of 48 participants).

In version 8.0, only IP+48 cards that are assigned to the IP Network Service designated to work in SIP-CX environment are limited to 24 IP participants. All other IP+48 cards installed in the MCU can connect up to 48 H.323 and standard SIP participants using a non SIP-CX IP Network Service.

To designated an IP Network Service for SIP-CX connections, the appropriate system.cfg flags must be modified.

Modifying the system.cfg Flags

The SIP-CX environment is enabled for the MCU in the system.cfg, in the SIP Section, by setting the flag SIP_CONF_WATCH_CONTROL to YES. (This flag is available also in version 7.5.)

To designate a SIP-CX enabled IP Network Service, in the system.cfg, in the SIP Section, set the prefix of the IP network service name in the flag MSFT_IP_SERVICE_NAME_PREFIX.

For example, if you enter MICROSOFT as the prefix, the IP Network service whose name starts with MICROSOFT (MICROSOFT1, MICROSOFT2, etc.) will be considered by the system as SIP-CX enabled.

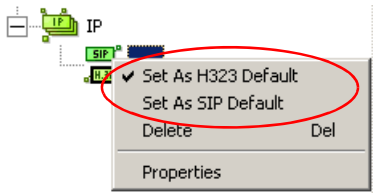
Setting the Default IP Network Service

When defining participants, the default Network Service is assigned to the participant according to the participant's connection type, unless you explicitly assign a different one.

With IP Network Services, you can define one IP Network Service as default for H.323 connections and another Network Service as default for SIP connections. If the IP Network Service supports both H.323 and SIP connections, you can set the same Network Service as default for both H.323 and SIP, or for H.323-only or for SIP-only.

To designate an IP Network Service as the default IP Network Service:

1. In the *Browser* pane, connect to the MCU and expand its tree.
2. Expand the *MCU Configuration* tree.
3. Expand the *Network Services* tree.
4. Expand the *IP Network Services* tree.
5. Right-click the IP Network Service to be set as the default, and then click **Set As H.323 Default,** or **Set As SIP Default**.



The next time you access this menu, a check mark is added next to the network service type to indicate its selection as default.

To set this IP Network Service for both H.323 and SIP connections, repeat step 5 and select the option you need.

The following icons are used to indicate the default IP Network Service type:

Table 3-29: Default IP Network Service Icons

Icon	Description
	This Network Service supports both SIP and H.323 connections and is designated as default for both SIP and H.323 connections.
	This Network Service supports both SIP and H.323 connections and is designated as default for H.323 connections.
	This Network Service supports both SIP and H.323 connections and is designated as default for SIP connections.
	This Network Service supports only H.323 connections and is set as default for H.323 connections.
	This Network Service supports only SIP connections and is set as default for SIP connections.

Defining an MPI Network Service

The MGC unit supports connection to endpoints communicating with protocols such as V.35, RS-449 and RS-530 over a serial connection. The MCU can either be Data Terminal Equipment (DTE) or Data Communication Equipment (DCE).

DCE (Data-Communications Equipment): The equipment that enables a DTE (the MCU in Figure 3-1) to communicate over a telephone line or data circuit. The DCE establishes, maintains, and terminates a connection, and performs the conversions necessary to enable communication over an ISDN network. It provides the clock to the ports, which are connected to the DCE. In the configuration described in Figure 3-1, the DCE transmits and receives data from the MCU using a serial connection and distributes the data to the appropriate channels of the ISDN connection.

DTE (Data Terminal Equipment): User devices, such as terminals and computers that connect to data communications equipment (DCE); they either generate or receive the data carried by the network.

When the MCU acts as a DTE it dials the number of the endpoint. This number is transferred over a serial connection to the DCE. The DCE translates this number to the appropriate ISDN switch where it may be routed to an ISDN endpoint or to another DCE connected serially to an endpoint.

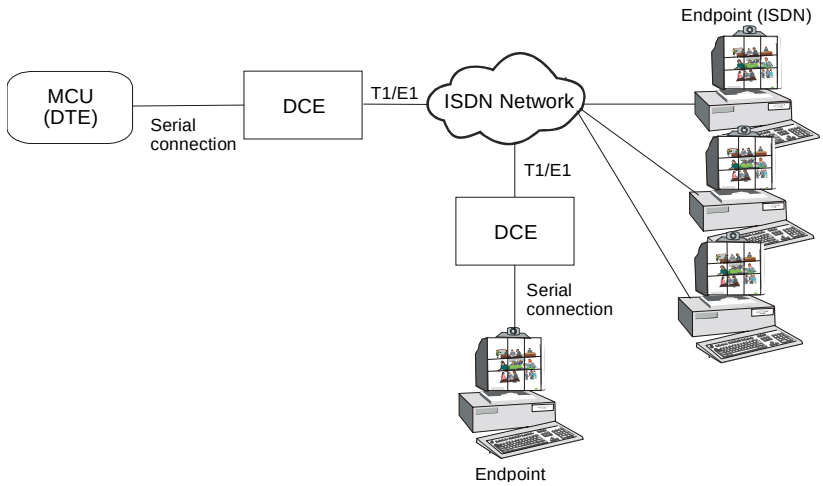


Figure 3-1: Typical Configuration With Serial Connection - MCU as DTE

When the MCU acts as a DCE it is able to communicate directly with an endpoint over a serial connection, by dialing the endpoint's number or using a dedicated line. The DCE can also connect to an ISDN endpoint. It does so by dialing the endpoint's number. This number is transferred over a serial connection to another DCE. The DCE then translates the number to the appropriate ISDN switch where it may be routed to an ISDN endpoint.

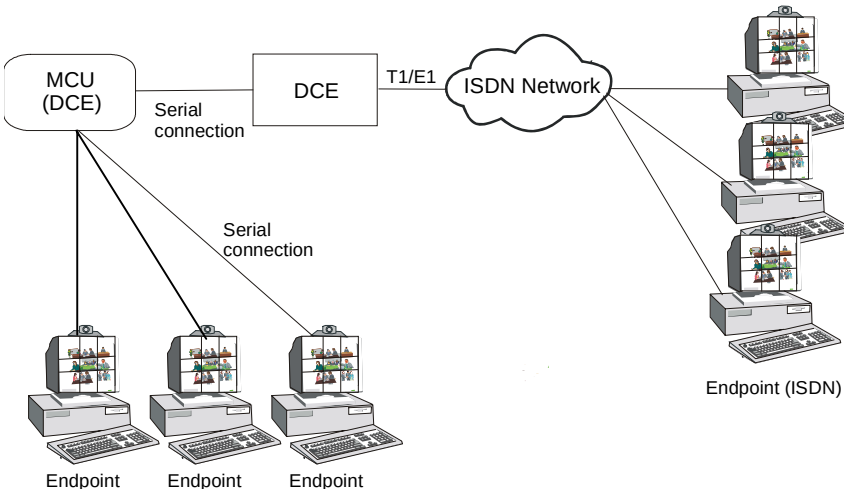


Figure 3-2: Typical Configuration With Serial Connection - MCU as DCE

The MPI (Multi Protocol Interface) box together with the MPI-8 Network interface card installed in the MGC unit provide the interface from the MGC unit to the serial components in the network.

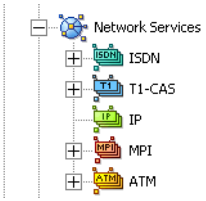
Defining a New MPI Network Service

To set up a conference with endpoints connecting over a serial connection a special Network Service must be defined in the Network Service. The MPI box must be installed prior to the definition of the MPI Network Service. See "MPI-8 Hardware Installation for the MGC-100" in the Hardware & Installation Manual.

To define a new MPI Network Service:

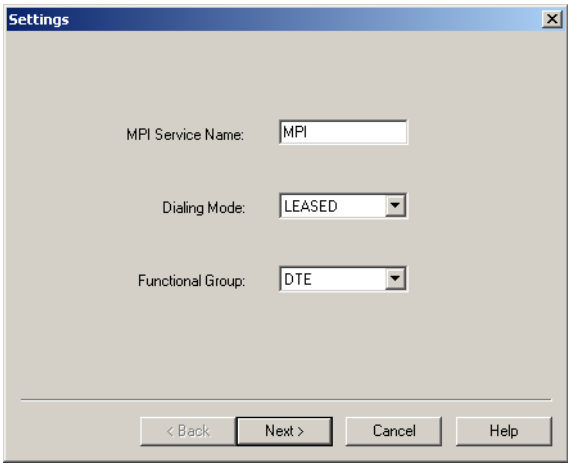
1. Connect the MGC Manager to an MCU. For more information, see the MGC Manager User's Guide, Volume I, Chapter 3, "Connecting to an MCU".
2. In the *Browser* pane, click the plus [+] icon next to the *MCU* icon to list its options.
3. Double-click the *MCU Configuration* icon, or click the plus [+] icon next to the *MCU Configuration* icon, to expand the configuration options tree.
4. Double-click the *Network Services* icon, or click the plus [+] icon next to the *Network Services* icon.

   A list of Network Service types is displayed below the *Network Services* icon.



5. Right-click the *Network Services–MPI* icon, and then click **New MPI Service**.

The *Settings* dialog box opens.

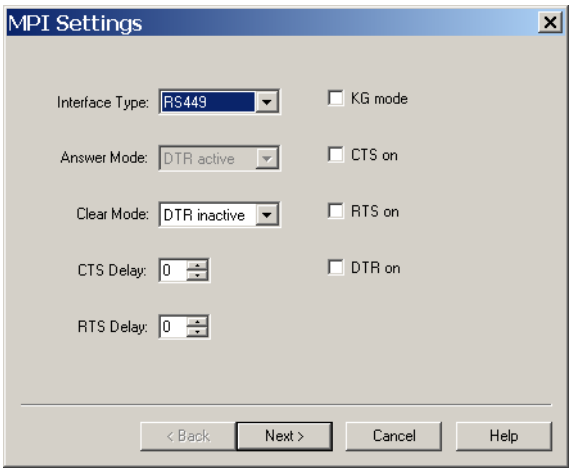


6. Define the following parameters:

Table 3-30: Settings Dialog Box Options

Field	Description
MPI Service Name	Specify the service name, using up to 20 characters. The *MPI Service Name* identifies the service to the system.
Dialing Mode	You can connect the MCU to the endpoints via leased lines, or via a switch that requires dialing to the endpoint. Select **Leased** for direct connection between the MCU and the endpoint. Select **Dial** for dial-up connection between the MCU and the endpoint.
Functional Group	If *Leased* is selected, you may select whether the MCU acts as DCE or DTE. If *Dialing* is selected, the system automatically sets the MCU as DTE.

7. Click **Next** to continue.
   The *MPI Settings* dialog box opens.



   The MPI settings parameters are used to identify the serial protocol used between the MCU and the DCE.

8. Define the following parameters:

Table 3-31: MPI Settings Dialog Box Options

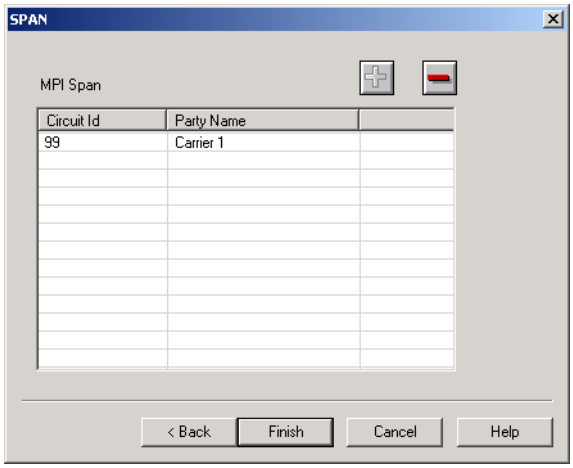
Field	Description
Interface Type	Select from the drop down list the serial protocol used between the DCE and the MGC unit. The available protocols are RS-449 (which is the default), V.35 and RS-530. The selected protocol defines the way data is transmitted via the serial connection and how it will be interpreted by the MPI Network Interface module.
Answer Mode	Indicates how the MGC unit answers the call. **DTR active** is the option automatically set by the system.
Clear Mode	Indicate how the call is terminated. **DTR inactive** indicates that the call is terminated when a DTR signal becomes inactive. Select **Terminal** when the call is terminated by the DCE (hanging up from the DCE).

Table 3-31: MPI Settings Dialog Box Options

Field	Description
CTS Delay	The CTS (Clear To Send) delay indicates when to start synchronizing with the clock signals sent from the DCE. Some DCEs send a CTS signal before the channels are BONDED. In these cases, a delay should be entered.
RTS Delay	Delay between DTR (Data Terminal Ready) active and RTS (Request to Send) active. Usually, it will be set to 0 (zero), but some DCE equipment may require a delay between the activation of these signals.
KG Mode	Select this check box when an encryption device is used.
CTS On	Select this check box when the DCE does not return the *Clear to Send* signal as expected. When this option is checked, the MCU sends the data to the DCE without waiting for the CTS signal from the DCE. When On, the signal is sent continuously.
RTS On	Select this check box when the endpoint does not return the *Request to Send* signal as expected. In such a case, the DCE will get the RTS signal and will return the clock and required signals from the endpoint. When On, the signal is sent continuously.
DTR On	Select this check box when the endpoint does not return the *Data Terminal Ready* signal as expected. In such a case, the DCE will receive the DTS signal and will return the clock and required signals from the endpoint. When On, the signal is sent continuously.

9. Click **Next** to continue.

The *Span* dialog box opens.

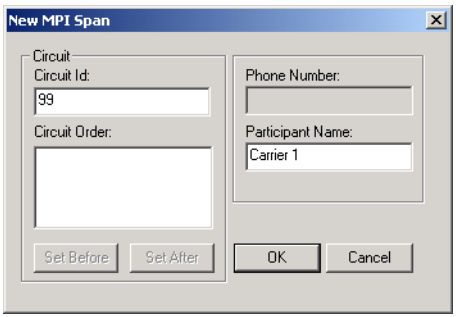


The Span dialog box displays the list of spans currently defined in the system. This dialog box is used to assign circuit identification numbers and the phone numbers to be used in dial-in conferences. Circuit orders are automatically assigned to spans. If all the DCE ports are connected using the same protocol and characteristics, one network service may be defined. In such a case, a separate circuit Id and phone number must be defined for each port. These numbers will be used to identify the participant and display the participant phone number in the *Status* and *Monitor* pane during an On Going Conference.

The phone number has no influence on receiving or rejecting calls. It is used only to attach a participant to a specific port.

10. Click the **Plus** button to define a new span.

The *New MPI Span* dialog box appears.



11. Define the following parameters:

Table 3-32: New MPI Span Dialog Box Options

Field	Description
Circuit ID	The Circuit Identification is a logical number used to identify the span to the MGC Manager. This number is later used to assign the span to the network interface card. Type an integer from 0 to 65535, to be used as the circuit identification number in the MGC Manager. If you enter any other number, the system will reject it and you will be prompted to re-assign the circuit identification number. **Note:** If other services are already defined, make sure to use numbers other than those already assigned to the existing services.

Table 3-32: New MPI Span Dialog Box Options (Continued)

Field	Description
Circuit Order	The circuit order determines the span order in which an MCU dials out. The Circuit Order is assigned automatically by the system according to the order in which the spans are added. In dial-out connections, when the operator calls the participant, the MGC unit allocates ports from the spans starting with the span having the lowest number and the lowest port number within that span. You can change the span order (if there are several spans defined in the system) using the **Set Before** or **Set After** buttons. To do so: 1.Click the name of a circuit in the Circuit Order list, which is to be adjacent to the circuit you are defining. The circuit's entry is highlighted. 2. To insert the new circuit, do one of the following: • Click **Set Before** to insert the new circuit before the highlighted entry. Click **Set After** to insert the new circuit after the highlighted entry.
Phone Number	Enter the number of the DCE port that will be used by a dial-in participant when connecting to the conference. This number is used to identify the participant name when a dial-in participant connects to the conference. According to the span carrying the call, the system identifies the Network Service and takes the phone number from it. This phone number is also defined in the *Participant Properties* dialog box (as the CLI number). The system is therefore able to display this participant's name in the *Monitor* and *Status* panes. **Note:** The *Phone Number* box is only enabled when the *Dialing Mode* is set to **Dial** in the *Settings* dialog box.

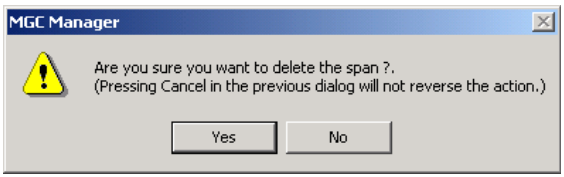
Table 3-32: New MPI Span Dialog Box Options (Continued)

Field	Description
Participant Name	When using a leased line, type the participant's name, so that the MCU can identify the endpoint. **Note:** The *Participant Name* box is only enabled when the *Dialing Mode* is set to **Leased** in the *Settings* dialog box.

12. Click **OK** to confirm your settings.
    You are returned to the *Span* dialog box and the new span definition is added to the Spans table.
13. Repeat steps 10 to 12 to define additional spans.

    To delete a span from the table, highlight the span to delete and click the **Minus** button.

    A confirmation dialog box is displayed.



    Select **Yes** to confirm or **No** to cancel.
14. Click **Finish** to complete the MPI Network Service definition.

    The new MPI Network Service is added to the *MPI Network Services* list in the *Browser* pane.

To set up an MPI Network service as the default or to modify the Network Service parameters, follow the procedure described for all other Network Services. For details, see "Modifying a Network Service" on page 3-124 and "Defining a New MPI Network Service" on page 3-101.

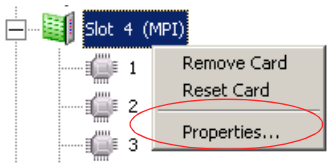
Assigning the MPI Network Service to the MPI Network Interface Module

To enable the connection between the MGC unit and DCE, you must assign the MPI network service to the appropriate span of the MPI Network interface module.

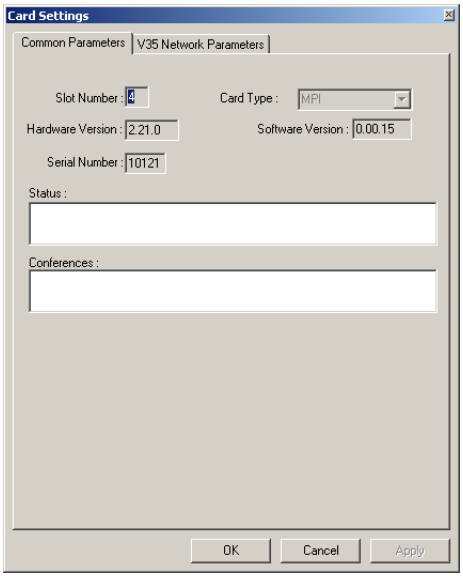
For information about clocking in a serial-only environment (no ISDN), see "Clocking in Serial Environment" on page 5-142.

To assign the Network Service to the MPI Network Interface module:

1. In the *Browser* pane, right-click the slot containing the MPI card and then click **Properties**.
   Alternatively, double-click the slot containing the MPI card.



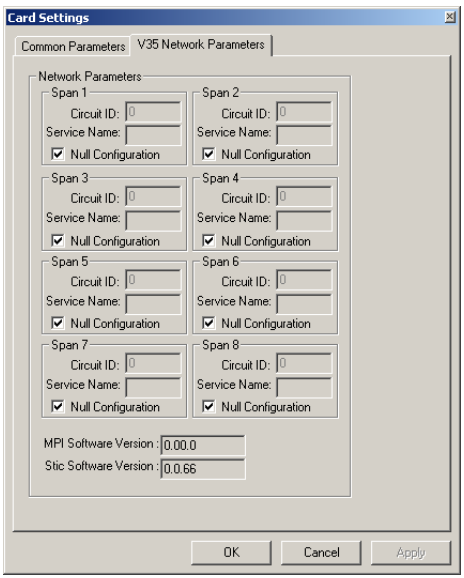
The *V.35 Card Settings–Common Parameters* dialog box opens.



This dialog box displays the settings common to all modules. These parameters are described in Chapter 4, “Viewing the Common Card Parameters” on page 4-10.

2. Click the **V35 Network Parameters** tab.

This tab contains settings specific to the MPI Network Interface module.



Each of the spans listed here represents one serial port on the MPI Box.

3. To assign a circuit ID to the appropriate port:

   a. In the *Span n* box (where *n* is the port number on the MPI Box to which the serial cable connects), clear the **Null Configuration** check box to enable this port.

   b. In the *Circuit ID* box, enter the circuit ID as defined in the *Network Service–Span* dialog box. According to the selected circuit ID, the Network Service is assigned to the MPI network card. A different circuit ID must be assigned to each port. The circuit IDs can be taken from the same Network Service or from different Network Services, if the port characteristics are different.

   c. Click **Apply**.
   The name of the Network Service appears in the *Service Name* box.

4. Click **OK**.

Defining an ATM Network Service

ATM (Asynchronous Transfer Mode) is a network technology based on transferring data in cells or packets of a fixed size. The cell used with ATM is relatively small compared to units used with older technologies. The small, constant cell size allows ATM equipment to transmit video, audio, and computer data over the same network, and assure that no single type of data hogs the line. ATM provides connectivity to LANs, WANs, private and sub-networks. It supports applications requiring high transmission speeds, large transmission capacities and bandwidth on demand, transports voice, video and data traffic on common networks and provides effective network management.

A typical system configuration when working with an ATM service includes the MGC unit, a switch and a UNI address router (V-Gate). The V-Gate stores the UNI address book containing a table of dialed numbers and their equivalent UNI address. To connect between endpoints and the MCU in an ATM network, the UNI addresses of the endpoints have to be transferred from the V-Gate to the switch. This configuration is exclusive to First Virtual (FVC) ATM networks.

The ATM-25 Network Interface module installed in the MCU contains 64 channels and it supports up to 10 H.321 endpoints at 2B or 384 Kbps. The ATM-155 Network Interface module installed in the MCU contains 128 channels and it supports up to 20 H.321 endpoints at 2B or 384 Kbps. The following table summarizes the port capacity in different line rates:

Table 3-33: Port Capacity Line Rates

Line Rate	# of Ports at 25 Mbps	# of Ports at 155 Mbps
2B or 384 Kbps	10	20
512 Kbps	8	16
768 Kbps	4	8
2MB	2	4

Data Flow

In a dial-out conference (Figure 3-1), the MCU dials the number of the endpoint. This number is transferred via the switch (which is connected to the ATM network) to the V-Gate. The V-Gate translates the dialed number to the appropriate UNI address and sends it back to the MCU. The MCU now connects to the endpoint.

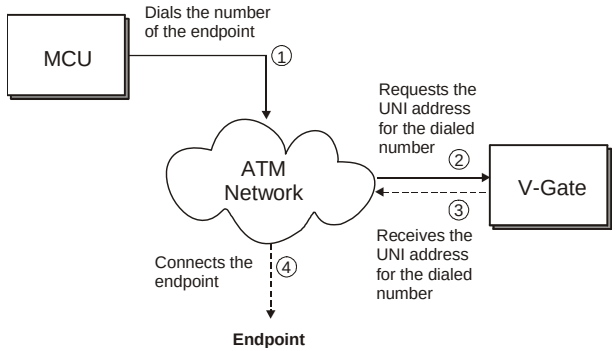


Figure 3-3: Data flow in dial-out conferences

In a dial-in conference (Figure 3-2), the endpoint dials the MCU number. This number is transferred via the switch (which is connected to the ATM network) to the V-Gate. The V-Gate translates the dialed number of the MCU to the appropriate UNI address and sends it back to the endpoint. The endpoint now connects to the MCU.

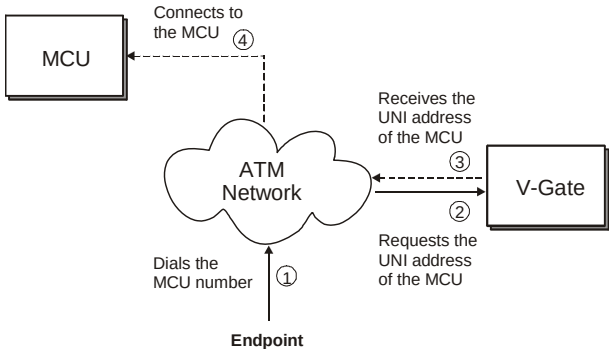


Figure 3-4: Data flow in dial-in conferences

ATM Setup Flow

ATM setup and configuration consist of the following procedures:

- Defining the ATM Network Service. For details, see “Defining a New ATM Network Service” on page 3-114.
- Configuring the ATM card. For details, “Assigning the ATM Network Service to the ATM Network Interface Module” on page 3-121.
- Defining the UNI address of the MCU and the endpoints in the V-Gate. To accomplish this task you will need to obtain the UNI number of the ATM card installed in the MCU. For details on how to obtain the UNI address and define these numbers in the V-Gate application refer to the V-Gate's User's Guide.

These steps are identical for ATM-25 and ATM-155 Network Interface Modules.

Defining a New ATM Network Service

The ATM Network Service is used to define the UNI address of the V-Gate, which allows communication between the MCU and the V-Gate. In addition, you need to define the span and the dial-in phone numbers to be used by the conference participants.

Before defining an ATM service, you should:

- Make sure that the ATM Network Interface module is installed in the MCU. If not, install it first.
- Obtain the UNI address of the V-Gate.
- Make sure that the MCU power is on.

To define a new ATM Network Service:

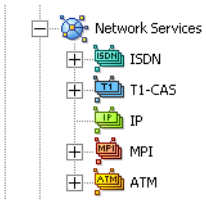
1. Connect the MGC Manager to the MCU. For more information, see the MGC Manager User's Guide, Volume 1, Chapter 3, “Connecting to an MCU”.
2. In the *Browser* pane, double-click the *MCU* icon, or click the plus [+] icon next to the *MCU* icon.

   A list of options is displayed below the MCU icon.
3. In the MCU options list, double-click the *MCU Configuration* icon, or click the plus [+] icon next to the *MCU Configuration* icon.

A list of configuration options is displayed below the *MCU Configuration* icon.

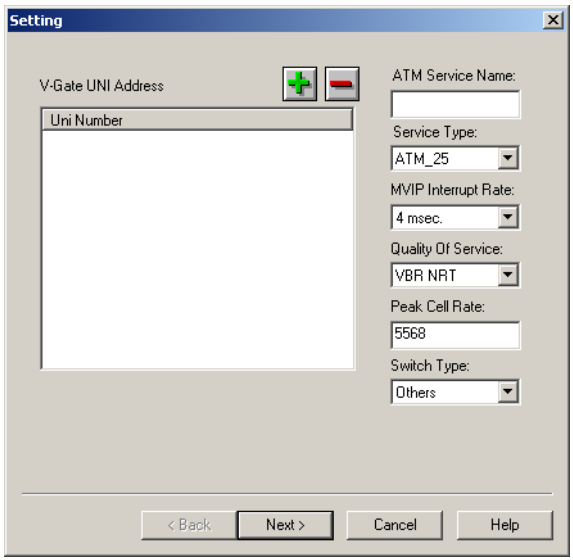
4. Double-click the *Network Services* icon, or click the plus [+] icon next to the *Network Services* icon.

   A list of Network Service types is displayed below the *Network Services* icon.



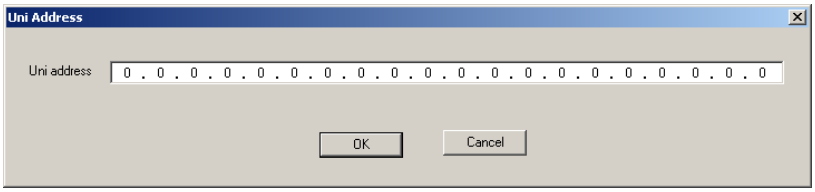
5. Right-click the *ATM* icon, and then click **New ATM Service**.

The *Setting* dialog box opens.

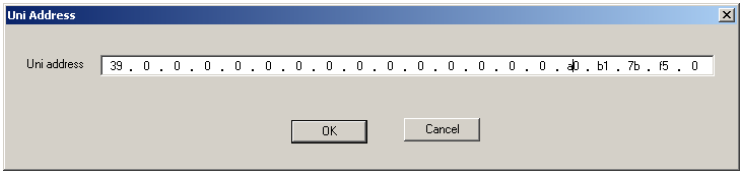


This dialog box is used to define the properties of the ATM network, and UNI address of the V-Gate. These properties should be obtained from your service provider.

6. Click the **Plus** button in the *V-Gate UNI Address* pane.
   The *UNI Address* dialog box opens.



7. Enter the V-Gate's UNI Address.
   Usually, the first number and the last six numbers in the UNI address are modified.
   The V-Gate UNI Address is defined by the operator. It stores the address book of the endpoints UNI Addresses.



8. Click **OK**. The UNI address is added to the *V-Gate UNI Number* list
   Up to six V-Gates may be defined in the system. The order in which the V-Gates are defined determines the order in which they will be addressed by the MGC unit when searching for the UNI Address of endpoints.
   To define additional V-Gates, repeat steps 7 and 8.

   To delete a *UNI Number* from the UNI number list, select the desired number, and then click the **Minus** button in the V-Gate UNI Address pane.

   A confirmation dialog box is displayed.

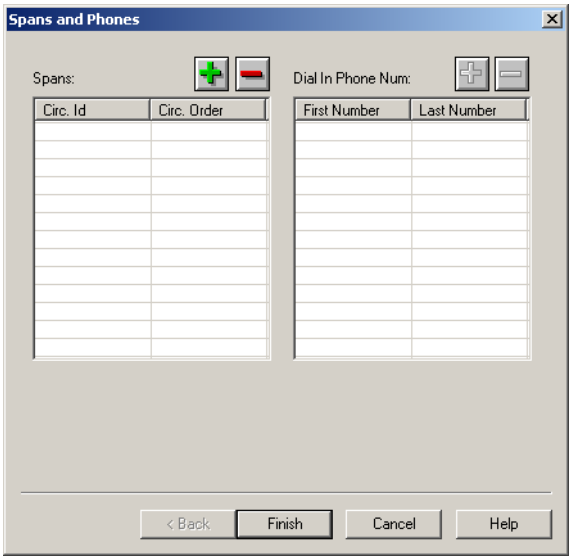
   Select **Yes** to confirm or **No** to cancel.

9. Define the following parameters:

Table 3-34: ATM Settings Dialog Box Options

Field	Description
ATM Service Name	Enter the Network Service name using up to 20 characters. The ATM Service Name identifies the service to the system.
Service Type	Select the network transfer rate from the drop-down list according to the ATM Network Interface module installed in your system. There are two network transfer rates currently available for ATM networks: ATM-25 (which is the default) – for a transfer rate of 25 Mbps, and ATM-155 – for a transfer rate of 155 Mbps.
MVIP Interrupt Rate	An internal parameter used by the VC-NIC. By default, the MVIP Interrupt Rate is set to 4 milliseconds. This value can be modified to 8 milliseconds, but should only be changed with the authority of a support engineer.
Quality of Service	**CBR** – Constant Bit Rate. Used for real time applications like voice and audio. **VBR-RT** – Variable Bit Rate – Real Time. Similar to CBR. This service allows statistical multiplexing and consistent service quality to applications such as compressed voice and audio. **VBR-NRT** – Variable Bit Rate – Non-Real Time. This service is defined for non-real time applications whose data transfer is performed in random bursts.
Peak Cell Rate	The maximum cell rate at which a source may send its cells during the connection lifetime.
Switch Type	There are two types of switches that can be used depending on the default Quality of Service settings. **Others** – Set this switch type when the default Quality of Service settings is **VBR-RT**. **FORE Switches** – Set this switch type when working with FORE Swithes and the default Quality of Service settings is **VBR-NRT**.

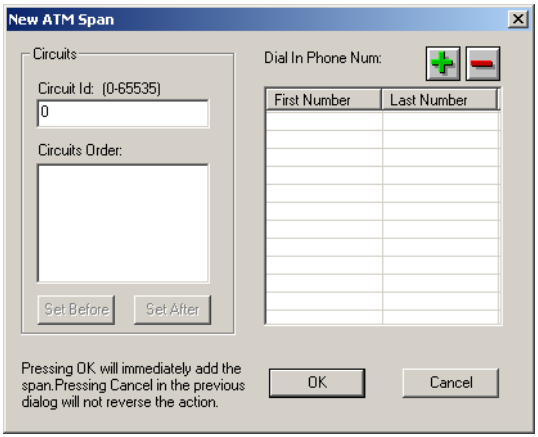
10. Click **Next**.
    The *Spans and Phones* dialog box opens.



    This dialog box is used to assign identification number to the spans used by the service provider. For more details, see “Spans and Phones Dialog Box” on page 3-14.

11. Click the **Plus** button in the *Spans* pane to define the ATM span.

    The *New ATM Span* dialog box opens.



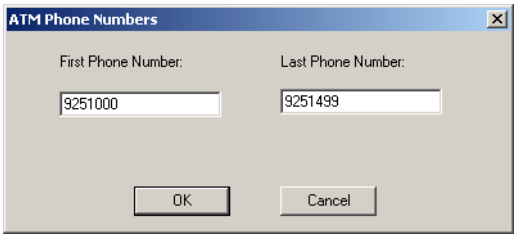
12. Define the following parameters:

Table 3-35: New ATM Span Dialog Box Options

Field	Description
Circuit Id (0-65535)	The Circuit Identification is a logical number used to identify the span to the MGC Manager. This number is later used to assign the span to the network card. Type any integer number from 0 to 65535, to be used as the circuit identification number in the MGC Manager. **Note:** If there are other Network Services defined in the system, the Circuit ID must be a unique number, not used by any other Network Service.
Circuit Order	The circuit order determines the span order in which an MCU dials out. The Circuit Order is assigned automatically by the system according to the order in which the spans are added. In dial-out connections, when the operator calls the participant, the MGC unit allocates ports from the spans starting with the span having the lowest number and the lowest port number within that span. You can change the span order (if there are several spans defined in the system) using the **Set Before** or **Set After** buttons. To do so: 1.Click the name of a circuit in the Circuit Order list, which is to be adjacent to the circuit you are defining. The circuit's entry is highlighted. 2. To insert the new circuit, do one of the following: • Click **Set Before** to insert the new circuit before the highlighted entry. • Click **Set After** to insert the new circuit after the highlighted entry.

13. Click the **Plus** button in the *Dial In Phone Num* pane to define the numbers that will be used in dial-in conferences.

The *ATM Phone Numbers* dialog box opens.



14. Enter the range of numbers that can be used in the dial-in connection.
    In the *First Phone Number* box, enter the first number in the range of dial-in numbers.

    In the *Last Phone Number* box, enter the last number in the range of dial-in numbers.

- The range of dial-in numbers should not exceed 1000 numbers. For example: from 2000 to 2999.
- It is recommended to define a separate range for dial-in numbers using ISDN services and those using ATM service. For example, 2000 to 2999 for ATM dial-in numbers and 5000 to 5999 for ISDN dial-in numbers.

15. Click **OK**.
    The system returns to the *New ATM Span* dialog box displaying the new phone numbers.

    To remove a phone number range, select the range in the *Dial In Phone Num* pane, and then click the **Minus** button.

    The dial-in numbers should also be defined in the V-Gate, assigning them the UNI number of the ATM card installed in the MCU. This is done at the end, once the circuit order is assigned to the appropriate Span in the card configuration.
16. Click **OK**.
    The system returns to the *Spans and Phones* dialog box.
17. Click the **Finish** button.
    The new ATM service is added to the ATM services list in the *Browser* pane of the MGC Manager main window.

Completing the ATM Service Definition

To complete the definition of the ATM network service you need to:

- Assign the circuit ID to the span of the ATM Network Interface module. This procedure is described in "Assigning the ATM Network Service to the ATM Network Interface Module" on page 3-121.
- Obtain the UNI address of the ATM card installed in the MCU. For more details, see "Assigning the ATM Network Service to the ATM Network Interface Module" on page 3-121.
- In the V-Gate application, define the UNI address of the ATM Network Interface module are installed in the MCU in order to identify the network.
- Make sure that the UNI address of all endpoints connected to the network are defined in the V-Gate application and define the missing ones, if required.

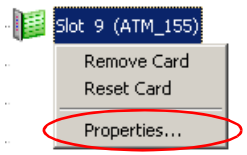
Assigning the ATM Network Service to the ATM Network Interface Module

In order to connect the MCU to the ATM network (and the V-Gate), you must configure the ATM Module in conjunction with the ATM Network Services defined in the MGC Manager. The configuration of the ATM-25 and ATM-155 Network Interface module is identical for both cards.

To assign the Network Service to the ATM Network Interface module:

1. From the MCU expanded options list, click the plus [+] icon next to the *MCU Configuration* icon, or double-click it.
2. Expand the *Cards* list by clicking the plus [+] icon next to the *Cards* icon or double-click the *Cards* icon.

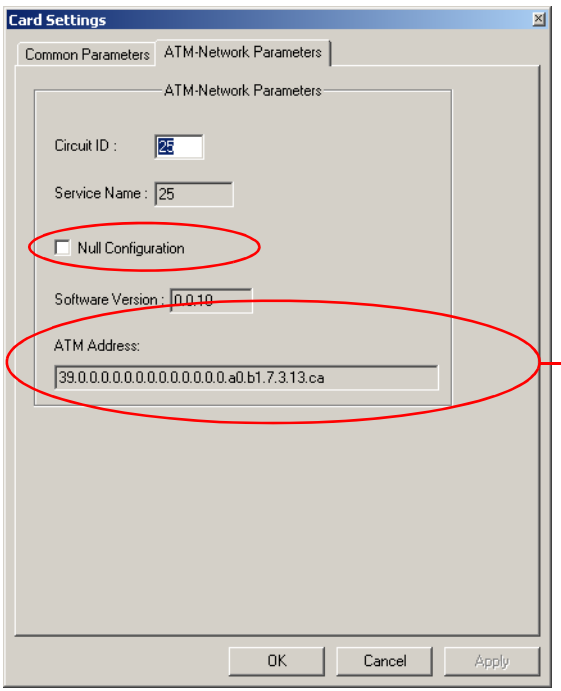
3. In the *Cards* list, right-click the slot containing the ATM network interface card, and then click **Properties**.



Alternatively, double-click the slot containing the ATM network interface card.

The *Card Settings - Common Parameters* dialog box opens.

4. Click the **ATM Network Parameters** tab.
The *ATM Network Parameters* dialog box opens, displaying the settings that are specific to the ATM module.



UNI Address of the ATM card installed in the MCU. It is required to complete the ATM service definition.

The first time you access the *ATM Network Parameters* dialog box, the *Null Configuration* option is checked and the *ATM Address* box, which indicates the UNI Address of the ATM card, is blank.

5. Clear the **Null Configuration** check box to activate the card settings. The *Circuit ID* box is enabled and the ATM card's UNI address is displayed in the *ATM Address* box. Write down this number, as you will need it to define the MCU in the V-Gate application.
6. Assign the ATM's circuit ID as defined in the *ATM Network Services–Spans and Phones* dialog box to the ATM module.
   The Network Service Name is automatically assigned to the Service Name.
7. Click the **Apply** button.
   The name of the network service appears in the *Service Name* box.
8. Click **OK**.

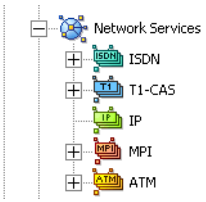
Modifying a Network Service

After you finish defining a new Network Service, you may review or edit the Network Service's parameters.

To review or edit a Network Service's parameters:

1. In the *Browser* pane, connect to the MCU and expand its options tree.
2. Double-click the *MCU Configuration* icon, to list the configuration options.
3. Double-click the *Network Services* icon, or click the plus [+] icon next to the *Network Services* icon to expand the list.

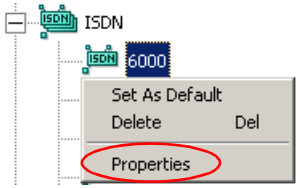
   A list of Network Service types is displayed below the *Network Services* icon.



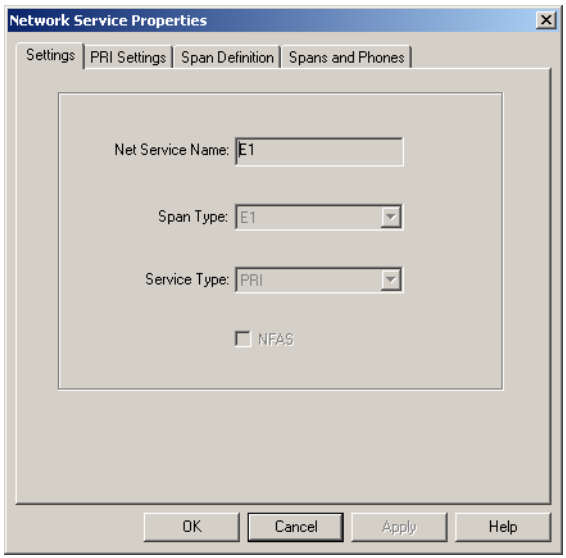
4. Double-click the appropriate *Network Service* icon, or click plus [+] icon next to the appropriate *Network Service* icon to expand the list of network service of the selected type.

   A list of the Network Services of the selected type defined for the MCU appears below the *Network Services* icon.

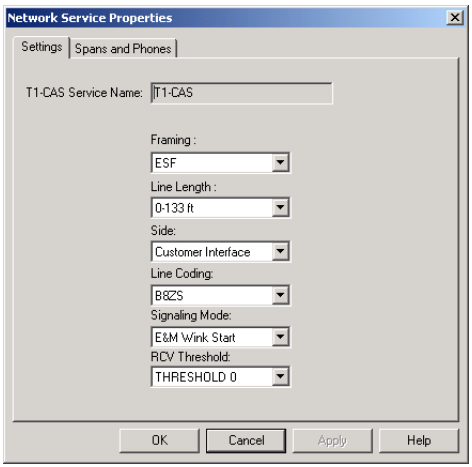
5. Right-click the icon of the Network Service to review or edit, and then click **Properties**.
   Alternatively, double-click the *Network Service* icon to display its properties.



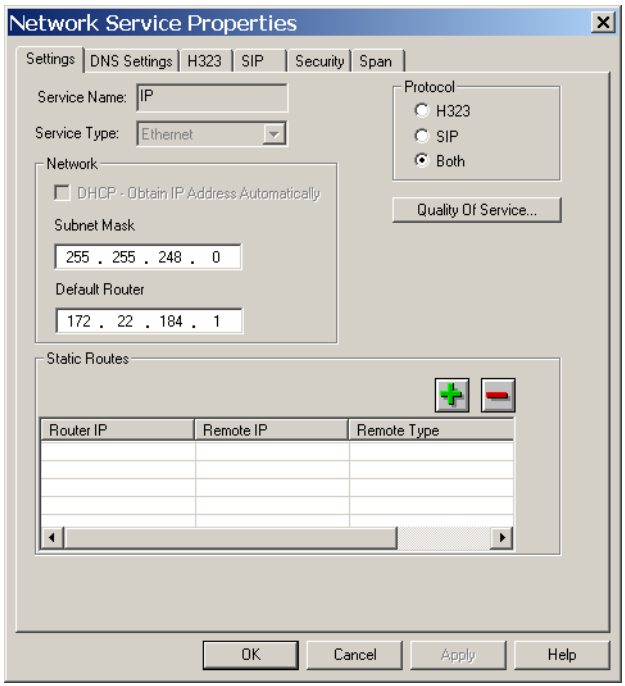
— If you are modifying an ISDN network service, the *Network Service Properties–Settings* dialog box opens. The tabs of this dialog box correspond exactly to the dialog boxes that were displayed by the wizard during the definition of a new ISDN Network Service. For details, see "Defining an ISDN Network Service" on page 3-3.



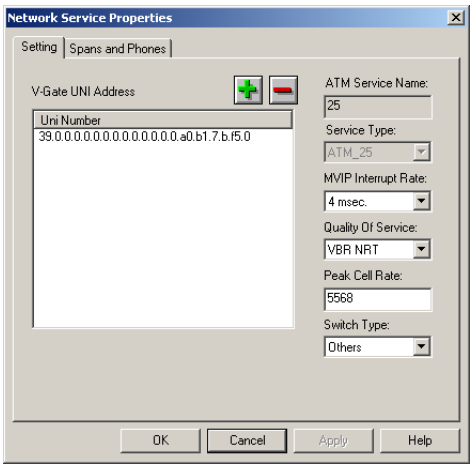
— If you are modifying a T1-CAS Network Service, the *Network Service Properties–Settings* dialog box opens. The Network Service parameters are identical to those displayed by the wizard during the definition of a new T1-CAS Network Service. For details, see “Defining a new T1-CAS Network Service” on page 3-40.



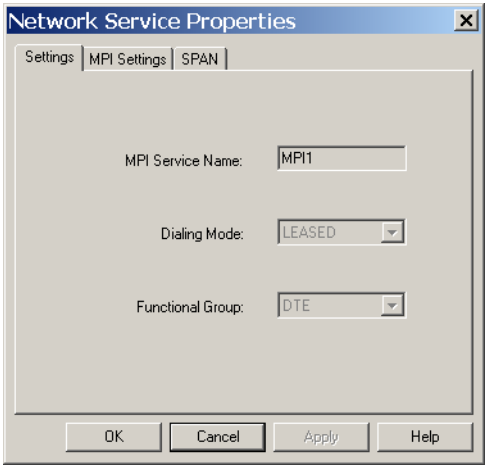
— If you are modifying an IP Network Service, the *Network Services Properties–Settings* dialog box opens.The Network Service parameters are identical to those displayed by the wizard during the definition of a new IP service. See "Defining an IP Network Service" on page 3-54.



— If you are modifying an ATM Network Service, the *Network Services Properties–Settings* dialog box opens. The Network Service parameters are identical to those displayed by the wizard during the definition of a new ATM Network Service. For details, see “Defining an MPI Network Service” on page 3-99.



— If you are modifying an MPI Network Service, the *Network Services Properties–Settings* dialog box opens. The Network Service parameters are identical to those displayed by the wizard during the definition of a new MPI service. See “Defining an MPI Network Service” on page 3-99.



6. Click the relevant tab containing the parameters that you wish to view and if necessary modify the settings in the various tabs.
7. Click **OK** to save your changes, or click **Cancel** to discard your changes. The *Network Service Properties* dialog box closes.

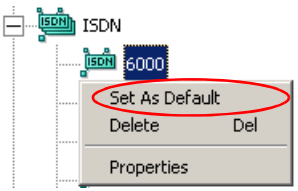
Setting the Default Network Service

Whenever a new conference is configured, the default network service is assigned to the conference unless you explicitly assign a different one. This section describes how to set the default network service for an MCU.

For instructions on setting the default IP network service see “Setting the Default IP Network Service” on page 3-97.

To make a Network Service the default:

1. In the *Browser* pane, connect to the MCU and expand its tree.
2. Double-click the *MCU Configuration* icon.
3. Double-click the *Network Services* icon to expand the list of network services types.
4. Double-click the *ISDN/T1-CAS/ATM/MPI Network Service* icon to expand the list of network services.
5. Right-click the icon of the Network Service to be set as the default, and then click **Set As Default**.



The name of the network service appears in bold to indicate that it is the default Network Service for that type.

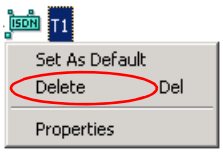
You may define a default Network Service for each Network Service type (ISDN, T1-CAS, ATM, or MPI).

Deleting a Network Service

You may remove a Network Service from the MGC Manager.

To delete a Network Service:

1. In the *Browser* pane, connect to the MCU and expand its tree.
2. Double-click the *MCU Configuration* icon. to display the configuration options.
3. Double-click the *Network Service* icon to display the Network Services types list.
4. Double-click the appropriate *Network Service* icon, or click plus [+] icon next to the appropriate *Network Service* icon to expand the list of network service of the selected type.
5. Right-click the icon of the network service to delete, and then click **Delete**.



A confirmation dialog box opens.

6. Click **Yes** to delete the Network Service or **No** to cancel the operation. The Network Service is removed from the Network Services list shown under the *Network Service* type.

4

MCU Card Management

This chapter describes how to manage the MGC modules. In particular, the following tasks are described:

- Listing the installed functional modules (cards)
- Viewing the functional module (card) parameters
- Configuring the MUX (card) module
- Listing the card's units and their options
- Removing a card from the MCU
- Resetting a card

The MCU must be connected in order to perform the above tasks. For details, see the *MGC Manager User's Guide, Volume I, Chapter 3, "Connecting to an MCU"*.

Only users (MGC Manager operators) with Superuser rights can perform MGC Manager configuration tasks. In addition the user must have Superuser rights on the computer on which the MGC Manager application is running, or any other permission than enables the application to access the Registry (read/write) and read/write files on the C: drive (root directory) and under the Windows directory folder.

Managing the Functional Module Cards (MGC-50/MGC-100/MGC+50/MGC+100)

A description of the MGC-25 cards can be found in the *MGC-25 Getting Started Guide*.

The MGC-100/MGC+100 can contain up to 16 functional module cards, which can occupy slots 1 through 16. The MGC-50/MGC+50 can contain up to 8 functional module cards, which can occupy slots 1 through 8. It is based on the “universal slot” concept, where different modules may be installed depending on the users’ port capacity and functionality requirements forming user specific configurations. The Functional Modules perform the various audio, video, and data processing functions for the MGC unit.

An additional slot (Slot A) is used by the Main Control Module.

Any module may be inserted into any slot. All functional modules are hot-swappable.

Each module is automatically identified by the system, as well as the versions of the programs embedded in it. These parameters may be viewed in the card *Properties–Card Settings* dialog box. When a card is installed in the MCU, its hardware and software versions are read by the system. The MCU's Control Unit checks these versions, and if they do not match the expected versions, the Control Unit downloads the appropriate software versions stored in its memory. Table 4-1lists the available functional modules.

The MGC+ hardware can include the Net-2/4/8, IP+24/48/96, MPI, MUX+, Audio+, Video+ and T.120 cards.

Table 4-1: Functional Modules

Functional Module	Function	Port capacity
Net-T1/Net-E1 ISDN Network Interface	Interfaces between the MGC unit and the ISDN network.	46/60 ISDN channels
Net-2 ISDN/T1-CAS Network Interface	Interfaces between the MGC unit and the ISDN network.	46/60ISDN channels or 48 T1-CAS Channels

Table 4-1: Functional Modules (Continued)

Functional Module	Function	Port capacity
Net-4 ISDN/T1-CAS Network Interface	Interfaces between the MGC unit and the ISDN network.	92 channels/120 ISDN channels or 96 T1-CAS Channels
Net-8 ISDN/T1-CAS Network Interface and Net-8L ISDN Network Interface	Interfaces between the MGC unit and the ISDN network.	184 /240 ISDN channels or 192 T1-CAS Channels
ATM-25 Network Interface	Interfaces between the MGC unit and the ATM network.	10 ports
ATM-155 Network Interface	Interfaces between the MGC unit and the ATM network.	20 ports
MG323/IP12	Audio, video and data communications across IP based (LAN) networks, including the Internet.	12 channels at 128, 256 and 384Kbps 6 channels at 768Kbps 3 participants at T1/E1
IP24	Audio, video and data communications across IP based (LAN) networks, including the Internet.	48 channels at 128Kbps 24 channels at 384Kbps 12 channels at 768Kbps 6 participants at T1/E1
IP48	Audio, video and data communications across IP based (LAN) networks, including the Internet.	48 channels at 128Kbps 48 channels at 384Kbps 24 channels at 768Kbps 12 channels at T1/E1
IP+12	Performs signaling and capabilities exchange for conferencing. Encrypted conferences with IP participants, SIP sessions and mixed component conferences that include SIP participants require IP+ cards	32 channels at 128Kbps

Table 4-1: Functional Modules (Continued)

Functional Module	Function	Port capacity
IP+24	Performs signaling and capabilities exchange for conferencing. Encrypted conferences with IP participants, SIP sessions and mixed component conferences that include SIP participants require IP+ cards	48 channels at 128Kbps
IP+48	Performs signaling and capabilities exchange for conferencing. Encrypted conferences with IP participants, SIP sessions and mixed component conferences that include SIP participants require IP+ cards	96 channels at 128Kbps
MPI-4	Uses dialing protocols to communicate to endpoints using “Data Terminal Equipment” (DTE), or Data Communications Equipment (DCE).	120 channels/92 channels
MPI-8	Uses dialing protocols to communicate to endpoints using “Data Terminal Equipment” (DTE), or Data Communications Equipment (DCE).	240 channels/184 channels
Audio (Standard)	Performs audio compression, decompression, and bridging.	12 ports per card (standard conference) Audio Bridge: 16 participants, or 30 participants (Large Video Switching conference)

Table 4-1: Functional Modules (Continued)

Functional Module	Function	Port capacity
Audio+	Performs audio compression, decompression. Number of ports changes according to the Audio Algorithm used in the conference.	Audio+8A - 24/48 ports Audio+8V - 24 ports Audio+12/24 - 12/24* ports Audio+24/48 - 24/48* ports Audio+48/96 - 48/96* ports * video/audio conferences
Video	Performs video processing and Transcoding.	Single – 6 ports Double – 12 ports
Video+	Performs video processing and Transcoding.	Video+8 - support of up to 8 participants
MUX Module	Multiplexes and demultiplexes audio, data, video, and control information; performs channel aggregation (inverse multiplexing).	Up to 16 ports
MUX+10	Multiplexes and demultiplexes audio, data, video, and control information; performs channel aggregation, enables Encryption.	18 channels at 128Kbps
MUX+20	Multiplexes and demultiplexes audio, data, video, and control information; performs channel aggregation, enables Encryption.	128 36 channels at 128Kbps

Table 4-1: Functional Modules (Continued)

Functional Module	Function	Port capacity
MUX+40	Multiplexes and demultiplexes audio, data, video, and control information; performs channel aggregation, enables Encryption.	72 channels at 128Kbps
Data Module	Performs data routing and conference control.	T.120 standard card - 12 ports T.120-24 card - 24 ports

The different types of functional modules are used to produce a variety of configurations. In the MGC-50 up to eight individual Functional Modules can be used to build the desired configuration. In the MGC-100, 16 modules can be used.

The configuration of each functional module can be checked and for specific modules, and if required, modified. Any operator can view the Functional Module configuration settings. Only an operator defined as Superuser can modify the configuration settings of a functional module.

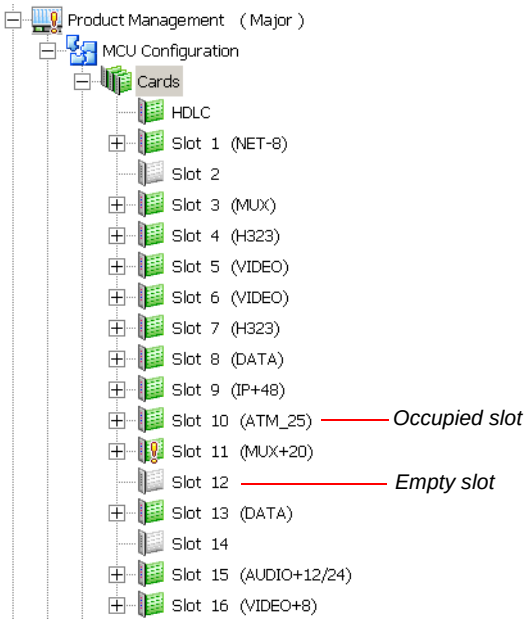
Listing the Installed Modules

You can check which functional modules are installed in a particular MCU by listing them.

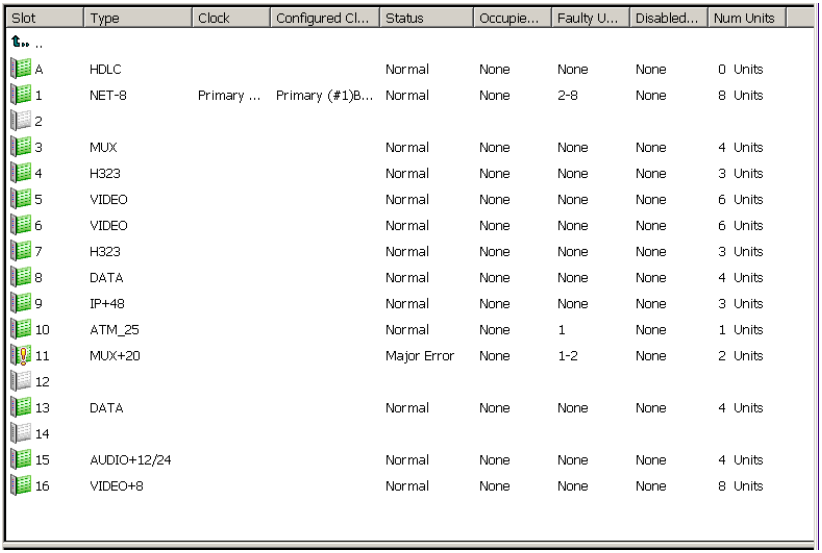
To list an MCU's functional modules:

1. Connect to the MCU whose modules you want to list.
2. Expand the *MCU* tree to list its options.
3. Expand the *MCU Configuration* tree to list the configuration options.
4. Expand the *Cards* tree.

   All the MCU slots are listed (16 slots for the MGC-100, 8 slots for the MGC-50). Empty slots are indicated by a white card icon. Occupied slots are indicated by a green card icon. The name of the functional module occupying the slot appears next to the slot number.



When double-clicking the *Cards* icon in the *Browser* pane, the *Status* pane displays the status of each card.



Slot	Type	Clock	Configured Cl...	Status	Occupie...	Faulty U...	Disabled...	Num Units
..								
A	HDLC			Normal	None	None	None	0 Units
1	NET-8	Primary ...	Primary (#1)B...	Normal	None	2-8	None	8 Units
2								
3	MUX			Normal	None	None	None	4 Units
4	H323			Normal	None	None	None	3 Units
5	VIDEO			Normal	None	None	None	6 Units
6	VIDEO			Normal	None	None	None	6 Units
7	H323			Normal	None	None	None	3 Units
8	DATA			Normal	None	None	None	4 Units
9	IP+48			Normal	None	None	None	3 Units
10	ATM_25			Normal	None	1	None	1 Units
11	MUX+20			Major Error	None	1-2	None	2 Units
12								
13	DATA			Normal	None	None	None	4 Units
14								
15	AUDIO+12/24			Normal	None	None	None	4 Units
16	VIDEO+8			Normal	None	None	None	8 Units

Occupied slots appear in green while empty slots appear in white. The slot number appears next to the slot icon. Table 4-2 describes the *Status* pane columns.

Table 4-2: MCU's Cards Status Columns

Field	Description
Slot	Displays the slot icon and number; a white icon indicates an empty slot and a green icon indicates an occupied slot.

Table 4-2: MCU's Cards Status Columns (Continued)

Field	Description
Type	Displays the type of card that occupies the slot. The following card types are available, as listed in Table 4-1: • Network (Net-T1/Net-E1, Net-2, Net-4, Net-8, ATM-25 or ATM-155, H.323, IP24, IP48,IP+12, IP+24, IP+48, MPI-8) • MUX or MUX+ • Data • Audio or Audio+ • Video or Video+
Clock	This column is valid only for ISDN and Serial (MPI-8) Network Interface cards. One Net-T1/Net-E1 Module in each MCU serves as the "master clock," which synchronizes the system clock to the network clock. A second Net-T1/Net-E1 Module provides a backup clock, which is used if the master clock fails. The primary and backup clocks can only be set in span A of the Net-T1/Net-E1network cards. On the Net-2/Net-4/Net-8 Network Interface Module, the Master and the Backup clocks can be set on any of the spans connected to the module. This column indicates which Network card/span is used as the Master Clock and which one is used as the Backup clock.
Configured Clock	Indicates which ISDN Network card or MPI Span was configured as the Primary network interface (for clocking), and which one is used as backup. Changes take effect and are updated during the next MCU reset or power up.
Status	Indicates the card status.
Occupied Units	Indicates the units on the card that are currently used to run conferences. For example, 1, 6 indicates that two units, unit # 1 and unit # 6 are used to run conferences.

Table 4-2: MCU's Cards Status Columns (Continued)

Field	Description
Faulty Units	Indicates if there are units on the card which are faulty and the sequential number of the faulty unit.
Disabled Units	Indicates the units that were disabled by the operator.
Num Units	Indicates the total number of units available for each module.

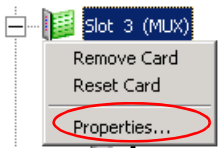
When the MCU is updated with a new software version, the current card configuration definitions are automatically copied to the new configuration files and are loaded to the card during the software download process.

Viewing the Common Card Parameters

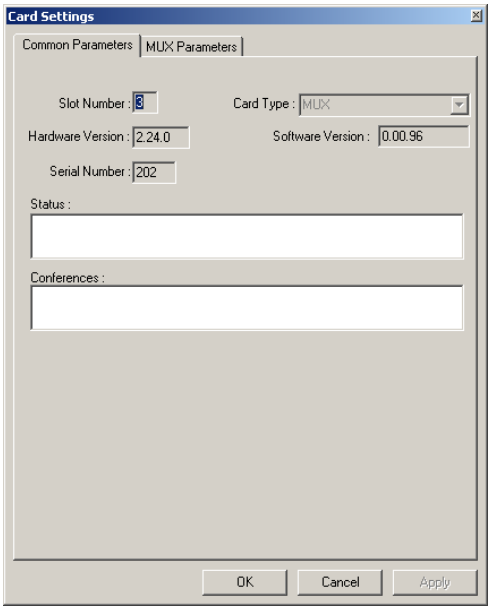
You may want to view the cards parameters, disable one or more of the card's units, or modify the cards configuration.

To view any card parameters:

- Right-click the slot containing the card to check or configure, and then click **Properties**.



The *Card Settings – Common Parameters* dialog box opens.



This dialog box appears in the properties of all functional modules. It contains parameters common to all the cards.

The system indicates the slot in which the card is inserted, the card's type, hardware version, software version and serial number as identified by the MCU's software.

The *Status* box displays all the error messages related to the card. When there is a problem with the card, a detailed description of the problem appears in this box.

The *Conferences* box displays the name of the conferences which are currently run by this card.

The *Card Type* box specifies the card type.

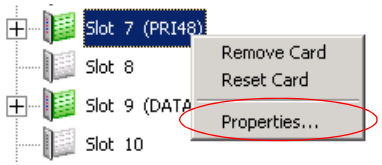
The configuration of the Network Services include the assignment of the card to a network service, as described i*n Chapter 3, "Defining Network Services" on page 3-1*.

Viewing the NET-T1/NET-E1 Card Properties

To connect the MCU to the ISDN network switch, you need to assign the ISDN Network Service to the appropriate span of the Net-T1/Net-E1Network Interface module. For details, see Chapter 3, “Assigning the ISDN Network Service to the NET-T1/NET-E1 Card” on page 3-29.

To view the Net-T1/Net-E1 ISDN card properties:

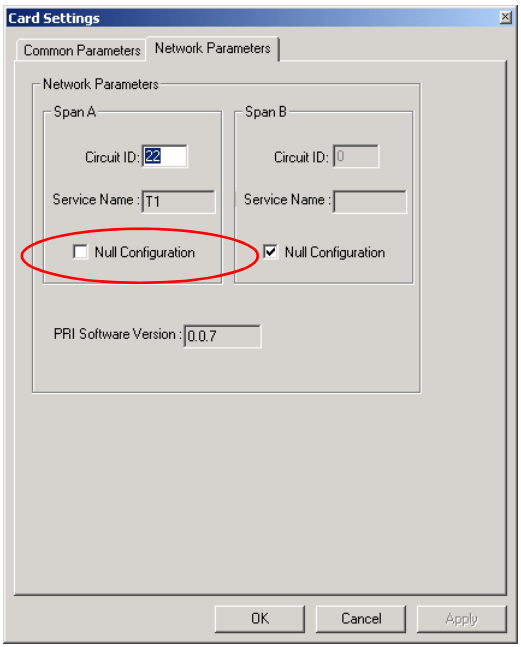
1. In the *Browser* pane, right-click the slot containing the Net-E1/T1 card, indicated by PRI48 and PRI64, and then click **Properties**. Alternatively, double-click the slot containing the card.



   The *Card Settings–Common Parameters* dialog box opens. For details, see *“Viewing the Common Card Parameters” on page 4-10*.

2. To view the status of the connection to Net-E1/T1 card, click the **Network Parameters** tab.

The *Card Settings–Network Parameters* dialog box opens, displaying the settings that are specific to the Net-T1/Net-E1 Network Interface module.



The following information is displayed:

Table 4-3: Card Settings-Network Parameters Options

Field	Description
Circuit ID	Displays the circuit ID assigned to an ISDN Network Service. For further information, *see Chapter 3, "Assigning the ISDN Network Service to the NET-T1/ NET-E1 Card" on page 3-29.*
Service Name	The name of the Network Service.
Null Configuration	When the *Null Configuration* option is checked, the circuit ID is set to 0.
PRI Software Version	Displays the version of the PRI software.

Viewing the Net-2/Net-4/Net-8 Card Properties

To connect the MCU to the ISDN network switch, you need to assign the ISDN Network Service to the appropriate span of the Net-2/Net-4/Net-8 Network Interface module. For details, *see Chapter 3, "Assigning the ISDN Network Service to the Net-2/Net-4/Net-8 Card" on page 3-34.*

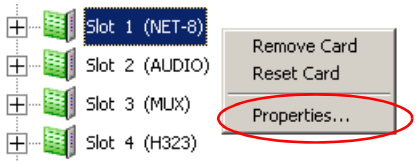
In the same way, to connect the MCU to T1-CAS lines, you need to assign the T1-CAS Network Service to the appropriate span of the Net-2/Net-4/Net-8 Network Interface module. For details, *see Chapter 3, "Assigning the T1-CAS Network Service to the Net-2/Net-4/Net-8 Card" on page 3-46.*

It is not possible to mix an ISDN Network Service and a T1-CAS Network Service on the same Net-2/Net-4/Net-8 Network Interface module. Therefore, the Net-2/Net-4/Net-8 card can only be used with either ISDN or T1-CAS Network Service. Before you assign the T1-CAS Network Service to the card, you must set the following 'system.cfg' flag: in the NET8_PARAMETERS section, set NET8_DEFAULT_TYPE = to T1-CAS.

In addition, you may define which span in the network interface card will be used as the primary clock and which one as the backup clock to synchronize with the network clock. For details, *see Chapter 5, "Clocking" on page 5-139.*

To view the Net-2/Net-4/Net-8 ISDN card properties:

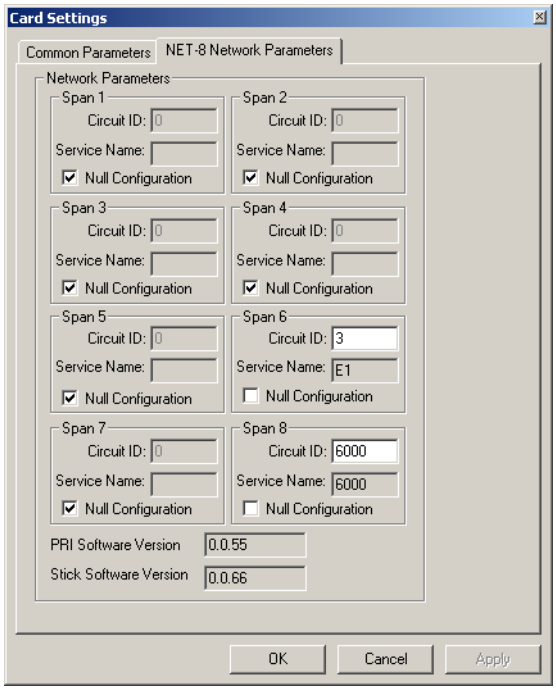
1. In the *Browser* pane, right-click the slot containing the Net-2/4/8 card, and then click **Properties**.
   Alternatively, double-click the slot containing the card.



   The *Card Settings – Common Parameters* dialog box opens. For details, see *"Viewing the Common Card Parameters" on page 4-10*.

2. To view the status of the connection to Net-2/Net-4/Net-8 card, click the **NET–8 Network Parameters** tab.

The *Card Settings NET-8 Network Parameters* dialog box opens, displaying the settings that are specific to the Net-2/Net-4/Net-8 Network Interface module.



The following information is displayed:

Table 4-4: Card Settings-Net-8 Network Parameters Options

Field	Description
Circuit ID	Displays the circuit ID assigned to an ISDN/T1-CAS Network Service. For further information see *Chapter 3, "Assigning the ISDN Network Service to the Net-2/Net-4/Net-8 Card" on page 3-34* and *Chapter 3, "Assigning the T1-CAS Network Service to the Net-2/Net-4/Net-8 Card" on page 3-46*.
Service Name	The name of the Network Service.
Null Configuration	When the *Null Configuration* option is checked, the circuit *ID* is set to 0.

Table 4-4: Card Settings-Net-8 Network Parameters Options (Continued)

Field	Description
PRI Software Version	Displays the version of the PRI software.
Stick Software Version	Displays the version of the Stick software.

Viewing the IP/IP+ Card Properties

The IP/IP+ card properties enable you to view additional information about the IP network, the Network Service assigned to this card, the card details, such as, the card type, hardware version, the MCU slot number, the card status, and the conferences that are handled by the card. The IP card units interface between the IP network and the MCU. There are several types of IP cards: standard IP (MG323) and IP+ cards.

The IP cards can be of one of the following combinations:

- Hardware version 1.24/1.41 with 8 MB memory and 12 port capacity
- Hardware version 2.21 with 16 MB memory and 24 port capacity

The IP+ cards are available in three port sub-assemblies: IP+12/IP+24/IP+48, and are associated with version 4.23 and higher.

For conferences that include SIP defined participants, IP+ cards from version 4.23 or higher are required. For H.323-only conferences, IP (12 or 24) cards are sufficient.

The following table lists the main characteristics of the various IP card types.

Table 4-5: IP Card Types

IP Card Name	HW Version	SIP Support	Number of Units	VOIP Call Capacity	Encryption
MG323	1.24/1.41	–	3	12	No
IP24	2.21	–	3	24	No
IP48	4.23> 4.41	+	3	96	✓

Table 4-5: IP Card Types (Continued)

IP Card Name	HW Version	SIP Support	Number of Units	VOIP Call Capacity	Encryption
IP+12	> 4.41	+	1	32	✓
IP+24	> 4.41	+	2	64	✓
IP+48	> 4.41	+	3	96	✓

To view the IP card properties:

1. Expand the MCU tree.
2. Expand the MCU Configuration tree
3. Expand the Cards tree.
4. Right-click the IP card icon and click Properties, or double-click the card.

   The IP card properties are described in six tabs:

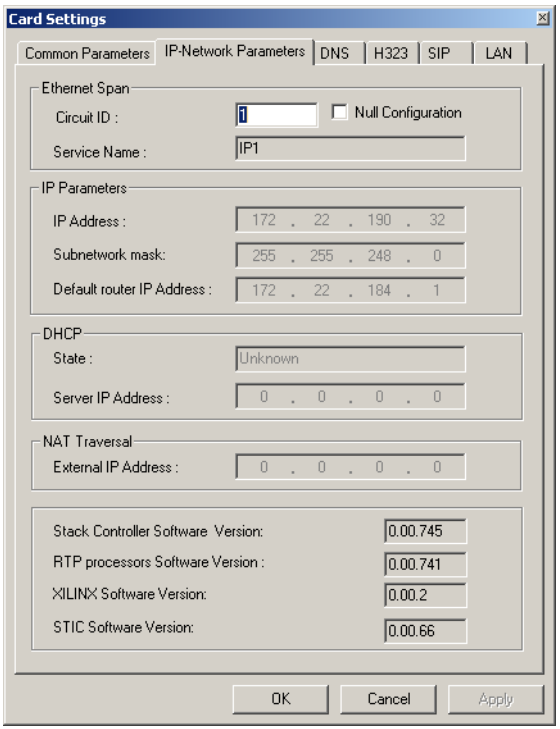
   — Common Parameters
   — IP-Network Parameters
   — DNS
   — H.323
   — SIP
   — LAN

Common Parameters

The *Common Parameters* tab is for viewing purposes only and displays the following information: slot number, card type, hardware version number, software version number, serial number, card status, and conferences that are currently running on this card. The card's common parameters are detailed in *"Viewing the Common Card Parameters" on page 4-10*.

IP-Network Parameters

The *Card Settings-IP-Network Parameters* tab is used for assigning a Network Service to the IP card.



In addition, the *IP-Network Parameters* tab displays the following information:

Table 4-6: IP Card Settings-IP-Network Parameters

Field	Description
Ethernet Span	
Circuit ID	The Circuit ID defined for this card in the IP network Service assigned to this card
Service Name	The name of the IP Network Service assigned to this card.

Table 4-6: IP Card Settings-IP-Network Parameters (Continued)

Field	Description
IP Parameters	
IP Address	The card's IP address. If a DHCP server is used for dynamic address allocation, this field displays the IP address allocated to the card by the DHCP.
Subnetwork mask	The subnetwork mask the card is part of.
Default router IP Address	The default router for this subnetwork.
DHCP	
State	The DHCP IP address assignment can be in one of the following states: • Unknown [None] – DHCP is not used. • Selecting – The card is in the process of locating the DHCP. • Requesting – The card has located the DHCP and has requested an IP address. • Binding – The card is validating whether the assigned IP address is suitable. If not, it reissues a request. • Bound – The normal state, the card has a working IP address. • Renew – The IP address has expired and the card has issued a renewal request. • Rebind – The renewal request is not acknowledged [the DHCP server may be down], the card continues using the expired IP address. If the card was assigned a new IP address an error message appears stating that the IP has changed and that the card needs to be reset.
Server IP Address	The IP address of the server hosting the DHCP service.
NAT Traversal	
External IP Address	The external IP address of the card, that will be used to replace the internal IP address of this card using NAT mapping.

Table 4-6: IP Card Settings-IP-Network Parameters (Continued)

Field	Description
Software Versions	
Stack Controller; *RTP processors;* *XILINX;* *STIC*	The associated software versions embedded on the various card processors.

DNS

The *Card Settings-DNS* tab displays information derived from the *IP Network Service-DNS* dialog box.

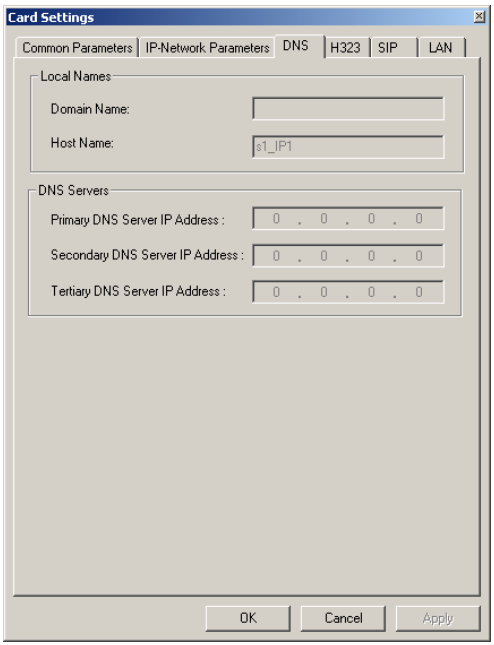


Table 4-7: IP Card Settings-DNS

Field	Description
Domain Name	Not currently used.

Table 4-7: IP Card Settings-DNS (Continued)

Field	Description
Local Domain Name	The name of the domain the IP card is part of.
Span Host Name	The host name of the IP card, as defined in the IP Network Service or retrieved from the DHCP.
Primary DNS Server IP Address	The IP address of the primary DNS server, as defined in the IP Network Service or retrieved from the DHCP.
Secondary/Tertiary DNS Server IP Address	The IP addresses of the fallback DNS servers that resolve names into IP addresses in case of primary DNS server failure. The IP address is either defined in the IP Network Service or retrieved from the DHCP.

H.323

The *Card Settings-H.323* tab displays information derived from the *IP Network Service-H.323* dialog box.

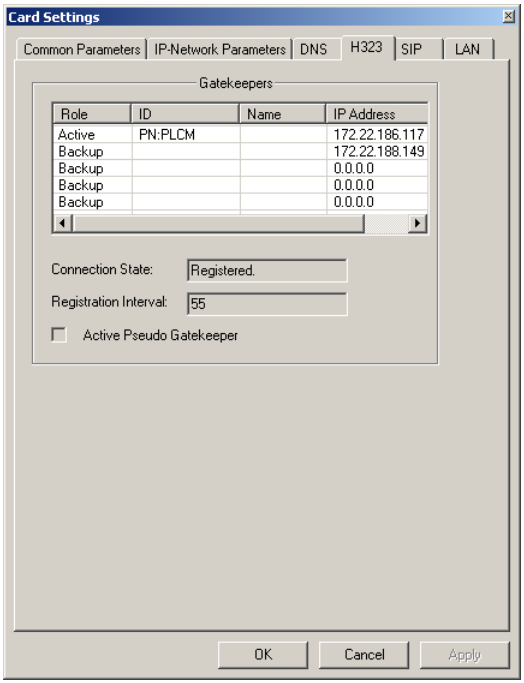


Table 4-8: IP Card Settings-H.323

Field	Description
Role	**Active**: The active gatekeeper. **Backup**: The backup gatekeeper that can be used in case the connection to the preferred gatekeeper fails. Up to three backup gatekeepers can be defined.
ID	A gatekeeper ID retrieved from the gatekeeper during the registration process.
Name	The gatekeeper's host name.
IP Address	The gatekeeper's IP address.
Connection State	The state of the connection between the H.323 card and the Gatekeeper. The following statuses may be displayed: ***Discovery*** – The card is looking for the gatekeeper. ***Registration*** – Indicates that the card is in the process of registering in the gatekeeper. ***Registered*** – Indicates that the H.323 card is registered in the Gatekeeper. **Not registered** – Indicates that there is no gatekeeper defined in the system. ('Off').
Registration Interval	Indicates the interval in seconds between the card's registration messages to the gatekeeper. This value is taken from either the IP Network Service or from the Gatekeeper during the registration choosing the smaller value of the two.
Active Pseudo Gatekeeper	When working in the Pseudo Gatekeeper mode, indicates whether this card acts as the Master (the card that answers LRPs).

SIP

The *Card Settings-SIP* tab displays information derived from the *IP Network Service-SIP* dialog box, from the DHCP or the DNS server.

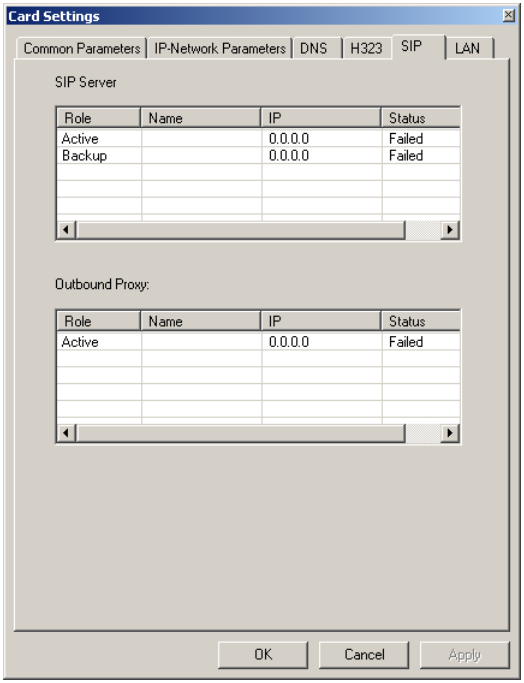


Table 4-9: IP Card Settings-SIP

Field	Description
SIP Server	
Role	*Active*—The default SIP Server used for SIP traffic. *Backup*—The SIP Server used for SIP traffic in case the preferred proxy fails.
Name	The name of the SIP Server.
IP	The outbound SIP Server's IP address.
Status	The connection state between the SIP Server and the IP card.

Table 4-9: IP Card Settings-SIP (Continued)

Field	Description
Outbound Proxy	
Role	*Active*—The default outbound proxy if different from the SIP Server.
Name	The name of the outbound proxy
IP	The outbound proxy's IP address.
Status	The connection state between the outbound proxy and the IP card.

LAN

The *Card Settings-LAN* tab displays information derived from the network.

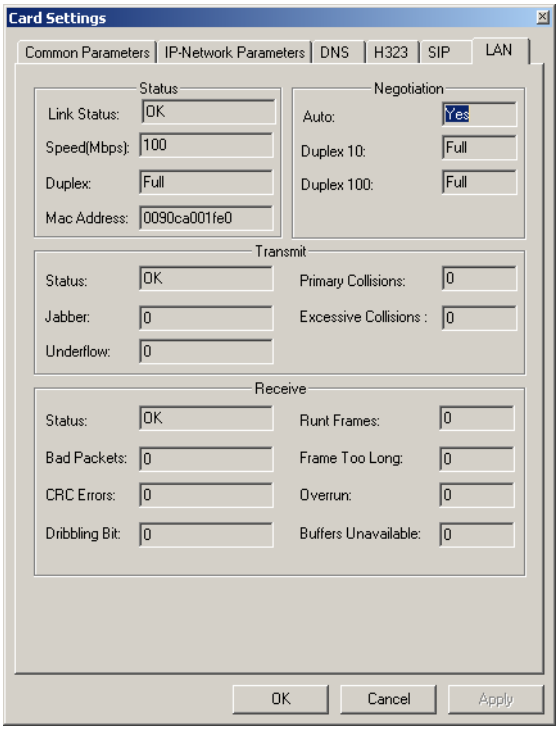


Table 4-10: Card Settings–LAN

Field	Description
Status	
Link Status	The status of the link from card to the hub/switch. Options are *OK* or *Fail*.
Speed(Mbps)	Indicates the transfer rate between the card and the hub/switch. It can be 10 Mbits/Sec or 100 Mbits/Sec.
Duplex	Full duplex means that transmit and receive operations can proceed simultaneously between the card and the hub. If the service is set to Video Bit Rate of 10 bits/sec, the system will always work in half duplex.
Mac Address	Specific hardware address of card. This address is burnt on the card and is automatically identified by the system.
Negotiation	
Auto	Indicates whether the card automatically links to the hub/switch.
Duplex 100/Duplex 10	Indicates the LAN defined speed and duplex. For details regarding Duplex, see the *Status - Duplex* field.
Transmit	
Status	The status of the transmit module.
Jabber	Indicates the number of times that the LAN controller transmit time exceeded the limit.
Underflow	The number of data packets that did not arrive during the expected time period to the LAN controller. If the counter shows a number higher than 0 it means that data packets could be lost. It may indicate an internal problem in the card.
Primary Collisions	The number of times the LAN controller had to re-transmit data packets due to collisions. Collisions occur when data packets bump into each other, causing a disruption in the transmission.
Excessive Collisions	The number of packets lost due to collisions on the LAN.

Table 4-10: Card Settings–LAN (Continued)

Field	Description
Receive	
Status	The status of the receive module.
Bad Packets	The number of other types of bad packets.
CRC Errors	The number of received packets with CRC (Cyclic Redundancy Check) errors.
Dribbling Bit	The number of received packets not consisting of full octets.
Runt Frames	The number of received packets discarded because of internal problems – usually due to interrupted transmission.
Frame Too Long	The number of packets whose length exceeds 1514 bytes (illegal length).
Overrun	The number of packets lost due to unavailable internal LAN controller resources (the LAN controller buffer was full).
Buffers Unavailable	The number of packets that were lost due to the LAN controller inability to forward the data packets, and overcrowding its buffer.

Viewing and Configuring the MUX Module Specific Properties

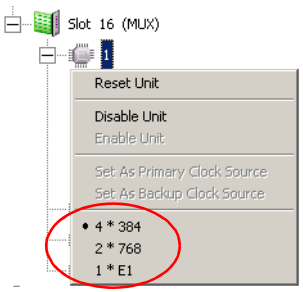
The MUX card is used for connecting ISDN and T1-CAS video participants to the conference.

IP video conferences do not require a MUX or MUX+ card. The H.323 and IP cards have a built in MUX functionality.

Before running conferences, it is important that the MUX units are configured to the appropriate line rate, as this defines the maximum line rate for each participant. The unit configuration determines the total number of participants in all the conferences run simultaneously. For example, a unit set to 4x384, a unit can carry four participants, each at a line rate of up to 384 Kbps. You can set different units to different line rates to accommodate different participant capacities. If the system does not have enough resources to accommodate a certain line rate, it will automatically allocate units of higher line rates to carry the conference. For example, if one unit is configured as 4x384 and all the other units are configured as 2x768, or E1/T1, and there are five participants using line rates of 384 Kbps, the system will automatically allocate one of the units configured as 2x768 to run as the fifth participant in the conference (the first four participants are handled by the unit configured as 4x384). The line rate should be set according to the expected number of conferences at each line rate to be handled by the MCU.

To configure the MUX module:

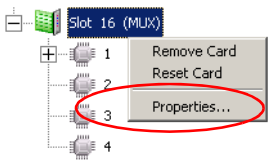
1. In the *Browser* pane, click the plus icon [+] next to the slot containing the MUX module to list its ports (units).
2. Right-click the port to configure.



3. Select the desired line rate:
   - **4x384** – Four participants at line rates of up to 384 Kbps each
   - **2x768** – Two participants at line rates of up to 768 Kbps each
   - **1xE1** – One participant at a line rate of up to 1920 Kbps

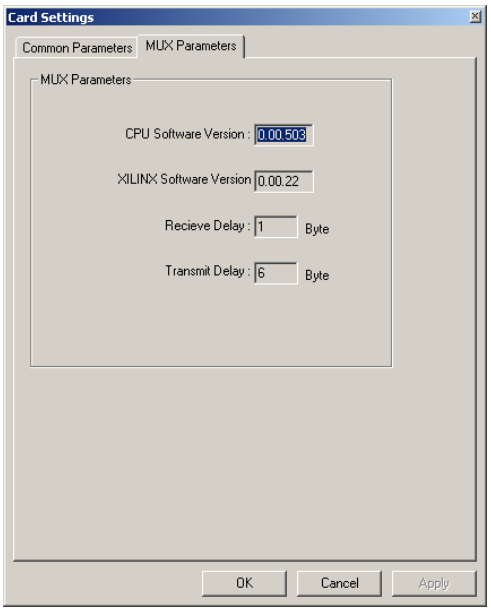
To display the card's configuration

1. Right-click the slot containing the card and then click **Properties**.



The *Card Settings-Common Parameters* dialog box opens. For details, see *"Viewing the Common Card Parameters" on page 4-10*.

2. Click the **MUX Parameters** tab.
   The *MUX Parameters* dialog box displays the MUX specific settings.



The fields in the *Card Settings – MUX Parameters* dialog box are read-only fields that cannot be edited.

3. Click **OK**.

Viewing and Configuring the MUX+ Module Specific Properties

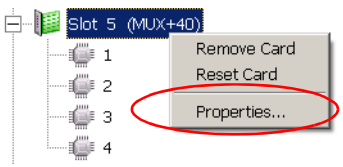
The MUX+ card, like the MUX card, is used for connecting ISDN and T1-CAS video participants to the conference. Encrypted participants require MUX+ resources.

IP video conferences do not require a MUX or MUX+ card. The H.323 and IP cards have a built in MUX functionality.

A flexible port resource allocation mechanism is available with the MUX+ card and allocates ports dynamically thereby decreasing fragmentation. It enables the MCU to allocate and free resources according to the conference requirements without pre-configuring the Line Rate on each card unit.

To display the card's configuration

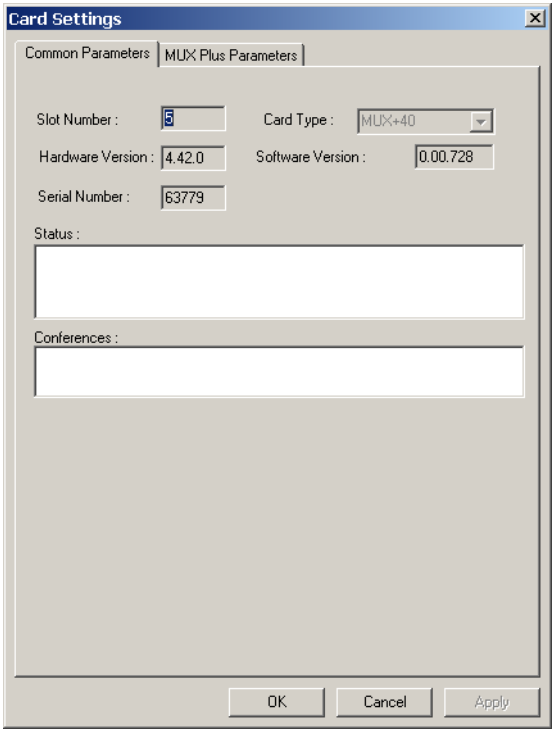
1. Right-click the slot containing the card and then click **Properties**.



The *Card Settings-Common Parameters* dialog box opens. For details, see *"Viewing the Common Card Parameters" on page 4-10*.

This dialog box displays the MUX+ settings such as the slot in which the card is inserted, the card's type, hardware version and serial number as identified by the MCU's software and the card's status.

2. Click the **MUX PLUS Parameters** tab.
   The *MUX Plus Parameters* dialog box displays the MUX+ specific settings.



   The fields in the *Card Settings – MUX Plus Parameters* dialog box are read-only fields that cannot be edited.

3. Click **OK**.

Viewing and Configuring the Audio Module Specific Properties

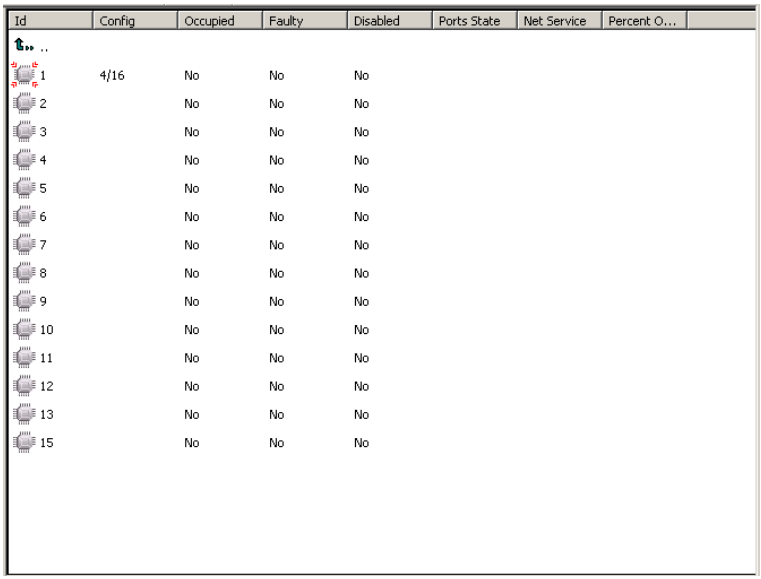
The Audio Functional Modules perform the audio processing functions for the MGC unit. The Audio module properties displays additional information on the status and state of the connection.

To view the audio card units:

To list the Audio module's units in the *Browser* pane, click the plus icon [+] next to the card icon.

To display the module's units in the *Status* pane, click the card icon.

A list of the Audio ports appears below the slot icon and in the *Status* pane.



Id	Config	Occupied	Faulty	Disabled	Ports State	Net Service	Percent O...
..							
1	4/16	No	No	No			
2		No	No	No			
3		No	No	No			
4		No	No	No			
5		No	No	No			
6		No	No	No			
7		No	No	No			
8		No	No	No			
9		No	No	No			
10		No	No	No			
11		No	No	No			
12		No	No	No			
13		No	No	No			
15		No	No	No			

The Audio module contains 13 units. The first unit is the Audio Bridge, which is the controller used for audio mixing of the participants and to identify the conference speaker. The remaining 12 units (2 to 13) are used to connect the audio channels of the participants, one unit per endpoint. Each codec performs audio coding and decoding. Each unit is capable of using any of the following audio algorithms: G.711, G.722, G.728, 722.1 and Siren7.

The audio module may contain two additional units (14 and 15). These units are used for Greet and Guide conferences and have to be configured in the "system cfg." In such a case, port number 14 is used for music, and port

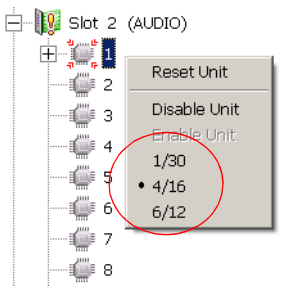
number 15 is used for the audio message deployed in Greet and Guide conferences.

The Audio Bridge can run four conferences simultaneously, totaling up to 16 participants (4/16). To increase the maximum number of participants in a conference to 30 participants set the Audio Bridge to 1/30. When set to 1/30 the Audio Bridge can run only one conference at a time even if the conference includes 16 participants or less and not all the resources are used. The audio card can support up to six gateway sessions with two participants in a session, with a maximum of 12 participants. To enable the gateway sessions set the Audio Bridge to 6/12. When set to 6/12, the audio cards can run only gateway sessions and cannot be used for multipoint conferences. The audio bridge can use units from the same audio card or from different cards.

The default setting of the Audio cards is 4/16. You can change this configuration to suit the type of conferences that are required in your site.

To modify the audio bridge configuration:

In the *Browser* pane, right-click the *Audio Bridge* icon, and then select the appropriate configuration, **1/30**, **4/16**, **6/12**.



The audio card settings are modified accordingly.

The total number of conferences that can be run by an MCU that contains only Audio cards (no Audio+ cards) is determined by the configuration of the audio bridge of each of the audio cards installed in the MCU. For example, if the MCU contains two audio cards and one card's Audio Bridge is set to 1/30 the maximum number of conferences is set to 5.

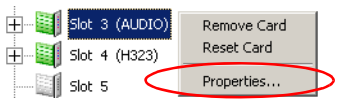
The total number of Audio ports available is determined by the:

- Number of Audio modules x 12

- Maximum number of participants in a conference when the 1/30 option is selected for the Audio Bridge is:
  - — Video Switching: 30 participants
  - — Continuous Presence: 12 video + 18 Audio only participants
- Maximum number of Gateway Sessions when the Audio Bridge is set to 6/12 is the number of Audio cards x 6 sessions.

To display the card's properties:

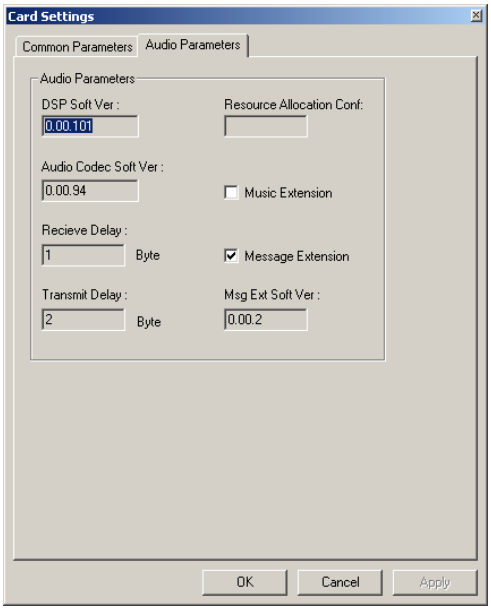
1. In the *Browser* pane, right-click the slot containing the card, and then click **Properties**.



   The *Card Settings – Common Parameters* dialog box opens.
   For details, see *"Viewing the Common Card Parameters" on page 4-10*.

2. Click the **Audio Parameters** tab.

   The *Audio Parameters* dialog box displays settings that are specific to the *Audio* module.



If the Greet and Guide option is added to the MCU, one Audio Module per MCU is used to store the Greet and Guide messages and play background music. To enable the Greet and Guide mode, two additional extensions are installed on the Audio Module: the Audio Message daughter card (Messages Extension) and the Music I/O card (Music Extension).

Only one Music extension and Messages daughter card are installed per MCU.

Once these extensions are installed in the MCU, they are automatically detected by the system at restart. The **Message Extension** and the **Music Extension** check boxes are checked to indicate that these extensions are installed in this Audio module and that they are enabled.

3. Click **OK** to exit the *Card Settings* dialog box.

Viewing the Audio+ Module Specific Properties

The Audio+ Functional Module performs the audio processing functions for the MGC unit. The Audio+ card properties display additional information on the status and state of the connection.

Audio messages are stored directly on the card, and no daughter card is required (as with the standard Audio card).

There are five different types of Audio+ cards (Audio+8A, Audio+8V, Audio+12/24, Audio+24/48 and Audio+48/96) available for Audio and Video conferences. The type of card determines the number of units available and the audio algorithms that are supported. The number of ports for each card type varies, depending on the audio algorithm used.

To view Audio+ card units:

To list the Audio+ module's units in the *Browser* pane, click the plus icon [+] next to the card icon.

To display the module's units in the *Status* pane, click the card icon.

A list of the Audio+ ports appears below the slot icon and in the *Status* pane.

Id	Config	Occupied	Faulty	Disabled	Ports State	Net Serv...	Percent ...
..							
1		No	No	No			
2		Yes	No	No			50%
3		Yes	No	No			75%
4		Yes	No	No			75%
5		Yes	No	No			75%
6		Yes	No	No			75%
7		Yes	No	No			75%
8		Yes	No	No			50%
9		Yes	No	No			50%
10		Yes	No	No			50%
11		Yes	No	No			50%
12		Yes	No	No			50%
13		Yes	No	No			50%
14		Yes	No	No			50%
15		Yes	No	No			50%

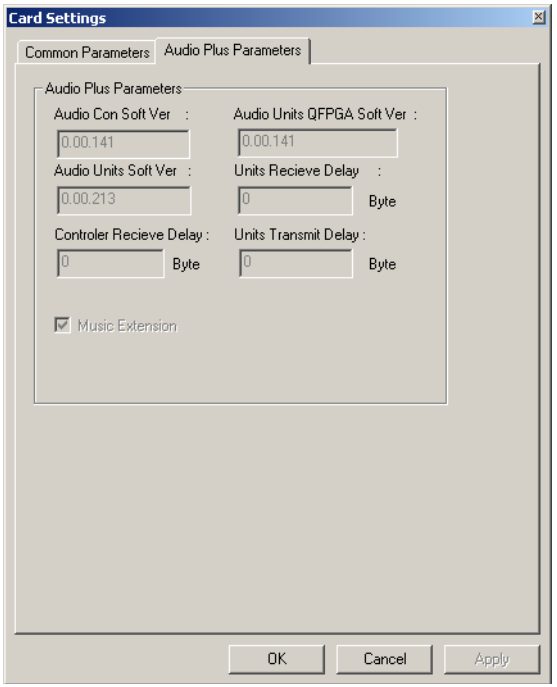
One unit may be connected to 3 or 6 participants depending on the card type and the audio algorithm used by the endpoint. Unit 14 represents the messages storage and unit 15 represents the connection to an external device.

To display the card properties:

1. In the *Browser* pane, right-click the slot containing the card and choose **Properties**.

The *Card Settings – Common Parameters* dialog box opens. For details, see *"Viewing the Common Card Parameters" on page 4-10*.

2. Click the **Audio Plus Parameters** tab to display the settings that are specific to the *Audio+* module.



If the Greet and Guide option is enabled in the MCU, the standard Audio Module must be used to store the Greet and Guide messages and play background music. The Audio Module is used to store the IVR message.

When installed in the VoicePlus unit, this card stores the audio messages used in the IVR Message Services. The number of messages that can be stored on the card is defined in the "system.cfg".

A music I/O card may be installed for the MCU with one module per MCU. This music extension is automatically detected by the system, and the appropriate indication is shown in this dialog box (the *Music Extension* check box is checked). The Music Extension is used to play background music when participants are placed on hold during an Audio only conference.

3. Click **OK** to exit the *Card Settings* dialog box.

Viewing the Video Module Specific Properties

The video channels of the conference can be run by a standalone module, which contains six units, or dual-video module, which is comprised of two cards and contains 12 units in total. The video resources allocated to a conference cannot be split between modules (the dual-video module is considered as one module). All the participants in one video conference must be managed using the same standalone or dual-video card.

When a Video+ card is installed on the MCU, in the *Conference Properties–Resource Force* dialog box, the default *Video* settings are set to **auto**. When set to **auto** the system first uses or allocates the resources on the Video+ card. To have the system assign or use first the Standard Video module for this conference, in the *Conference Properties - Resource Force* dialog box, select **Standard** from the *Video Card Type* drop-down list. If more than one Standard Video module is installed, you can select the specific module to use for this conference by selecting the card's slot in the *Slot* drop-down list in the *Conference Properties - Resource Force* dialog box.

If a dual-video module is used, one card is considered as the master and the other slave. The definition of Master and Slave is automatically defined by the system according to the slot in which the video cards are placed.

The maximum transmission capability of E1 lines (up to 1920 Kbps) can be used in Transcoding or Continuous Presence conferences. To enable the high line rate transmission, a newer video card version (version 1.43 and up) must be installed. In addition, the high bit rate support must be enabled in the "system.cfg" file: In the GENERAL FLAG section, the HIGH_BIT_RATE

flag must be set to YES. The MCU also provides high quality video (30 frames per second) for line rates up to T1/ E1 in Transcoding and Continuous Presence conferences, by allocating two video units (codecs) per participant. One of the video codecs is used for encoding, while the other is used for decoding the incoming video stream. This allows the video module to work at the high frame rate of 30 fps in both incoming and outgoing video streams. When running the conference, you can check which video codec handles the participant video by checking the video card properties.

- The two video codecs allocated to one Enhanced Video participant **must be** located on the **same** Video Bridge, but they do not have to be allocated to the same DSP processor. This may be problematic when a reserved conference is started, as at the reservation time the system only checks if there are free VCP processors without checking whether they are located on the same video board.
- Using two video units per participant reduces the number of participants that can be handled by a video card by half (to 6 participants in Continuous Presence conferences using Dual-video module).

To view the Video module units:

To list the Video module's units in the *Browser* pane, click the plus icon [+] next to the card icon.

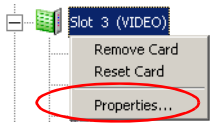
To display the module's units in the *Status* pane, click the card icon.

A list of the Video ports appears below the slot icon and in the *Status* pane.

Id	Config	Occupied	Faulty	Disabled	Ports State	Net Service	Percent Occupied
..							
1		No	No	No			
2		No	No	No			
3		No	No	No			
4		No	No	No			
5		No	No	No			
6		No	No	No			

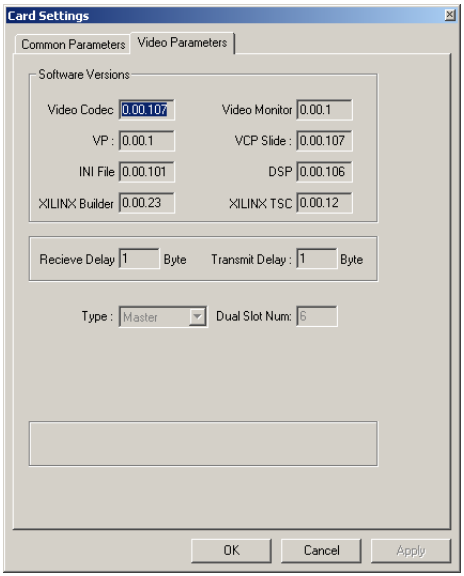
To view the video module properties:

1. In the *Browser* pane, right-click the slot containing the video card, and then click **Properties**. Alternatively, double-click the card icon.



The *Card Settings – Common Parameters* dialog box opens. For details, see *"Viewing the Common Card Parameters" on page 4-10*.

2. Click the **Video Parameters** tab to display the settings that are specific to the Video module.



The video module can be installed as standalone or dual video. In single mode, up to 6 endpoints can be connected to a conference. In a dual-video installation up to 12 participants can be connected to a conference. The installation type is indicated in the *Type* field. If a Dual module is installed, the bridged slot is indicated in the *Dual Slot Number* field. When standalone is indicated, the *Dual Slot Number* field indicates a random number (irrelevant to the MCU configuration).

The *Receive Delay* and *Transmit Delay* fields represent markers on the Backplane of the video card, and indicate the frequency that the receive and transmit information can be read.

The *Video* parameters are for viewing purposes only and cannot be modified as they are embedded in the card.

3. Click **OK** to exit the *Card Settings* dialog box.

Viewing the Video+ Module Specific Properties

The Video+ card is required for running conferences defined as Click&View or Continuous Presence - Quad Modes.

A flag in the "system. cfg" must be enabled: In the VIDEO PLUS FLAGS section the VIDEO_PLUS_YES_NO flag must be set to YES.

When a Video+ card is installed on the MCU, in the *Conference Properties–Resource Force* the default *Video* settings are set to **auto**. When set to **auto**, the system first uses or allocates the resources on the Video+ card. If the video settings are set to **standard**, the regular *Video* card is allocated. For more information see the MGC Manager User Guide, Volume I, Chapter 4. The number of Video+ cards that can be installed on the MCU is only limited by the number of slots available on the MCU.

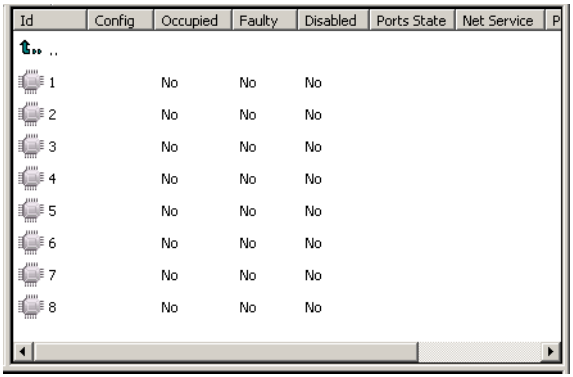
When more than one card is present you can select the specific card's slot from the *Slot* drop-down box in the *Conference Properties - Resource Force* dialog box.

To view the Video+ module units:

- To list the Video+ module's units in the *Browser* pane, click the plus icon [+] next to the card icon.

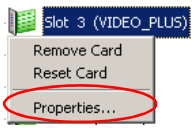
  To display the module's units in the *Status* pane, click the card icon.

A list of the Video+ ports appears below the slot icon and in the *Status* pane.



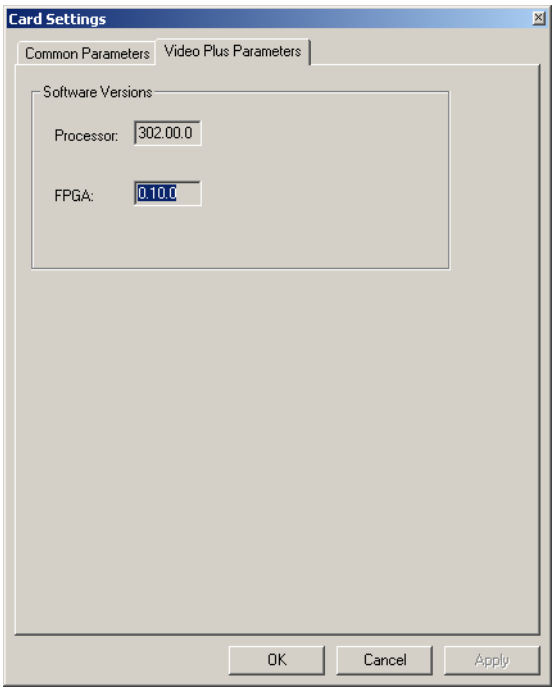
To view the Video+ module properties:

1. In the *Browser* pane, right-click the slot containing the Video+ card, and then click **Properties**. Alternatively, double-click the card icon.



The *Card Settings – Common Parameters* dialog box opens. For details, see *"Viewing the Common Card Parameters" on page 4-10*.

2. Click the **Video Plus Parameters** tab to display the settings that are specific to the Video module.



The Video+ module can accommodate up to 8 video participants. When more than one card is present on the MCU unit more video participants can be added. The Click&View application requires both Audio+ and Video+ capabilities.

The *Video Plus Parameters* are for viewing purposes only and cannot be modified as they are embedded in the card.

3. Click **OK** to exit the *Card Settings* dialog box.

Viewing the Data Module Specific Properties

The data module contains one bridge and three units. There are two types of data cards: T.120 standard and T.120-24. The following table describes the number of ports supported by each unit on the card and the total number of participants supported by each card type.

Table 4-11: T.120 Card Types

Card Type	Number of ports supported by each unit	Total number of participants
T.120 standard	4	12
T.120-24	8	24

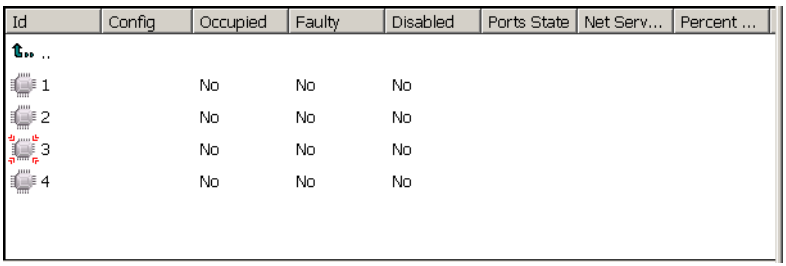
This also limits the number of conferences that can be handled by the data module. Up to 12 (24) conferences of one participant, one conference of 12 (24) participants, or any combination of number of conferences times the number of participants per conference, up to 12 (24) can be handled by the data module. The Data Bridge determines the participants to be handled by each unit and the number of simultaneous conferences to be handled by the data module.

To view the Data module units:

To list the Data module's units in the *Browser* pane, click the plus icon [+] next to the card icon.

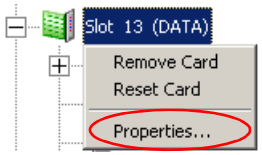
To display the module's units in the *Status* pane, click the card icon.

A list of the Data ports appears below the slot icon and in the *Status* pane.



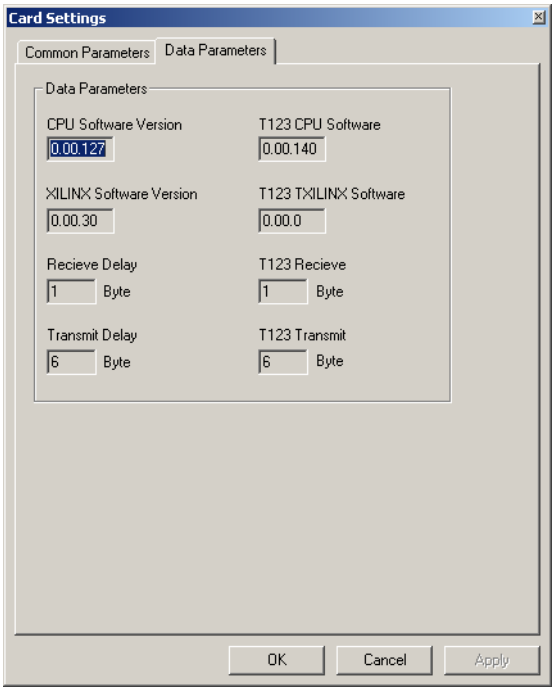
To display the card's properties:

1. Right-click the slot containing the data card, and then click **Properties**.



The *Card Settings – Common Parameters* dialog box opens. For details, see *"Viewing the Common Card Parameters" on page 4-10*.

2. Click the **Data Parameters** tab to display the settings that are specific to the Data module.



The *Data Parameters* are for viewing purposes only and cannot be modified as they are embedded in the card. *Data Parameters* indicate the software versions of the various components of the data card.

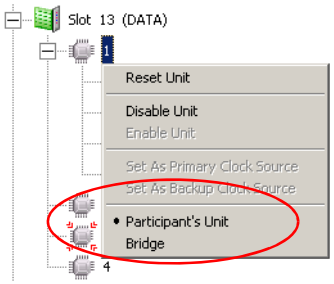
3. Click **OK** to exit the *Card Settings* dialog box.

Changing a Data Unit Type

You can designate a unit as a Data Bridge and change the Data Bridge configuration to a standard Data Unit (participant's unit).

To change a data unit type:

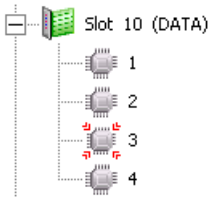
1. In the *Browser* pane, click the plus [+] next to the slot containing the Data module to configure.
2. Right-click the unit to configure.



3. Click the desired option:
   - To change the Bridge unit to a standard unit, click the **Participant's Unit** option. The *Bridge* icon changes accordingly.
   - To designate a unit as a Bridge, click the **Bridge** option. The unit's icon changes accordingly.

Listing the Ports for each Data Unit

You can view the list of ports per Data Unit by clicking the Data Unit or Data Bridge icon.



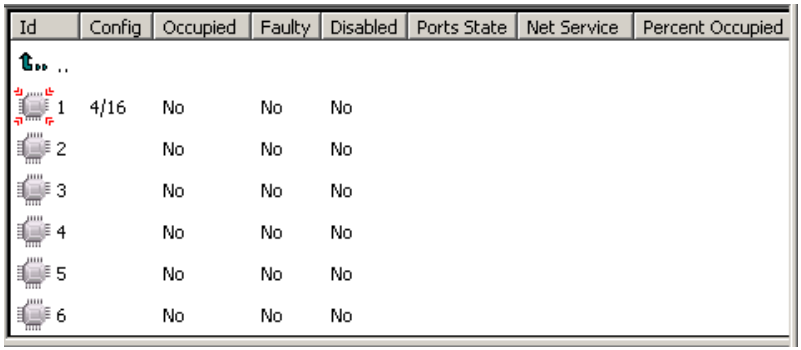
Resetting, Enabling and Disabling Units

Each card contains functional units which handle the conferences. These units may be reset, disabled or enabled. In addition, the units may have specific configuration options.

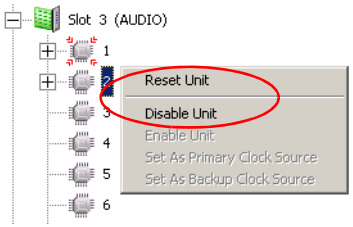
To reset, enable, or disable a unit:

1. In the *Browser* pane, expand the card tree.
   The module's units are displayed in the *Browser* pane.

   Alternatively, click the card icon to display their configuration in the *Status* pane.



2. Right-click the unit to reset, disable or enable.



3. Click the appropriate option according to the required operation.

Table 4-12: Unit Reset, Enable and Disable Options

Option	Description
Reset Unit	Resets the unit. Use this option when the unit causes problems while running a conference, and resetting may solve it. You cannot reset a unit while it is running a conference. Resetting a unit which was previously disabled automatically enables it.
Disable Unit	Disables the selected unit. A disabled unit cannot be used to run conferences. Use this option when the unit is faulty, and you do not want the MCU to try using it to run conferences.
Enable Unit	Enables the selected unit that was previously disabled.

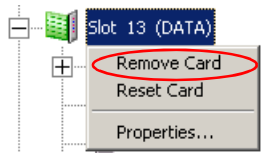
Removing a Card From the MCU

The MGC Manager allows you to remove a card from the available resources list in order to prevent its use by the system. In such a case, the system will change the color of the slot icon from green to white indicating that the slot is unused. The card will not be used from this point on to run conferences.

Resetting the MCU or using the *Reset Card* function for this slot while the card is still installed in the MCU will cancel the deletion of the card from the available resources list and reinstate it to its original function.

To remove a card from the available resources list:

- Right-click the slot containing the card to remove, and then click **Remove Card**.



The card is removed from the available resources list and the color of the slot icon changes from green to white. The card will not be used to run conferences until it is reset or the MCU is reset.

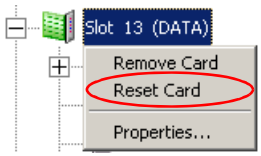
A card cannot be removed while it is running a conference.

Resetting a Card

If you notice that some conferences cannot run and you suspect that there is a problem with the card, resetting the card may solve the problem.

To reset a card:

- Right-click the slot containing the card to reset, and then click **Reset Card**.



A card cannot be reset when it is running a conference.

Resetting a card that was previously removed from the resources list (but still installed in the MCU) will reinstate the card for use.

IP and Video+ Reset Card and Self Recovery

If an RTP processor fails during a conference, the participants will be muted and video streams frozen.

Self Recovery is an automatic process performed by the Card Manager processor resulting in a reset of the IP unit. When the unit resets, the participants are not disconnected, and their video and audio are restored within 10 seconds.

Self Recovery is also performed by the Card Manager if the Video+ MAP unit fails. When the unit resets, the participants are not disconnected, and their video and audio are restored within 10 seconds.

Reset Unit allows you to manually reset the IP or Video+ unit. This operation can be performed only when the unit is free and not occupied by participants.

The manual and automatic reset procedures can be initiated by methods described in Table 4-13, "Automatic and Manual Reset Options."

Table 4-13: Automatic and Manual Reset Options

Process	Method	Initiated from	Flag/Card Settings
Reset Unit	• Manual Reset	MGC Manager	Manual Card reset by right-clicking the unit and selecting *Reset Unit*.
Reset Unit	• Manual Reset	IP Terminal	Manual Card reset command (card_reset<Board_Id><Unit_Id>) sent from the IP Terminal to the MCU.
IP Self Recovery (enabled)	• Auto Reset	MCMS Request	Implemented in the RTP processor (component failure). Initiated if the “system.cfg” flags in the CARDS section are configured as follows: RTP_SELF_RECOVERY=YES RESET_UNIT=NO
IP Self Recovery (disabled)	• Auto Reset	MCU (Card Manager)	Implemented in the RTP processor (component failure). Initiated if the “system.cfg” flags in the CARDS section are configured as follows: RTP_SELF_RECOVERY=NO RESET_UNIT=YES
Video+ Self Recovery (enabled)	• Auto Reset	MCMS Request	Implemented in the RTP processor (component failure). Initiated if the “system.cfg” flags in the CARDS section are configured as follows: MAP_SELF_RECOVERY=YES RESET_UNIT=NO
Video+ Self Recovery (disabled)	• Auto Reset	MCU (Card Manager)	Implemented in the RTP processor (component failure). Initiated if “the system.cfg” flags in the CARDS section are configured as follows: MAP_SELF_RECOVERY=NO RESET_UNIT=YES

5

MCU System Management

This chapter describes how to use the various utilities provided with the system.

Only users (MGC Manager operators) with Superuser rights can perform MGC Manager configuration tasks. In addition the user must have Superuser rights on the computer on which the MGC Manager application is running, or any other permission than enables the application to access the Registry (read/write) and read/write files on the C: drive (root directory) and under the Windows directory folder.

The following tasks are detailed:

- Setting audio look and feel (page 5-143)
- Setting the default communication parameters (page 5-144)
- Setting audible alarm to monitor Faults (page 5-146)
- Marking faulty participants in red(page 5-147)
- Setting the MGC Manager to monitor participants in all conferences (page 5-148)
- Configuring shortcut keys (page 5-149)
- Configuring audio alert event indications (page 5-151)

The MCU must be connected in order to perform the above tasks. For details, see the MGC Manager User's Guide, Volume I, Chapter 3, “Connecting to an MCU”.

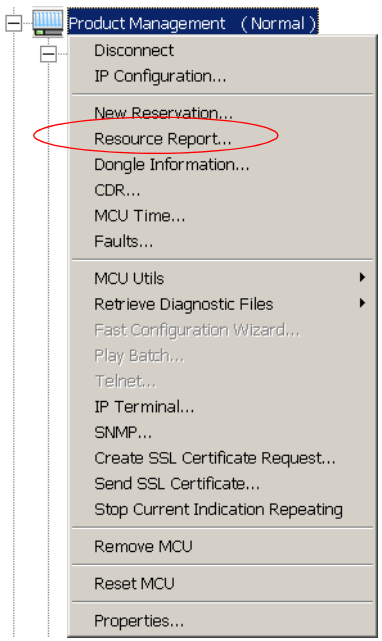
MCU Resource Report

The Resource Report details the availability and usage of the system resources (various card types). Filters may be used to minimize scrolling up and down allowing for ease of viewing information. The Resource Report generates a report of the resource allocation of all the Functional Module cards. Active and reserved resources are listed.

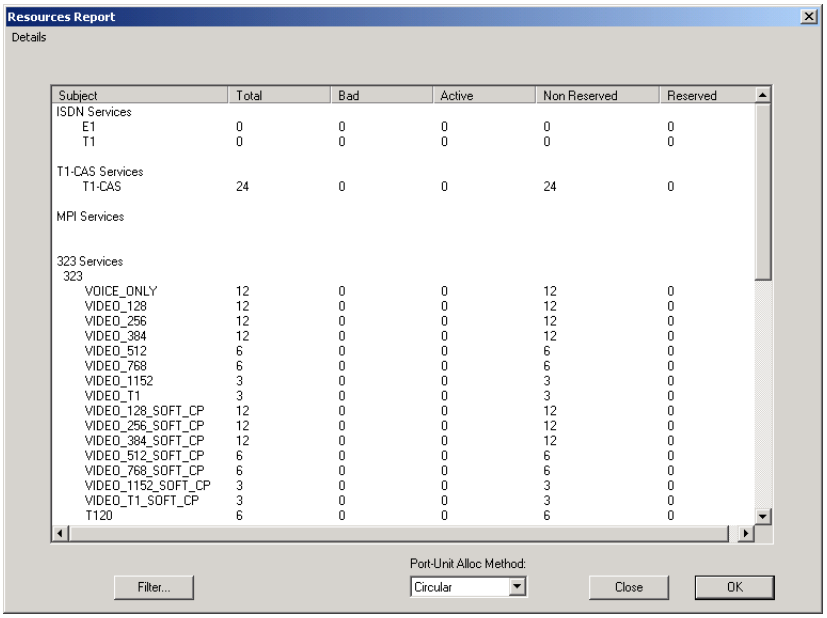
The Resource Report displays the number of ports that can be allocated to participants and the number of ports that cannot be used (Bad). Once the conference is reserved on the MCU or it has started, the Resource Report also displays the number of ports currently being used by participants (Active) and reserved (reserved to start within the next 5 minutes) to participants and the number of free ports that can still be allocated to participants for each card type.

To view the MCU resources:

Right-click the *MCU* icon, and then click **Resource Report**.



The *Resource Report* dialog box opens.



The Resource Report window contains the following columns:

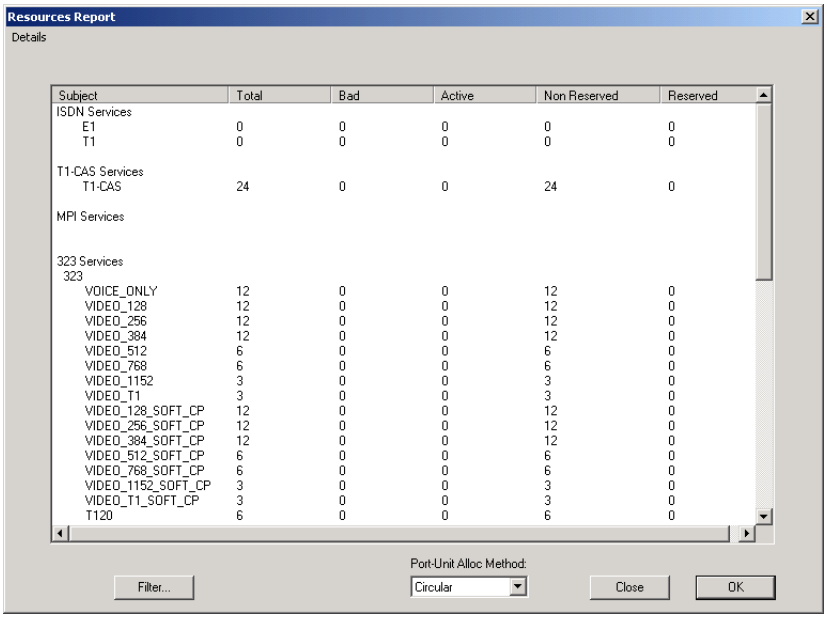
Table 5-1: Resource Report Columns

Column Title	Description
Subject	The type of resource. Resource types include the *Network Resources* that are used by participants to connect to the system, and *Media Resources* that are used by the system to run different types of conferences.
Total	The total number of resources of the same type installed on the system.
Bad	The number of disabled or faulty resources of each type.
Active	The number of ports currently used to run conferences for each resource type.
Non Reserved	The number of ports which are not reserved to be used within the next 5 minutes for each resource type.

Table 5-1: Resource Report Columns (Continued)

Column Title	Description
Reserved	For each resource type, the number of active ports plus the number of ports for conferences that have reserved resources but disconnected participants, and the number of ports for reserved conferences to be run in the next 5 minutes.

Resources Report - Network Area



The *Network Area* describes the bandwidth and port availability for participants connecting over various types of networks. This information includes **network resources only**. In order for a participant to connect to a conference, he/she may also require Audio, Video, and/or MUX/MUX+ resources, depending on the type of participant and the type of conference. Details about the availability of these resources are presented in the lower section of the *Resources Report* window and described in the "Resources Report - Media Resources Area" on page 5-8.

Network Area Parameters description

Each row item appearing in the *Network Area* is described below.

- **ISDN and ATM Network Services** - This section describes the available bandwidth, in Bearer Channels (B channels), for each type of ISDN and ATM network connection. Only the installed types of connections are displayed:
  - **155** - Number of B channels available with an ATM-155 Mbps card
  - **25** - Number of B channels available with an ATM-25 Mbps card
  - **E1** - Number of B channels available with E1 ISDN spans
  - **T1** - Number of B channels available with T1 ISDN spans
- **T1-CAS Network Services** - This section describes the available number of channels (B channels) for each T1-CAS span. Each T1-CAS span consists of 24 channels. Each T1-CAS (Audio Only) participant is allocated one network channel and one Audio+ port.
- **MPI Network Services -** This section describes the available number of ports for each type of MPI connection - Data Terminal Equipment (DTE) or Data Communication Equipment (DCE). For more information about these types of MPI connections, see “Defining an MPI Network Service” on page 3-99. Only the installed types of connections are displayed:
  - **DCE** - The number of ports configured as DCE
  - **DTE** - The number of ports configured as DTE
- **IP Services** - IP resources per participant type. This section describes the available ports for each possible type of IP (H.323 and SIP) participant. The available number of ports in any particular row represents the **total bandwidth and resources available for all types of participants**, so if one type of participant were to use some resources, the available resources for all other types of participants (rows) would be less.

  The Resources Report displays the total number of IP ports available according to the Conference Type, Line Rate, and Encryption in the format:

  Media_Line Rate_Conference Type. *Media* may include *Voice*, *Video* or *Encrypted Video* ports. For example: VOICE_ONLY, designating Audio Only participant resources; VIDEO-128-SOFT_CP, designating video participants using a line rate of 128 Kbps in a Software Continuous Presence conference.

All IP participant types are listed in this manner, listing the available resources for IP participants in Standard Video and Audio Conferences, Software Continuous Presence, Encrypted Participants, Encrypted Participants in Software CP and Encrypted Participants in People Plus Content.

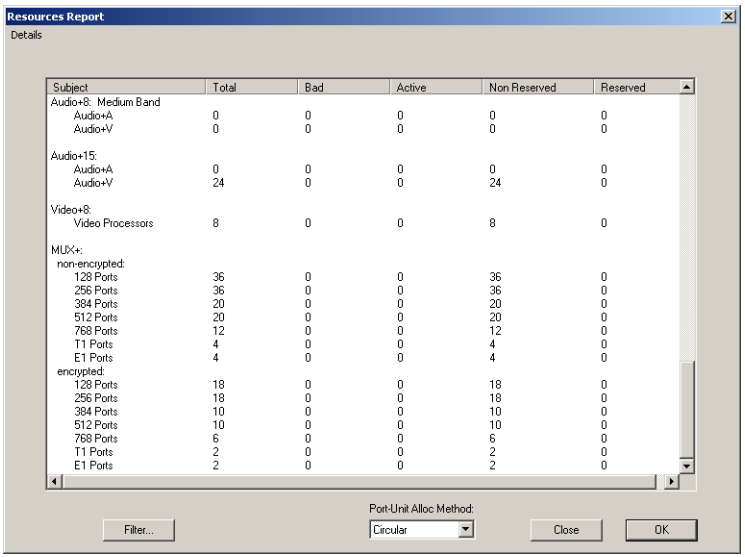
The following table lists the total number of ports available for both non-encrypted and encrypted participants based on their connection Line Rates and IP+ card type.

Table 5-2: IP+ Port Capacity With/Without Encryption

Line Rate Kbps	Number of Participants					
	IP+12		IP+24		IP+48	
	Non-encrypted	Encrypted	Non-encrypted	Encrypted	Non-encrypted	Encrypted
128	32	16	64	32	96	48
256	32	12	64	24	96	36
384	16	8	32	16	48	24
512	16	6	32	12	48	18
768	8	4	16	8	24	12
T1/E1	4	2	8	4	12	6

Resources Report - Media Resources Area

Resources used by participants from different types of networks are displayed in the lower section of the *Resources Report* window. To view the *Media Resources Area*, use the scroll bar on the right side of the window.



In the example shown here, the system lists the total number of ports available with the MUX+20 card for both non-encrypted and encrypted participants, based on their connection line rates. At a line rate of 128 Kbps, up to 36 non-encrypted and 18 encrypted participants can connect to conferences. At a line rate of 384 Kbps, 20 non-encrypted and 10 encrypted participants can connect to conferences running on the MCU.

Media Resources Area Parameters Description

Each row item appearing in the *Media Resources Area* is described below.

- **MUX -** The MUX card multiplexes and demultiplexes the audio, video and data streams for ISDN, MPI and ATM participants. When using the Standard Audio card, MUX resources are also required for Audio Only participants (in addition to video participants). MUX resources are not required for IP participants or Audio Only participants running on an Audio+ card.

Each MUX card contains four units. Each unit can handle 4 participants at up to 384 Kbps, 2 participants at up to 768 Kbps or 1 participant at up to 1920 Kbps (E1). Each unit can be configured by the Operator. For more information about configuring MUX units, see "Viewing and Configuring the MUX Module Specific Properties" on page 4-27. The data is presented as totals for all MUX cards installed in the MCU:

— Number of ports available for participants of up to 384 Kbps

— Number of ports available for participants of up to 768 Kbps

— Number of ports available for participants of up to1920 Kbps

- **MUX+** - Displayed is the total number of MUX+ port resources available according to the card type, line rate and encryption. The MUX+ card, like the MUX card, is used for connecting ISDN and T1-CAS video participants to the conference. A flexible port resource allocation mechanism is available with the MUX+ card and allocates ports dynamically thereby decreasing fragmentation. It enables the MCU to allocate and free resources according to the conference requirements without pre-configuring the Line Rate on each card unit. A conference can be run on multiple MUX+ cards. Encrypted participants always require MUX+ resources and use more resources than a regular participant. IP Video participants do not require the MUX+ card, because all IP cards have built-in MUX+ functionality. MUX+ resources are calculated according to the relative weight assigned to the different line rates.

  The following table details the number of ports available with the MUX+ cards.

Table 5-3: MUX+ Cards Port Capacity

Card type	Participant Line Rate	Number of non-encrypted ports capacity	Number of encrypted ports capacity
MUX+10			
	128	18	9
	256	16	9
	384	10	5
	512	10	5

Table 5-3: MUX+ Cards Port Capacity (Continued)

Card type	Participant Line Rate	Number of non-encrypted ports capacity	Number of encrypted ports capacity
	768	6	3
	T1	2	1
	E1	2	1
MUX+20			
	128	36	18
	256	32	18
	384	20	10
	512	20	10
	768	12	6
	T1	4	2
	E1	4	2
MUX+40			
	128	72	36
	256	64	36
	384	40	20
	512	40	20
	768	24	12
	T1	8	4
	E1	8	4

- **Audio** - Standard Audio cards resources. Each Standard Audio card contains 12 audio ports and 1 Audio Bridge unit. The Audio Bridge unit can be configured by the Operator to run one conference of up to 30 participants (from across multiple Standard Audio cards), up to 4 conferences of up to a total of 16 participants (from across multiple

Standard Audio cards) or up to 6 conferences for up to 12 participants (gateway sessions). For more information about configuring the Audio Bridge unit on the Standard Audio card, see "Viewing and Configuring the Audio Module Specific Properties" on page 4-31. The data is presented as totals for all Standard Audio cards installed in the MCU:

— Number of audio ports

— Total number of conferences configured (excluding 2-way conferences)

— Number of 2-way (gateway) conferences configured

- **Video** - Standard Video cards resources. The Standard Video card is used only for Transcoding and Continuous Presence conferences.

The Standard Video card is not required for H.323 Software Continuous Presence conferences. The resources for Video+ cards work differently from Standard Video cards resources and are presented separately in the Resources Report.

A single Standard Video card contains 6 video ports; a dual Standard Video card contains 12 video ports. All participants in a single conference must be managed by the same Standard Video card. Therefore, the maximum number of participants in a conference is 6 (single video card) or 12 (dual video card). The Standard Video cards resources are presented in the following manner:

— **Video Codecs** - Total number of video ports on all installed Standard Video cards. To check whether there are dual Standard Video cards installed, in order to run a Continuous Presence or Transcoding conference of more than 6 participants, or to view which resources are being used on which Standard Video cards, view the card parameters as described in "Viewing the Video Module Specific Properties" on page 4-37.

- **Data** - Total number of T.120 resources for data conferencing.

  — **T.123 Ports** - Total number of ports available for participants using T.120. These resources are used by ISDN, ATM and MPI participants and can be used across multiple T.120 cards.

- **Audio+8** - The Audio+8 card contains 8 DSPs and can support 24 or 48 ports, depending on configuration. When configured to *Medium Band*, each card can support 48 Audio Only participants or 24 Video participants, but cannot support the SIREN14 audio algorithm. When

configured to *Wide Band*, each card can support the SIREN14 audio algorithm, but the maximum number of participants supported is 24. Audio Only participants using Audio+ cards do not require MUX card resources and each Audio+ card is not limited in the number of conferences that it can run.

  - **Audio+A** - Total number of Audio Only (G.711) participants that can be supported by all Audio+8 cards installed in the MCU.
  - **Audio+V** - Total number of video participants supported by all Audio+8 cards installed in the MCU. Fewer participants can be supported, as the card must be prepared to compress/decompress audio algorithms used in video conferences, such as G.722, that require robust digital signal processing.

- **Audio+15** - The Audio+15 card contains 15 DSPs and can support 48 or 96 ports, depending on configuration. When configured to *Audio Only*, each card can support 96 Audio Only participants. When configured to *Video*, each card can support 48 participants and can support the SIREN14 audio algorithm. Audio Only participants using Audio+ cards do not require MUX card resources and each Audio+ card is not limited in the number of conferences that it can run.
  - **Audio+A** - Total number of Audio Only (G.711) participants that can be supported by all Audio+15 cards installed in the MCU.
  - **Audio+V** - Total number of video participants supported by all Audio+15 cards installed in the MCU.

The following tables detail the card capacities according to the Audio algorithm used in the conference when the MCU is configured to Medium/Wide Band.

Table 5-4: Audio+ Card Capacity Per Audio Algorithm - Medium Band Setting

Card Type	Audio Algorithm							
	G.711	G.722	G.722.1	G.728	G.723.1	G.729	Siren7	Siren14
Audio+8A	48	24	24	24	48	—	24	Not supported in Medium Band mode
Audio+8V	24	24	24	24	24	—	24	
Audio+12/24	24	12	12	12	21	21	12	
Audio+24/48	48	24	24	24	48	48	24	
Audio+48/96	96	48	48	48	96	96	48	

Table 5-5: Audio+ Card capacity Per Audio Algorithm - Wide Band Setting

Card Type	Audio Algorithm							
	G.711	G.722	G.722.1	G.728	G.723.1	G.729	Siren7	Siren14
Audio+8A	48	12	12	12	12	—	12	12
Audio+8V	12	12	12	12	12	—	12	12
Audio+12/24	24	12	12	12	21	21	12	12
Audio+24/48	48	24	24	24	24	48	24	24
Audio+48/96	96	48	48	48	48	96	48	48

Table 5-6 details the types of cards that can be used together in the same conference.

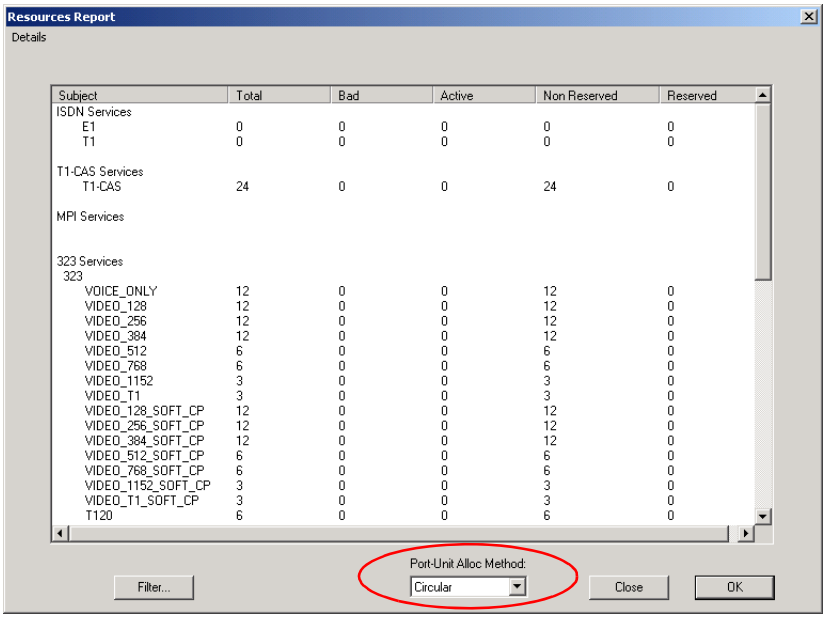
Table 5-6: Conference Compatibility Matrix

Card Type	Audio 12 (standard)	Audio+(n) with Audio	Audio+(n) with Video
Audio 12 (standard)	yes	no	no
Audio+(x) with Audio	no	yes	yes
Audio+(x) with Video	no	yes	yes

There is no limit on the number of conferences that can be handled by one module (the number of ports is the only limit), and there is no need to configure the audio bridge on the Audio+ module.

- **Video+8** - The Video+8 card contains 8 video processors and performs video processing for participants in Continuous Presence and Transcoding conferences. Conferences defined as *Continuous Presence - Quad Mode* must run on the Video+8 card. Participants from multiple Video+8 cards can take part in a single conference.
  - **Video Processors** - Total number of video processors from all Video+8 cards installed in the MCU. Each video processor can run a single Continuous Presence or Transcoding participant.

Port-Unit Allocation Area



The *Port-Unit Allocation Method* box determines how all the resources are allocated. The selection of the mode can be done only when no conference is running. The following modes are available:

Circular - The system allocates the next available sequential unit in the order in which it is numbered on the card according to the unit numbers. For example, if the last used unit is 2, the next time a conference is run, the system will allocate units starting with unit 3 (provided that unit 3 is free). This mode should be used when you suspect that there may be faulty units, allowing the system to allocate other units for the conferences while the faulty units are replaced, or reset. However, this mode should not be used when debugging the system, as the problems will be inconsistent if the problematic units are not used constantly.

Terminal - The system always starts the unit allocation from the first free unit on the first card. This mode may be problematic when there is one faulty unit (especially if it is the first or second) that prevents the system from running conferences. However, this should be the selected mode when debugging the system.

Viewing the Resource Report using Filters

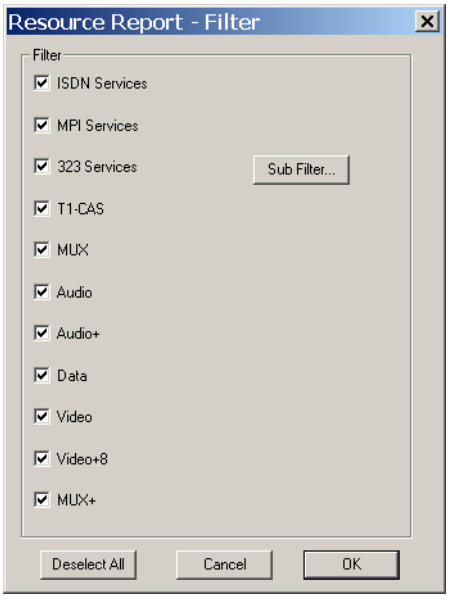
Filters may be used to include/exclude types of resources in/from the Resource Report enabling you to view only relevant and required information.

The *H.323 Sub Filter* allows the user to enable or disable algorithm groups together with their rates, for viewing in the Resource Report.

To view the MCU resources using filters:

1. In the *Resource Report* dialog box, click the **Filter** button.

   The *Resource Report - Filter* dialog box opens.



   The *Resource Report - Filter* dialog box enables the selection of resources according to services and boards. By default all items are selected. When selecting the H.323 Service the *Sub Filter* option enables you to select the Network Services to be included in the report.

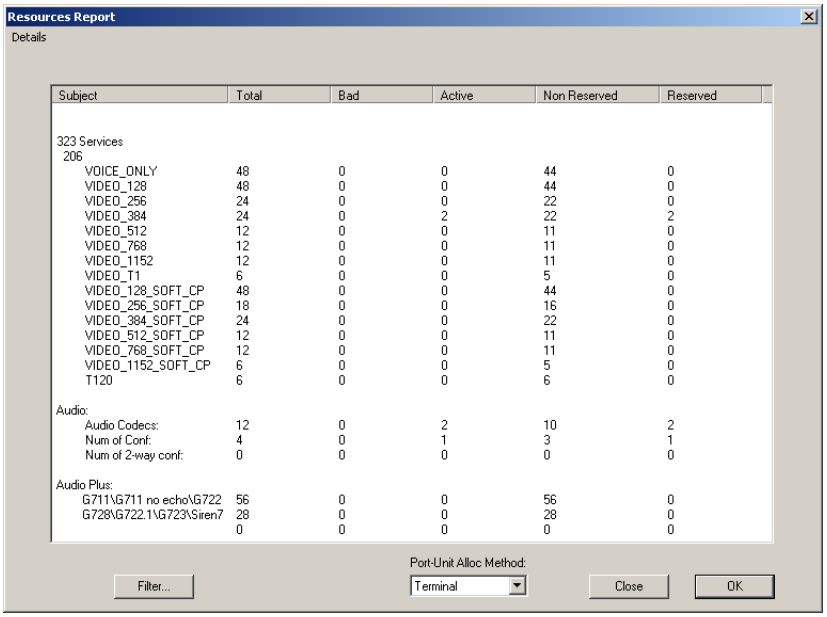
2. To exclude a resource type from the *Resource Report*, clear the check box.

   To exclude specific H.323 Line Rates from the *Resource Report* click the **Sub Filter** button.

The H.323 *Service-Filter* dialog box opens.

3. By default, all Line Rates are selected for display. To exclude Line Rates, clear their check boxes and then click **OK**.

4. Click **OK** or **Close**.
   The *Resource Report* window is refreshed showing only selected topics.

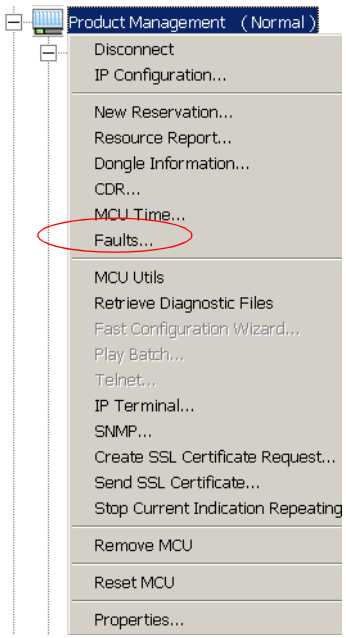


MCU Faults Report

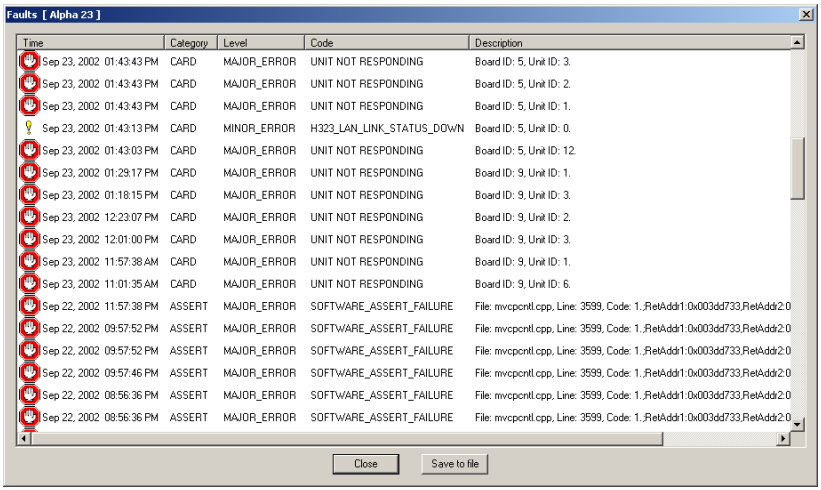
The *Faults* function records faults related to the MCU that are encountered during operation. In addition, if the automatic performance monitoring option is enabled to automatically monitor the performance of the ISDN lines connected to the system, the fault messages issued by the Performance Monitoring appear in the Faults list. For more details, see “Appendix C: Performance Monitoring NET-T1/Net-E1” on page C-1.

To view the Faults list:

1. Right-click the *MCU* icon, and then click **Faults**.



The *Faults* window opens.



The following columns appear in the *Faults* report:

Table 5-7: Faults Columns

Field	Description
Time	Lists the date and time that the fault occurred. This column also includes the icon indicating the fault Level. The Levels and their icons are detailed in the Level field.
Category	Lists the type of fault. The following categories may be listed: • *File* - the fault is caused when a problem is detected in one of the files stored on the MCU's hard disk. • *Reservation* - indicates that conferences that were reserved in the system when the system was shut down were not recovered when the system restarted. • *Card* - indicates problems with a card. • *Exception* - indicates errors reported by the computer (PC).

Table 5-7: Faults Columns (Continued)

Field	Description
Category (cont.)	• *General* - indicates general faults. • *Assert* - indicates internal software errors that are reported by the software program. • *Startup* - indicates errors that occurred during system startup.
Level	Indicates the severity of the problem. There are three fault indicators: • Major Error • Minor Error • System Message • MCU Startup indicator The icon of the fault Level appears in the Time column.
Code	Indicates the code of the problem, according to the fault category. A list of codes per category can be found in Appendix B.
Description	When applicable, displays a more detailed explanation of the cause of the problem.

If the *High Bit Rate* flag in the "system.cfg" is set to **Yes**, and the MCU contains video cards of a version older than 1.43, the MCU status changes to Major and an appropriate error message is added to the Faults log. The video card that does not support the High Bit Rate is pulled out from the available resources list and it is not used to run conferences.
If the *High Video Frame Rate* flag in the "system.cfg" is set to **Yes**, and the MCU contains video cards of a version older than 1.43, the MCU status changes to Major and an appropriate error message is added to the Faults log. The video card that does not support the High Frame Rate is pulled out from the available resources list and it is not used to run conferences.

2. You may save the Faults report to a text file. To do so, click the **Save to file** button.

The *Save As* dialog box opens.

3. Select a destination folder and enter the file name, and then click **Save**.

   You are returned to the *Faults* window.

4. To exit the *Faults* window without saving the data to file, click the **Cancel** button.

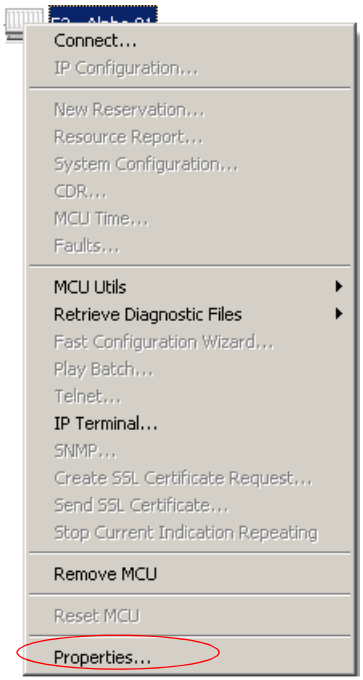
Verifying the MCU Properties

The *Properties* function is used to view the currently defined MCU settings, and modify them when required.

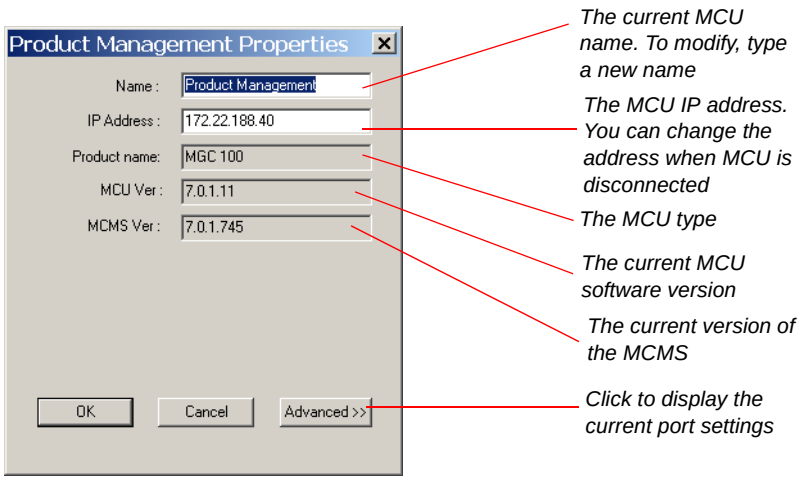
To verify the MCU properties

To modify any MCU settings apart from the MCU name, the MCU must be disconnected.

1. Right-click the *MCU* icon, and then click **Properties**.

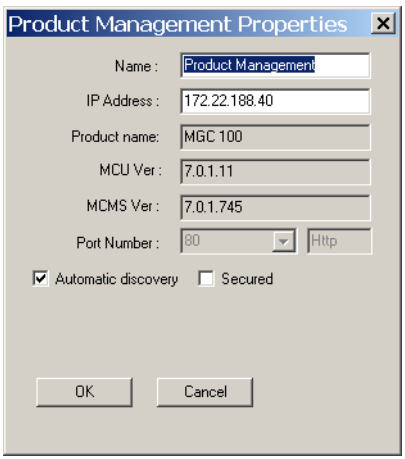


The MCU *Properties* dialog box opens.



2. To verify the port settings, click the **Advanced** button.

   The *Port Number* field, and the **Automatic Discovery** and **Secured** check boxes, appear in the *MCU Properties* dialog box.



The *Port Number* field identifies the MCU port to which the MGC Manager initially connects. If the *Automatic Discovery* option is enabled, then after initially connecting to the MCU, the system checks the system.cfg file for the preferred port. The preferred port is defined using

flags in the GENERAL section of the system.cfg file. If security is mandatory, that is, the value of the SECURED_PORT_MANDARTORY_FOR_API flag is YES, then the preferred port is actually the preferred secure port as defined in the PREFERRED_SECURED_PORT flag. Otherwise the preferred port is defined in the PREFERRED_PORT flag.

3. To modify the port settings:
   a. Clear the **Automatic Discovery** check box to enable the *Port Number* field.
   b. In the *Port Number* list, select the listening port number from the drop down list. For a secured connection, select port 443.
   c. For a secured connection to the MCU, select the **Secured** check box.
4. Click **OK.**

   For a detailed description of how to define the MCU's IP address, see *"First Entry IP Configuration" on page 2-7*.

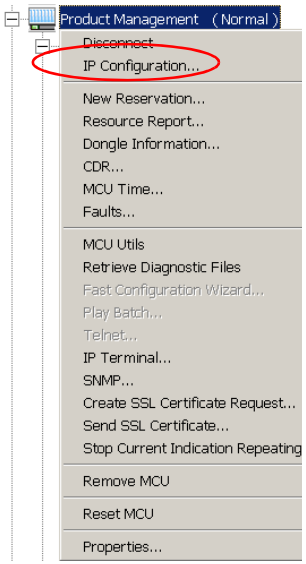
Modifying the MCU's IP Configuration

The IP Configuration function is used to view, and if required, to modify the MCU IP address. and additional network parameters.

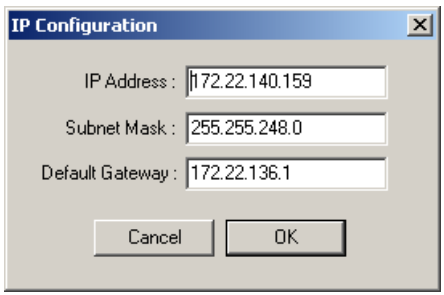
Warning!
The IP configuration defines the network access to the MCU. Modifying one of these parameters carelessly may suspend the communication with the MCU. Use this option when moving the MCU from one network to another, or when the addresses of the network elements are modified.

To view/modify the MCU's IP address:

1. Right-click the *MCU* icon, and then click **IP Configuration**.



The *IP Configuration* dialog box opens.



2. The following parameters may be modified:

Table 5-8: IP Configuration Options

Option	Description
IP Address	The system displays the currently defined IP address. To modify the address, enter the new address.
Subnet Mask	Displays the current IP address of the subnet mask. To modify it, enter a new IP address.
Default Gateway	Displays the current IP address of the default gateway. To modify it, enter a new IP address.

3. Click **OK**.

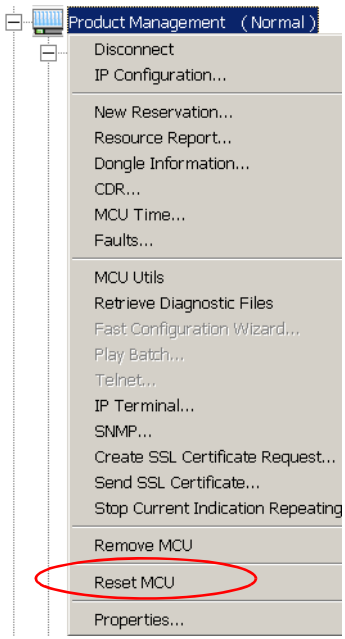
Reset MCU

The *Reset MCU* function is used to reset the MCU when there are substantial changes to the MCU hardware, or when there are problems with the MCU. If a reset is performed while running On Going Conferences, then at the end of the MCU Startup these conferences are automatically restored with all the participants in "Standby" state, and will be reconnected to the conference.

When the MCU is started, only the list of near future reservations is loaded to the MCU memory, while the information of all other reservations are kept on the MCU's hard disks, resulting in faster loading time.

To reset the MCU:

- Right-click the *MCU* icon, and then click **Reset MCU**.



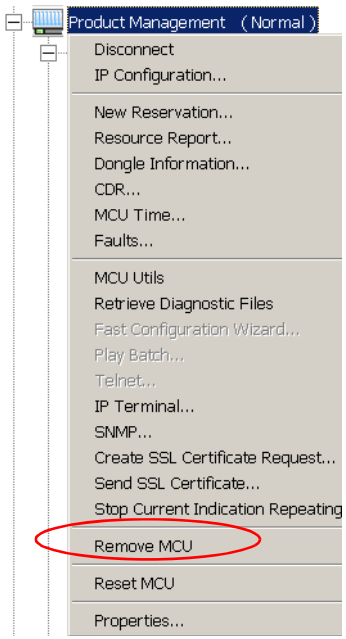
When the MCU is resetting, the MCU icon changes accordingly.

Remove MCU

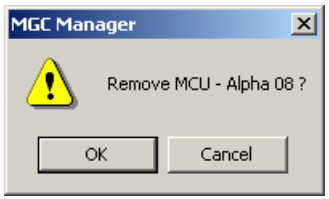
The *Remove MCU* function is used to remove an MCU from the MGC Manager - MCUs list. This function should be used if the MCU hardware was disconnected and removed from the network.

To remove the MCU:

1. Right-click the *MCU* icon, and then click **Remove MCU.**



A confirmation message is displayed.



2. Click **OK** to remove the MCU or **Cancel** to cancel the operation.

Telnet

The Telnet function is used to connect to another computer or MCU for file maintenance. The access to the MCU via Telnet is password protected, as with normal logging into the MCU. This function is intended for Polycom's internal use only.

IP Terminal

The IP Terminal is a feature used for debugging and recording traces of specific tasks that have been suspended due to an exception. An exception is an interruption to the normal flow of a program. The traces can then be analyzed to determine the source of the problem. The following are common exceptions:

- Division by zero
- Stack overflow
- Disk full errors
- I/O (input/output) problems with a file that is not open

The path of each task is recorded in its stack (a set of data storage locations that are accessed in a fixed sequence), and the IP Terminal feature traces all the addresses within that task's stack until the system finds the stage at which the exception occurred.

The system reads the value of the task's stack's first DWORD's (32 Bit) ESP (extended stack pointer) register values at the exception handling stage. This is done in a similar way to the mechanism that already exists in the system, by reading the EBP (extended base pointer) register values. The stack's contents are copied to a file. A new file is created every time the MCU is reset. It is possible to copy the contents to an existing file, in which case, the old data will be lost, as the latest traces will overwrite the file.

The IP Terminal only records traces of the first exception. The system is based on the assumption that the first exception is also the cause of other exceptions that may follow.

The file that is created contains the following details:

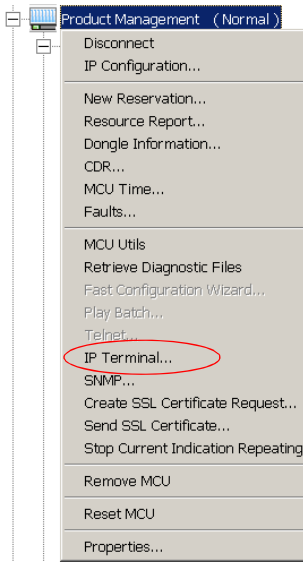
- Date and time of the exception
- MCMS software version number (allocated for internal use)
- Trace of the exception, as it already exists in the system
- Content of the stack

The stack's content is a sequence of DWORDs in HEX format (as it is shown in the debugger). The address of the first DWORD is printed at the beginning of each line.

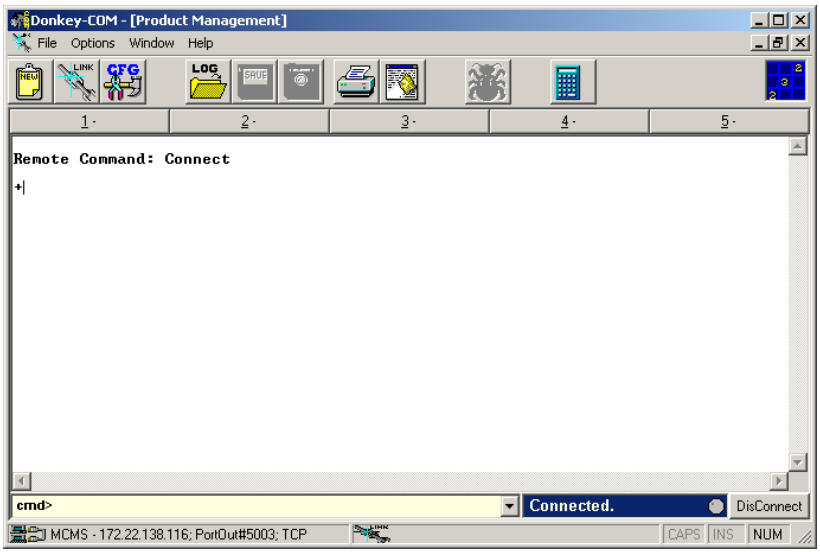
The exception files are kept on the MCU in the directory: c:\mcu\exceptns. This directory is created when the first exception occurs. If another exception occurs during a new lifetime of the MCU, the new exception file will be added to the same directory. Each exception file created by the system is named exceptns_n.txt, where n is the sequential number between 0 to 9. The first file starts with 0 and is named exceptns_0.txt. The c:\mcu\exceptns directory can hold a maximum of 10 files (the 10^{th} file is named exceptns_9.txt). When the directory is full (10 files are stored), and another exception occurs, the oldest file will be overwritten by the new exception file in a cyclic order.

To trace and capture a specific task that is suspended due to an exception:

1. Right-click the *MCU* icon, and then click **IP Terminal.**



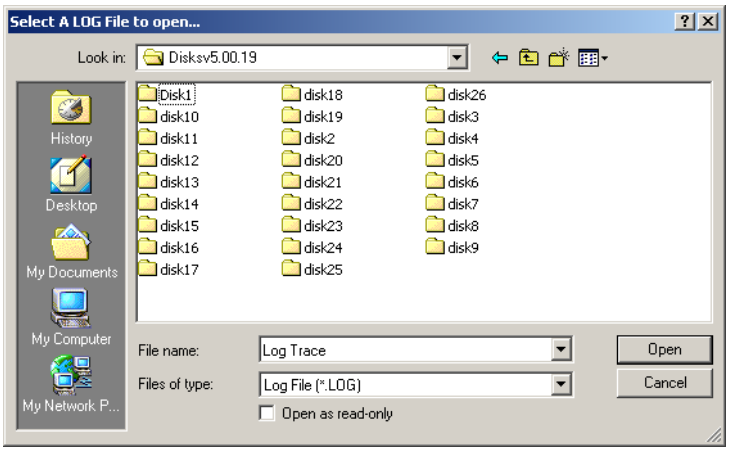
The *Donkey-COM* window opens.



An MCU can be configured to automatically begin a trace. Once the IP terminal is connected, the MCU activity is recorded and displayed on the screen. You can capture and save this information to a LOG file. Only information that was displayed after the creation of the LOG file will be saved in the file. All other information will be lost.

2. To create a new Log file, on the *File* menu, click **Open Log File**, or click the *Open Log File* icon on the toolbar.

   The *Select a LOG File to Open* dialog box opens.



3. In the *Look in* box, select a folder to which you wish to assign the log file.
   Use standard Windows procedure to open a folder.
4. In the *File name* box, enter the name of the file you wish to create.
5. Click **Open**.

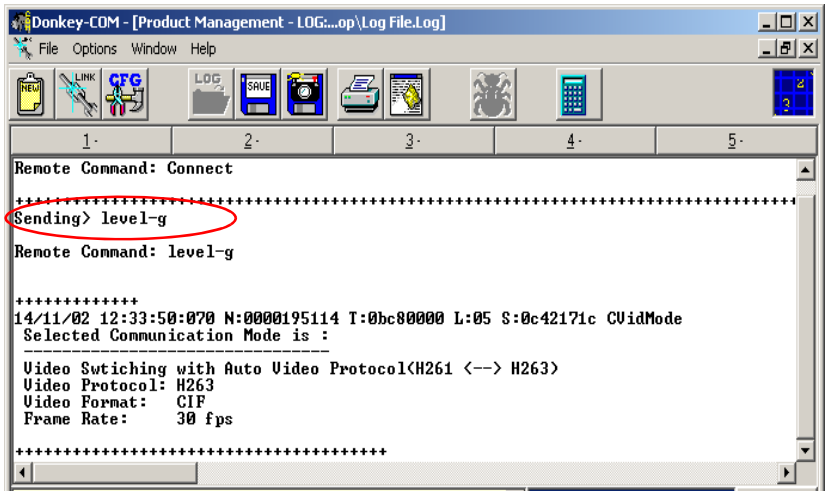
   You are returned to the *Donkey-COM* window, which displays the selected file name in the title bar.

This operation activates the capturing utility, which saves all the events that occur internally in the MCU to the LOG file. Once activated, the capturing utility remains active until you save the LOG file.

The information displayed in the automatic connection may be limited and too general. To display additional information for each trace, you need to define a different trace level.

6. In the command line of the *Donkey-COM* window, type **level-g** and press **Enter**.

The application acknowledges your command and the information will start downloading to the LOG file.



Step 6 should only be performed once.
Level-g is the most common level used to capture traces. The system does allow for trace capturing using different level commands, but is intended for internal purposes only.

7. When the downloading process is complete, save the LOG file by clicking **Save Log File** on the *File* menu, or by selecting the *Save* icon . All information that will be displayed in the IP Terminal window from this point on will not be saved to a file unless a new LOG file is created.

8. Repeat steps 2 to 5 and 7 to capture any new trace without closing the application.

Silence IT Fine-tuning

The SilenceIT mechanism enables the system to measure the audio energy, and based on this measurement, fine-tune the system usage of the SilenceIT algorithm. To reliably measure the audio energy, speech and noise/music must have sufficient energy, and be consistent across all audio ports.

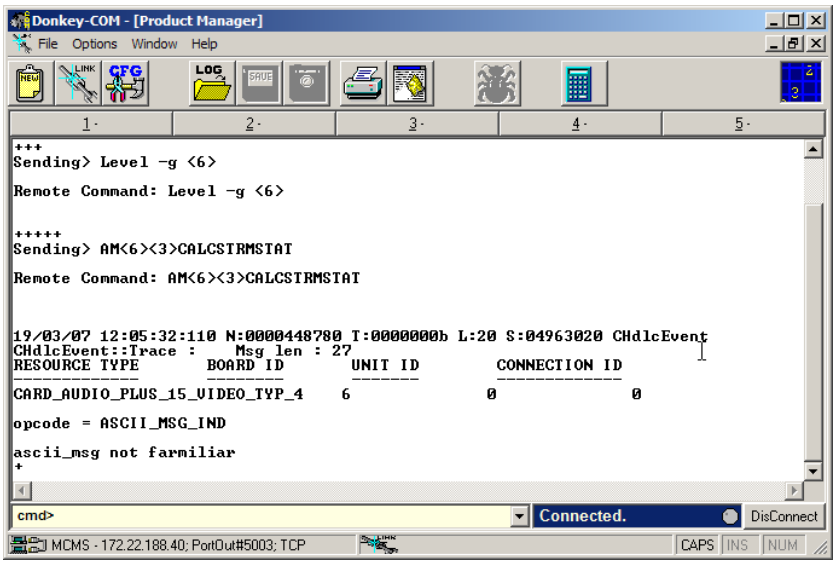
The audio energy measurements are done by connecting an endpoint to an ongoing conference, and using the IP Terminal to detect the noise/speech level. The values measured are then compared to the values listed in Table 5-9 on page 5-35. Based on the range of these values the user locates the corresponding parameter which is used to configure a system.cfg flag.

To enable the SilenceIT algorithm and fine-tune its operation:

1. Create an ongoing conference and connect an endpoint using a noisy line.
2. In the *Cards* section, locate the audio card used to handle the participant connection to the conference and write down the slot and unit numbers.
3. Using the participant's endpoint place the call on-hold.
   When the participant places the call on-hold music is heard.
4. Right-click the *MCU* icon, and then click **IP Terminal.**

   The *Donkey-COM* window opens.
5. In the *cmd*> field enter the following command: **Level -g <slot #>** and then press <Enter>.
6. In the command line enter: **AM<slot#><unit #>CALCSTRMSTAT** and press <Enter>.
   The message *"Started gathering signal statistics"* appears, indicating that the data gathering process has started.
7. Wait 15 seconds for the data gathering process to complete.

8. In the command line enter: **AM<slot#><unit #>GETCSTRMSTAT** and press <Enter>.



The signal statistics are retrieved and are displayed in the *Donkey-COM* window. Look for these parameters in the following format: "Average Energy = <Energy> Total VADS = <Total Vads>Consecutive VADS = < Consecutive Vads>".

If many messages are displayed, wait two minutes, and repeat step 8.

9. Record the *Energy, Total Vads* and *Consecutive Vads* values and locate these values in Table 5-9 on page 5-35 according to the *Noise Environment* (whether the call was placed from a quiet room or a noisy environment such as a cellular phone). Retrieve the corresponding parameter value.

Table 5-9: Noisy Line Tuning Table

Energy	Noise Environment	Total VADs	Consecutive VADs	Parameter Value
91<E<128 Or 182<E<256	Quiet	V < 50	V < 50	1

Table 5-9: Noisy Line Tuning Table

Energy	Noise Environment	Total VADs	Consecutive VADs	Parameter Value
76<E<91 Or 152<E<182	Quiet	V < 50	V < 50	2
67<E<76 Or 134<E<152	Quiet	V < 50	V < 50	3
0<E<67 Or 128<E<134	Quiet	V < 50	V < 50	4
91<E<128 Or 182<E<256	Noisy	V < 50	V < 50	5
76<E<91 Or 152<E<182	Noisy	V < 50	V < 50	6
67<E<76 Or 134<E<152	Noisy	V < 50	V < 50	7
0<E<67 Or 128<E<134	Noisy	V < 50	V < 50	8
E >1000	Variable	700<V	150<V<200	9
E >1000	Variable	650<V<700	150<V<200	10
E >1000	Variable	600<V<650	150<V<200	11
E >1000	Variable	500<V<600	150<V<200	12
E >1000	Variable	700<V	200<V<250	13
E >1000	Variable	650<V<700	200<V<250	14

Table 5-9: Noisy Line Tuning Table

Energy	Noise Environment	Total VADs	Consecutive VADs	Parameter Value
E >1000	Variable	600<V<650	200<V<250	15
E >1000	Variable	500<V<600	200<V<250	16
E >1000	Variable	700<V	250<V	17
E >1000	Variable	650<V<700	250<V	18
E >1000	Variable	600<V<650	250<V	19
E >1000	Variable	500<V<600	250<V	20

10. By default, the SilenceIT mechanism is disabled. To enable it, right-click the *MCU* icon and then click **MCU Utils>Edit "system.cfg"**.
11. In the **AUDIO PLUS FLAGS** section, add the flag **NOISE_LINE_DETECTION** = and enter the value found in step 9. Setting the flag value to 0 disables the SilenceIT mechanism.

    For more details about flag definition and system.cfg, see the *MGC Administrator's Guide, Chapter 5*.
12. Click **OK**.
13. Reset the MCU.

XPEK Silent Mode

To increase MGC unit security and as a hacking preventive measure, the MCU is now set by default to Silent Mode in order to ignore pings. MCU behavior is configured in the system configuration file (system.cfg), in the XPEK section, by defining the flag SILENT_MODE=YES.

For details of flag modification in the “system.cfg” see *“Edit “system.cfg”” on page 5-64*.

For those instances in which an MCU connection needs to be confirmed, there are several options for enabling pinging:

- Using IP Terminal commands to alter the ping settings temporarily without having to reset the system.

  In the IP Terminal window enter **allow_ping YES TIMEOUT**

  If SILENT_MODE=YES, the command allow_ping YES overrides the system.cfg settings, allowing the MCU to be pinged. The time-out is used to define an interval that restricts the time in which the MCU is exposed to pinging, after which the IP Terminal returns to the default Silent Mode setting defined in the system.cfg. The time-out is defined in seconds and it is added to the IP Terminal command. For example, if you define: allow_ping YES 30 there is a 30 second interval in which the MCU can be pinged.

  This combination of using a time-limited IP Terminal setting is the most secure method.

- Changing the default SILENT_MODE flag from YES to NO, which requires resetting the system.

  After changing this flag and resetting the system, the ping status can be determined using IP Terminal command only, changing the settings from YES to NO and vice versa. This last option may be easier to use, but is less secure.

  Using IP Terminal commands to alter the ping settings:

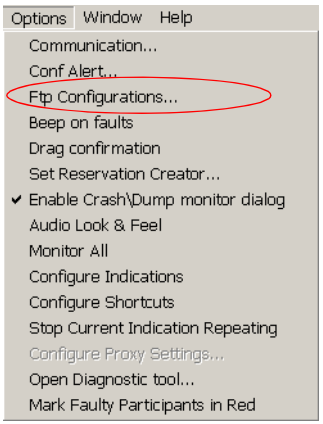
  In the IP Terminal window enter **allow_ping NO**.

HTTP and FTP File Transfer Modes

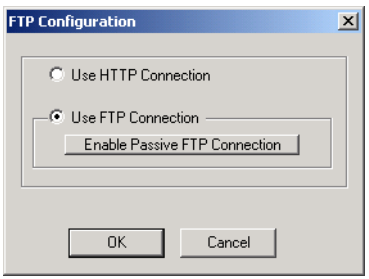
Files can be transferred using either an HTTP or an FTP connection. HTTP mode solves Firewall issues, PSOS limitations in the FTP mode and addresses security issues occurring in FTP. When selecting FTP mode, either an *Active* or *Passive FTP* connection can be enabled. Firewall issues can be solved by setting the MCU to Passive FTP mode. This is useful when the MGC Manager is within the Firewall zone and the MCU (hosted MCU) is outside the zone.

To set HTTP or FTP connection mode

1. In the *Options* menu, select **FTP Configurations**:

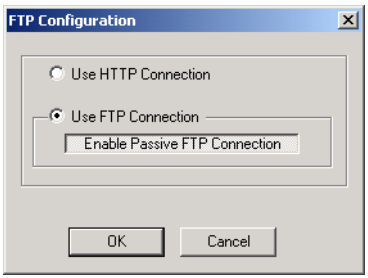


   The *FTP Configurations* dialog box opens.



2. To set the connection mode to HTTP, select **Use HTTP connection**. When the *HTTP* mode is active, *Enable Passive FTP Connection* is greyed out.

3. To set the connection mode to FTP, select **Use FTP Connection**.
4. To enable Passive FTP mode, click the **Enable Passive FTP connection** button.
   The **Enable Passive FTP connection** button appears selected.



When the Passive FTP connection is enabled, the client opens the primary connection to the server. The server acknowledges a connection request, and informs the client on which port to connect to the secondary connection. The client opens the secondary connection according to the port supplied by the server.

SNMP (Simple Network Management Protocol)

SNMP is a standard protocol for managing all types of network equipment. Adding SNMP functionality to the MCU enables monitoring of the MCU status by external managing systems, such as HP OpenView.

A network management system consists of two primary elements: a Manager and Agents. The Manager is the terminal through which the network administrator performs network management functions. Agents are entities that interface to the actual device being managed. Bridges, Hubs, Routers and MCUs are examples of managed devices that contain managed objects. These managed objects may be hardware, configuration parameters, performance statistics, and so on, that directly relate to the current operation of the device being monitored. These objects are arranged as a virtual information database, known as Management Information Base (MIB). SNMP allows managers and agents to communicate for the purpose of accessing these objects.

MIBs are a collection of definitions, which define the properties of the managed object within the device to be managed. Every managed device keeps a database of values for each of the definitions written in the MIB.

The H.341 standard defines the MIBs that H.320 and H.323 MCUs must comply with. In addition, other MIBs should also be supported, such as MIB-II and the ENTITY MIB, which are common to all network entities.

MIB (Management Information Base) Files

This section describes the MIBs that are included with the MGC Manager. These MIBs define the various parameters that can be monitored, and their acceptable values. The MIBS are contained in files in the *SNMP Mibs* sub-directory of the MGC Manager root directory. The files should be loaded to the SNMP external system and compiled within that application. Only then can the SNMP external application perform the required monitoring tasks.

The MULTI-MEDIA_MIB_TC must be compiled before compiling the other MIBs.

Standard MIBS

- MULTI-MEDIA-MIB-TC (MULTIMTC.MIB) – defines a set of textual conventions used within the set of MultiMedia MIB modules.
- *H.320ENTITY-MIB (H320-ENT.MIB)* – is a collection of common objects, which can be used in an H.320 terminal, an H.320 MCU and an H.320/H.323 gateway. These objects are arranged in three groups: Capability, Call Status, and H.221 Statistics.
- *H.320MCU-MIB (H320-MCU.MIB)* – is used to identify managed objects for an H.320 MCU. It consists of four groups: System, Conference, Terminal, and Controls. The *Conference* group consists of the active conferences. The *Terminal* group is used to describe terminals in active MCU conferences. The *Controls* group enables remote management of the MCU.
- *H323MC-MIB (H323-MC.MIB)*– is used to identify objects defined for an H.323 Multipoint Controller. It consists of six groups: System, Configuration, Conference, Statistics, Controls and Notifications. The *Conference* group is used to identify the active conferences in the MCU. The *Notifications* group allows an MCU, if enabled, to inform a remote management client of its operational status.
- *MP-MIB (H323-MP.MIB)* – is used to identify objects defined for an H.323 Multipoint Processor, and consists of two groups: Configuration and Conference. The *Configuration* group is used to identify audio/video mix configuration counts. The *Conference* group describes the audio and video multi-processing operation.
- *MIB-II/RFC1213-MIB (RFC1213.MIB)* – holds basic network information and statistics about the following protocols: TCP, UDP, IP, ICMP and SNMP. In addition, it holds a table of interfaces that the Agent has. MIB-II also contains basic identification information for the system, such as, Product Name, Description, Location and Contact Person. For details of the MIB-II sections supported by the MGC Manager for PSOS and XP see “Support for MIB-II Sections” on page 5-43.
- *ENTITY-MIB (ENTITY.MIB)* – describes the unit physically: Number of slots, type of board in each slot, and number of ports in each slot.

Private MIBS

- *ACCORD-MIB (ACCORD.MIB)* – holds the product name.
- *MGC-MIB (MGC-MIB.MIB)* – provides the statuses of the MCU and

each hardware module, with a conduit to the ACCORD-MIB. This MIB is responsible for sending status traps indicating when the status of a component changes.

Support for MIB-II Sections

The following table details the MIB-II sections that are supported in PSOS and XP:

Table 5-10: Supported MIB-II Sections

Section	Object Identifier	Supported In
system	mib-2 1	PSOS and XP
interfaces	mib-2 2	PSOS and XP (only control unit interface card)
at	mib-2 3	PSOS only
ip	mib-2 4	PSOS only
icmp	mib-2 5	PSOS only
tcp	mib-2 6	PSOS only
udp	mib-2 7	PSOS only
egp	mib-2 8	not supported
cmot	mib-2 9	not supported
transmission	mib-2 10	not supported
snmp	mib-2 11	PSOS and XP

The MGC-MIB

The MGC-MIB contains a table displaying the updated status of the MCU and the status of each of the modules. A status trap is sent whenever the status of a module changes to MAJOR or MINOR.

The first line in the status table relates to the MCMS. The second line relates to the HDLC. The remaining lines relate to the cards. Each card is identified by a four digit number. The ENTITY MIB, which contains a description of each component, can be used to identify the slot to which the number relates.

The status table contains the following data for each component:

Table 5-11: MGC.MIB Status

Column Name	Content	Remarks
Index	A four digit integer	The index identifies the component and is taken from the ENTITY MIB at card level.
Status Time	M D, Y HH:MM:SS	The last time the component status changed.
Status	STARTUP NORMAL MINOR MAJOR	The trap will be set on MAJOR and MINOR.
Status Code	NORMAL/ or the code text (as written to the fault file)	During the startup the code will be set to STARTUP and then changed to NORMAL.
Status Description	NORMAL/ or the fault description (as written to the fault file)	Contains additional information such as the board and unit IDs.

Traps

Four types of traps are sent as follows:

1. Cold or warm start trap. This is a standard trap which is sent when the MCU is reset.

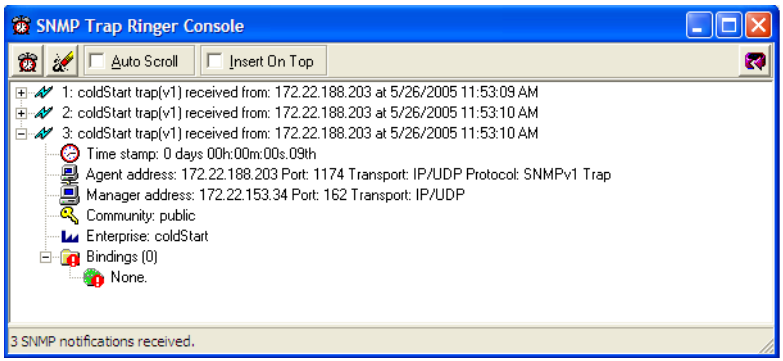


Figure 5-1: An Example of a Cold Start Trap

2. Authentication failure trap. This is a standard trap which is sent when an unauthorized community tries to enter.

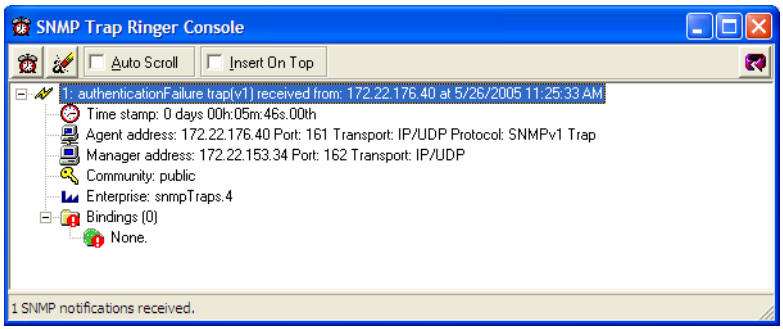


Figure 5-2: An Example of an Authentication Failure Trap

3. Configuration change trap. This is a private trap (trap number 11015) which is sent when there is a card or other system configuration change.

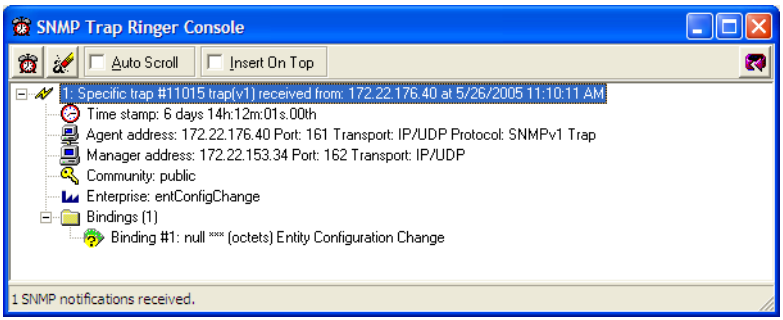


Figure 5-3: An Example of a Configuration Change Trap

4. Status trap. This is a private trap (trap number 11016) which is sent when a component fails, that is, when the status of a component changes to MAJOR or MINOR.

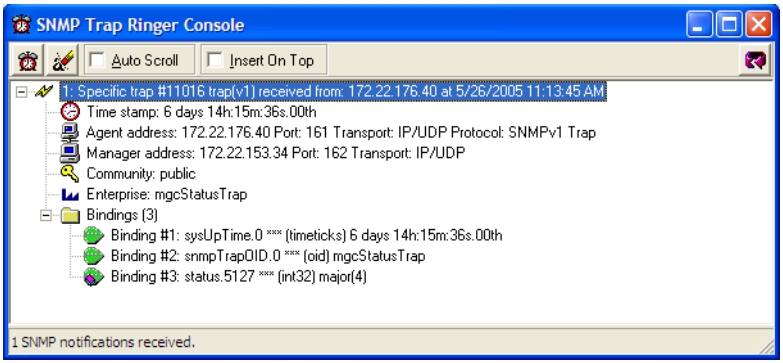


Figure 5-4: An Example of a Status Change Trap

Each trap is sent with a time stamp, the agent address and the manager address.

Status Traps

Status traps contain a number which can be used to identify the component that failed, but do not contain the full fault description. When you receive a status trap you can use the ENTITY MIB to identify the component to which the trap relates, and then look in the MGC MIB status table to find the status code.

Status Trap Content

The MCU can be set to send status traps only for specific statuses. The trap content can be set to:

- **NEVER** - A trap is never sent
- **MAJOR** - A trap is sent only when the card/MCU status is MAJOR
- **MINOR** - A trap is sent when the card/MCU status is MINOR or MAJOR

The default content is MINOR. The trap content is defined in the "system.cfg" file in the SNMP section.

Status Trap Timer

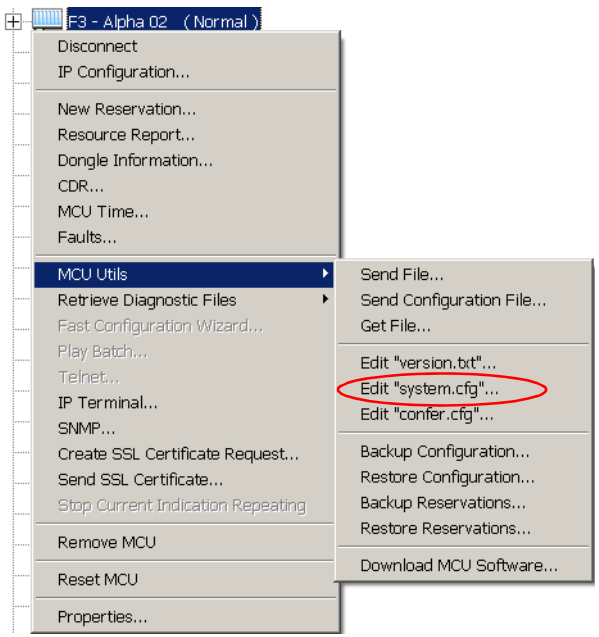
The MCU can be set to send the status trap according to a time interval. The default time interval for sending the trap is 60 seconds. The MCU will continue sending the trap as long as the status has not changed. Selecting a time interval of 0 will cause the trap to be sent only once. The time interval is defined in the "system.cfg" file in the SNMP section.

Enabling the SNMP Option and Configuring the Status Traps

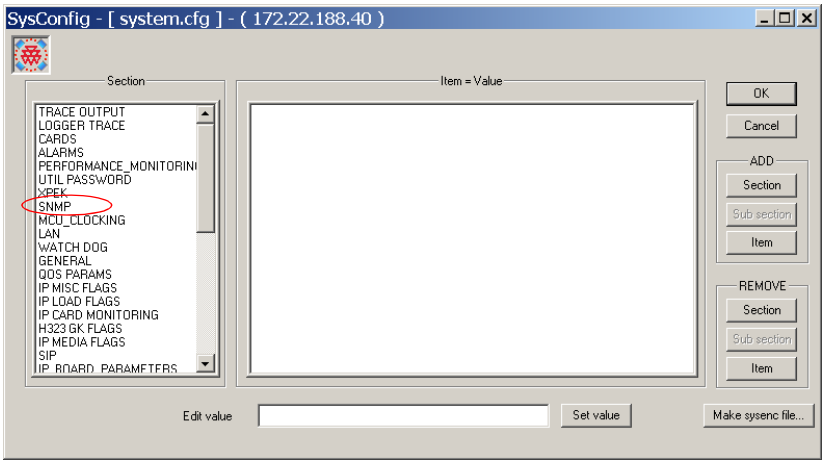
The SNMP option is enabled and the status traps are configured in the MCU "system.cfg" file.

To enable SNMP and configure the status traps:

1. Connect to an MCU.
2. Right-click the *MCU* icon, click **MCU Utils** and then click **Edit "system.cfg"**.

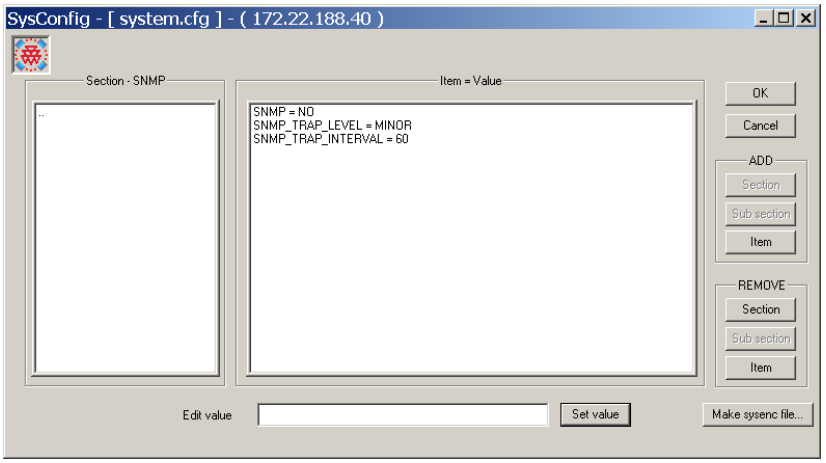


The *SysConfig* dialog box opens.



3. In the *Section* pane, double-click the **SNMP** option.

   The SNMP flags are displayed in the *Item = Value* pane.



4. Set the *SNMP* flag to **YES**.
   The SNMP option is enabled.
5. Set the *SNMP_TRAP_LEVEL* flag to **MAJOR**, **MINOR**, or **NEVER** as required.
6. Set the *SNMP_TRAP_INTERVAL* flag to a value between **0** and **100**.

7. Click **OK**.

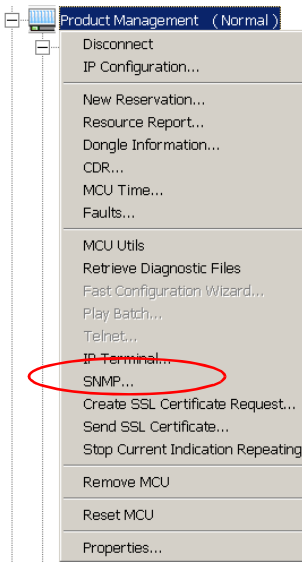
For more details on Flag modification in the “system.cfg”, see *“Edit “system.cfg”” on page 5-64*.

Defining the SNMP Parameters in the MGC Manager

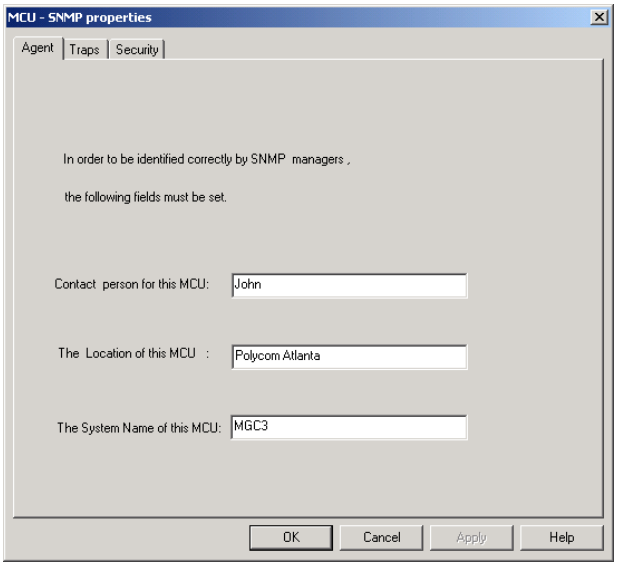
Managing or monitoring of the MCU by SNMP is done by **external** management systems such as HP OpenView or through web applications. These systems poll the MCU according to the MIB definitions. In addition, the MCU is able to send Traps to different managers. Traps are messages that are sent by the MCU to the SNMP Manager when an event such as MCU Reset occurs. The addresses of the Managers monitoring the MCU and other security information are defined in the MGC Manager application and are saved on the MCU’s hard disk. Only operators defined as a Superuser (Administrator) can define or modify the SNMP security parameters in the MGC Manager application.

To define or modify the SNMP parameters:

1. Connect to an MCU.
2. Right-click the *MCU* icon, and then click **SNMP**.



The *MCU-SNMP Properties – Agent* dialog box opens.



This dialog box is used to define the basic information for this MCU that will be used by the SNMP system to identify it.

3. Define the following information:

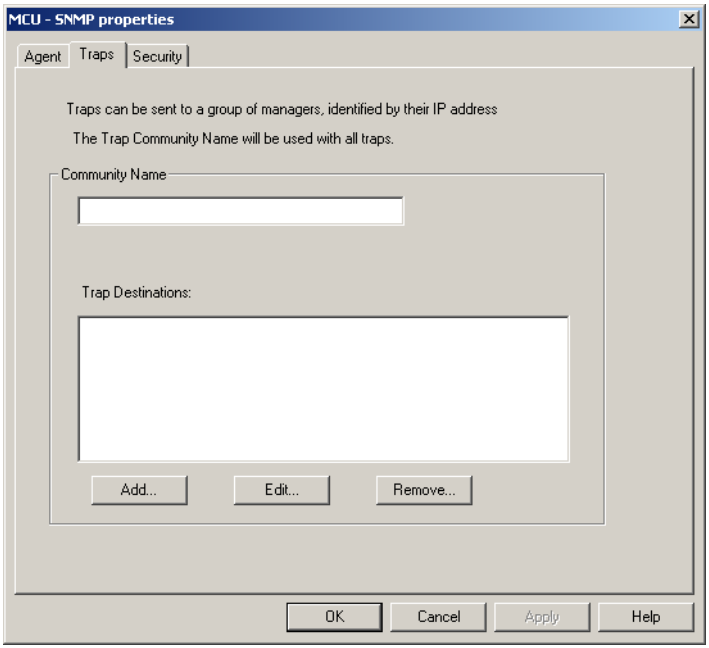
Table 5-12: SNMP Properties Options

Field	Description
Contact person for this MCU	Type the name of the person to be contacted in the event of problems with the MCU.
The Location of this MCU	Type the location of the MCU (address or any description).
The System Name of this MCU	Type the MCU's system name.

These details allow you to easily identify the MCU.

4. Click the **Traps** tab.

The *MCU-SNMP Properties – Traps* dialog box opens.



Traps are messages sent by the MCU to the SNMP Managers when events such as MCU Startup or Shutdown occur. Traps may be sent to several SNMP Managers whose IP addresses are specified in the *Trap Destinations* box.

5. Define the following parameters:

Table 5-13: SNMP Properties – Traps Options

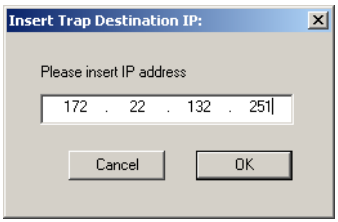
Field	Description
Community Name	Type a string of characters that will be added to the message that is sent to the external Manager terminals. This string is used to identify the message source by the external Manager terminals. **Note** – The Community Name must be defined identically in the external SNMP application.

Table 5-13: SNMP Properties – Traps Options (Continued)

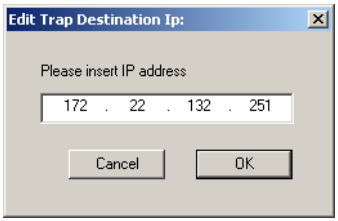
Field	Description
Trap Destination	This box lists the currently defined IP addresses of the Manager terminals to which the message (trap) is sent.

6. Click the **Add** button to add a new Manager terminal.

   The *Insert Trap Destination IP* dialog box opens.



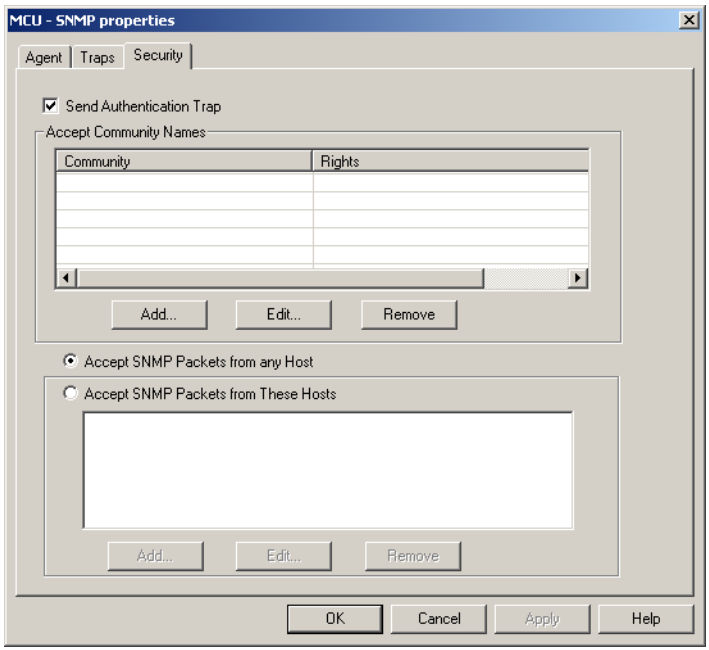
7. Type the IP address of the Manager terminal used to monitor the MCU activity, and then click **OK**.
   The new IP address is added to the *Trap Destinations* box.
8. To edit the IP Address of a Manager terminal:
   — Select the address that you wish to modify, and then click the **Edit** button.
   The *Edit Trap Destination IP* dialog box opens.



   — Edit the IP address, and then click **OK**.
   The IP address in the *Trap Destinations* box is modified.
9. To delete the IP Address of a Manager terminal:
   — Select the address that you wish to delete, and then click the **Remove** button.
   The IP address in the *Trap Destinations* box is removed.

10. Click the **Security** tab.

    The *MCU-SNMP Properties – Security* dialog box opens.



    This dialog box is used to define whether the query sent to the MCU is sent from an authorized source. A valid query must contain the appropriate community string and must be sent from one of the Manager terminals whose IP address is listed in this dialog box.

11. Define the following parameters:

Table 5-14: MCU-SNMP Properties – Security Options

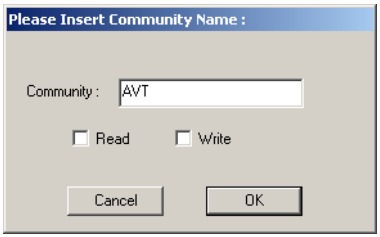
Field	Description
Send Authentication Trap	Select this check box to send a message to the SNMP Manager when an unauthorized query is sent to the MCU. When cleared, no indication will be sent to the SNMP Manager.

Table 5-14: MCU-SNMP Properties – Security Options (Continued)

Field	Description
Accept Community Names	This table lists the strings added to queries that have been sent from the SNMP Manager to indicate that they were sent from an authorized source. To define a new string, click the **Add** button (as described in the next step). **Note:** Queries sent with different strings will be regarded as a violation of security, and, if the *Send Authentication Trap* check box is selected, an appropriate message will be sent to the SNMP Manager.
Accept SNMP Packets from any Host	Select this option if a query sent from any Manager terminal is valid.
Accept SNMP Packets from These Hosts	Select this option to define an IP address of a specific Manager.

12. Click the **Add** button in the *Accept Community Names* box to add a new community string.

    The *Please Insert Community Name* dialog box opens.

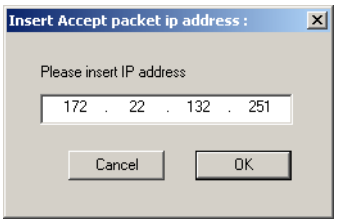


13. In the *Community* field, type the string that will appear in the message and will identify a valid query.

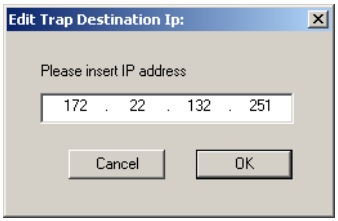
14. When working with the MCU, the external SNMP system can only monitor (Read) the MCU's activity, and is not allowed to modify any of its parameters, or cause the MCU to reset. Therefore, the queries sent to the MCU are only of a *Read* type, and not *Write*.
    Select the **Read** check box and then click **OK**.
    The details are displayed in the *Accept Community Names* table.
15. To edit a community string:
    — Select the entry to modify from the *Accept Community Names* box, and then click **Edit.**
    The *Please Edit Community Name* dialog box opens.

    — Modify the *Community* field and then click **OK**.
    The modified details are displayed in the *Accept Community Names* table.
16. To delete a community string:
    — Select the entry to delete from the *Accept Community Names* box, and then click **Remove**.
    The community string is removed from the *Accept Community Names* table.
17. To add, edit, or remove IP addresses of specific Manager terminals, click the **Accept SNMP Packets from These Hosts** option.
    The **Add**, **Edit** and **Remove** buttons are enabled.
18. To define the IP address of a specific Manager terminal, click the **Add** button.

The *Insert Accept Packet IP Address* dialog box opens.



19. Enter the *IP Address* of the Manager terminal from which valid queries may be sent to the MCU, and then click **OK**.
    The *IP Address* is displayed in the *Accept SNMP Packets from These Hosts* box.
20. To edit the IP address of a specific Manager terminal:
    — Select the relevant IP address, and then click the **Edit** button.
    The *Edit Trap Destination IP* dialog box opens.



    — Modify the *IP address*, and then click **OK**.
    The modified *IP address* is displayed in the *Accept SNMP Packets from These Hosts* box.
21. To delete a specific Manager terminal's IP address:
    — Select the IP address, and then click the **Remove** button.
    The IP address is removed from the *Accept SNMP Packets from These Hosts* box.

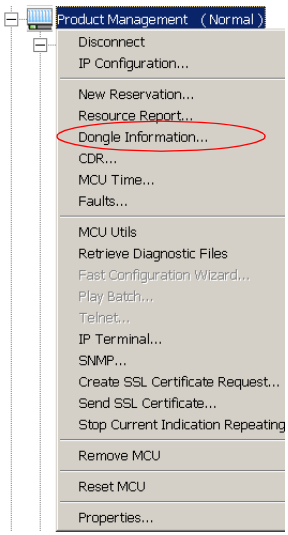
Queries sent from terminals not listed in the *Accept SNMP Packets from These Hosts* box are regarded as a violation of the MCU security, and if the *Send Authentication Trap* check box is selected, an appropriate message will be sent to all the terminals listed in the *SNMP Properties – Traps* dialog box.

22. In the *MCU - SNMP* properties dialog box, click **OK**.

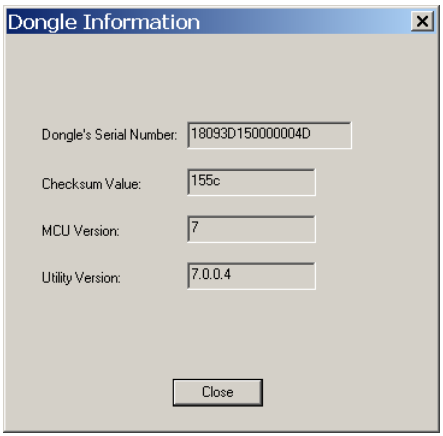
Dongle Information

Displays the information stored on the hardware key (dongle) attached to the rear panel of the MCU.

1. Right-click the *MCU* icon, and then click **Dongle Information**.



The *Dongle Information* dialog box is displayed.



This dialog box displays the dongle serial number and checksum and the software version installed in the MCU.

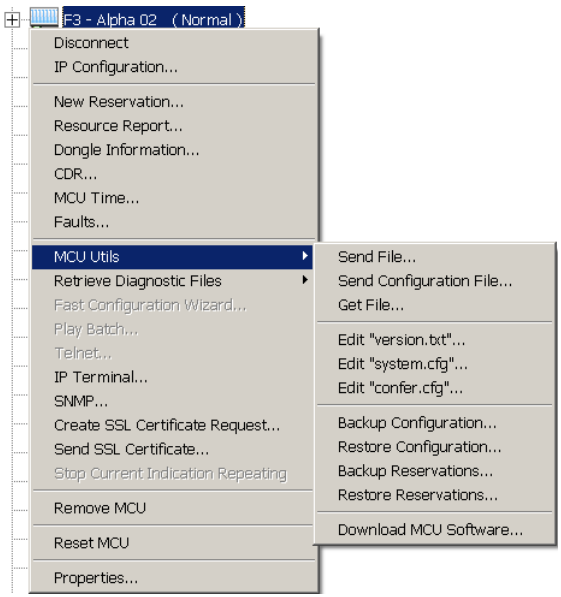
MCU Utilities

There are numerous MCU utilities that are used to manipulate files residing on the MCU's hard disk, back up and restore the system configuration and reservation data, and download software to the MCU. These utilities are:

- Send File
- Send Configuration File
- Get File
- Edit "version.txt"
- Edit "system.cfg"
- Edit "confer.cfg"
- Backup Configuration
- Restore Configuration
- Backup Reservations
- Restore Reservations
- Download MCU Software

To access the MCU Utilities:

- Right-click on the *MCU* icon, and then click **MCU Utils** to open its cascading menu.



After modifying one of the MCU files, the MCU must be reset for the modifications to take effect.

Send File

This utility downloads and installs software files as separate patches to the software installed on the MCU. The files that can be downloaded include:

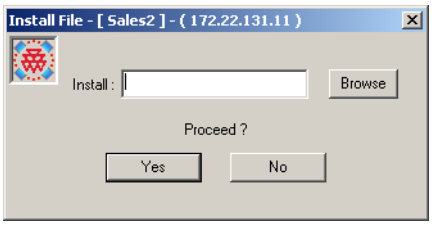
- Embedded system files
- system.cfg
- version.txt
- confer.cfg

In addition, it is used to download the audio and video files created for the Greet and Guide mode. These files are downloaded from the MGC Manager application to the MCU. Every patch/file must be downloaded separately.

To download a software patch or a file:

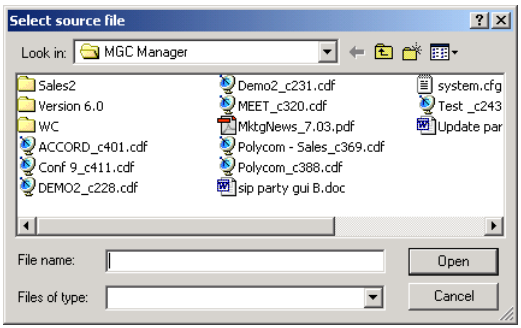
1. On the *MCU Utils* sub-menu, click **Send File**.

   The *Install File* dialog box opens.



2. In the *Install* text box, type the path and name of the file to be downloaded to the MCU, or click the **Browse** button to locate the file.

   If **Browse** is selected, the *Select Source File* dialog box opens.



   Select the desired software patch file, or if you are downloading audio and video files for the Greet and Guide mode, select an *.aca or *.acv file, and click the **Open** button.
   The system returns to the *Install file* dialog box, and the name of the file appears in the *Install* field.

3. Click **Yes** to download the file to the MCU or **No** to cancel the operation.

Send Configuration File

This utility is used for configuration updates to the dongle file. Contact Polycom support for additional information.

For a detailed description of the dongle upgrade procedure see the Release Notes of the relevant version.

Get File

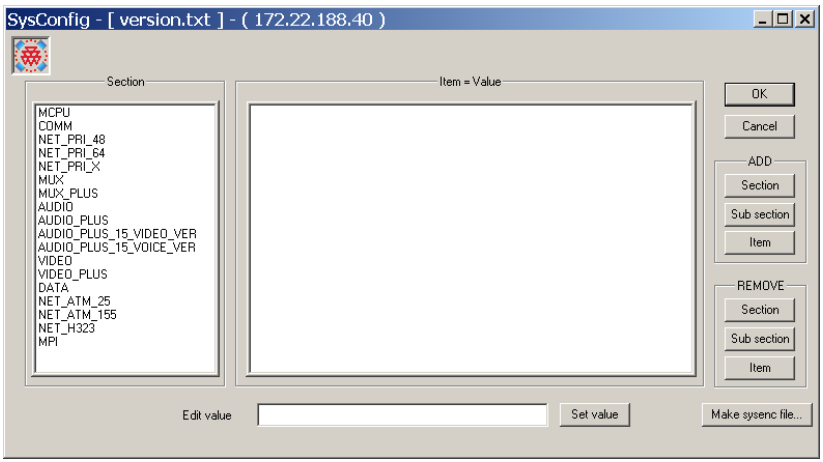
This utility is used to retrieve files from the MCU. This function is intended for Polycom's internal use.

Edit "version.txt"

The "version.txt" file contains a list of files that are to be used with each version of the card software. After installing a software patch, you may need to update the indicators in the "version.txt" file. You can also use this function to edit the values of the parameters that are found in the "version.txt" file.

To modify the version.txt file:

1. On the *MCU Utils* sub-menu, click **Edit "version.txt"**.
   The *SysConfig (version.txt)* dialog box opens.



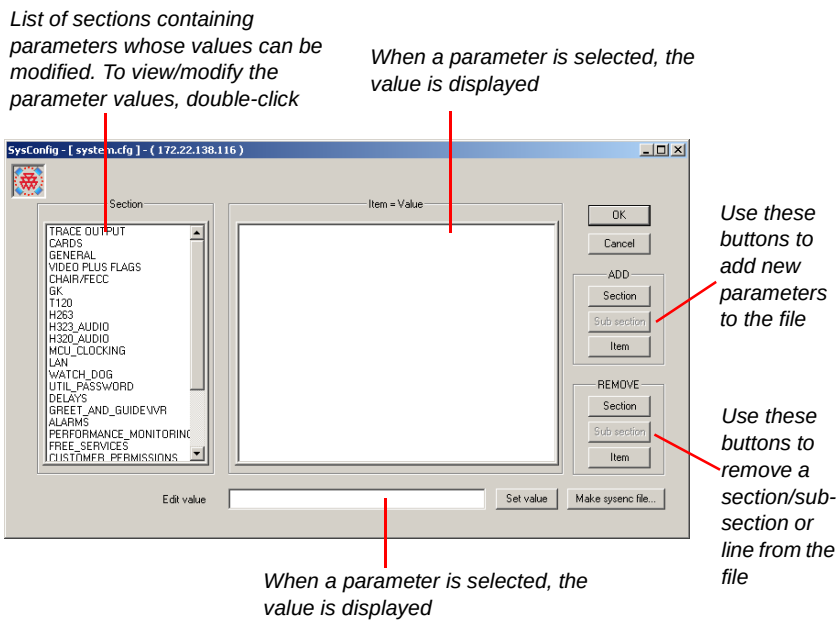
2. In the *Section* box, double-click the section you want to change.
   The available versions are displayed in the *Section* box.
3. Click the version you want to change.
   The parameter names and value are displayed in the *Item=Value* box.
4. In the *Item=Value* box, click the item whose value is to be modified.
   The item's value is placed in the *Edit value* text box.
5. In the *Edit value* text box, edit the value.
6. Click the **Set Value** button to apply the new value to the file.
7. Click **OK**.

Edit “system.cfg”

The “system.cfg” file is used to set up the system’s overall configuration and behavior and to change a configuration setting from its default value. To install the system.cfg file see “Send File” on page 5-60

To modify the “system.cfg” file:

1. On the *MCU Utils* sub-menu, click **Edit “system.cfg”**.
   The *SysConfig* dialog box appears.



2. In the *Section* box, double-click the section you want to change.
   The parameter names and value are displayed in the *Item=Value* box.
3. In the *Item=Value* box, click the item whose value is to be modified.

   The item’s value is placed in the *Edit value* text box.
4. In the *Edit value* text box, edit the value.
5. Click the **Set Value** button to apply the new value to the file.
6. Click **OK**.

System.cfg Flags

Only those flags which are intended for customer modification are documented here. Many system.cfg sections include flags with their default values as they are automatically set for the system. These flags have to be manually added to the relevant system.cfg file in order to modify the default system settings.

Section TRACE OUTPUT

The flags in this section must be manually added to the system.cfg file to modify their default values.

- PRINT = IP

  Defines the port to be used for Serial Traces.

  The flag may be set to one of the following values:

  — Console - Trace to the Console.
  — Serial_1 - on the back (Also of the MGC-25).
  — Serial_2 - front (Not applicable for the MGC-25).
  — IP

- TRACE = EXCEPTION

  Default Tracing level.

  This flag may be set to one of the following values:

  — NO- no trace
  — INTERACTIVE - level –I (accept input from terminal without dumping to trace)
  — EXCEPTION- level –e Asserts, memory exceptions
  — INTO_MCMS_TRACE - level –g (embedded to mcms information)
  — T120 - level –t GCC Trace
  — FULL - full information

Section LOGGER TRACE

The flags in this section must be manually added to the system.cfg file to modify their default values.

- TRACE_LOGGER_APPLICATION = YES

  Use this flag to enable (YES) or disable (NO) the Logger Utility.
- TRACE_LOGGER_LEVEL = FULL

  Indicates the detail level of messages to be saved to the Logger file. (INTO_MCMS, EXCEPTION, FULL)
- TRACE_LOGGER_MAX_FILE_SIZE = 640

  The maximum file size of the data file in kilobytes. When a file exceeds this size, the system closes the data file and opens a new data file.

The TRACE_LOGGER_MAX_FILE_SIZE and the TRACE_LOGGER_MAX_FILE_TIME_TO_LIVE flags limit the amount of information saved to one data file to facilitate the retrieval of information.

- TRACE_LOGGER_MAX_FILE_TIME_TO_LIVE = 600

  The period in minutes for which traces are saved to one file. At the end of this time period, the system closes the data file and opens a new data file for the following time period.
- TRACE_LOGGER_MAX_NUM_OF_FILE= 1000

  Defines a maximum on the number of files allocated to the system.

Section CARDS

- MAP_SELF_RECOVERY = YES

  Map Self Recovery is performed by the Card Manager processor resulting in changes in the Video+ unit. When the unit resets, the participants are not disconnected, and their video and audio are restored.

The following flags may be manually added to the [CARDS] section to modify their default values:

- CIRCULAR_MAPPING_MODE_FOR_AUDIO_VIDEO_PLUS = YES

  YES – Sets the MCU to circular mode. For Audio+ and Video+ cards the system allocates the next sequential unit that is free on the card.
  NO – Sets the MCU to terminal mode.
- CARD_STATUS_REQUEST = YES

  Sends a card status message to the cards and preforms a status check.

- RESET_UNIT = YES

  Reset Unit allows you to manually reset the IP card. This operation can be performed only when the unit is free and not occupied by participants.

The Main Control Module in the MGC unit contains a LAN network card that can be of different types. The Main Control Module operating system includes drivers for these cards. The Main Control Module's operating system automatically detects the card type by reading its identification in a predefined address. If the card is correctly identified, the system starts up correctly. If the system fails to detect any card type, it will start up according to the card type definition in the "system.cfg" file.

- RESET_CARD = YES

  When a card fails, an automatic reset of the card is initiated by the system.

- CARD_STARTUP_TIMEOUT = 420

  Defines the maximum time allowed for the card startup, after which the card's status is changed to 'NO_CONNECTION_WITH_CARD'.

- CARD_STATUS_REQUEST_TIMEOUT = 10

  Determines in seconds the frequency of sending a card status request.

- AUTO_VIDEO_PLUS_LOGGER = YES

  Set to YES to enable the Auto Video Plus logger. When a Video+ unit failure occurs, a VideoPlus log file is automatically created.

- AUTO_IP_CARD_MONITOR

  This flag may be set to one of the following options:

  — NO (no automatic monitoring - only manual monitoring is available)

  — UNIT (traces will be automatically saved for each unit failure)

  — CARD (traces will be automatically saved for each card failure)

  If Unit or Card are selected, a file containing the trace information for each failure will be created using the name format crdmn_nn.txt, where nn is a number between 00 and 19. The files are created sequentially, cyclically, when the 20th file overwrites the first file and so on. Recommended mode is NO (manual card monitor). For more information see *"IP Card Diagnostic Files" on page 5-121*.

- RTP_SELF_RECOVERY = YES

  Self Recovery is an automatic process performed by the Card Manager processor resulting in a reset of the H.323 card. When the card resets, the participants are not disconnected, and their video and audio are restored within 10 seconds.

Section ALARMS

The following flag may be manually added to the [ALARMS] section to modify their default values:

- EXT_ALARM=NO

  This flag enables the optional external alarm on the MCU. In case of an (Minor, Major) alarm on the system, a circuit activates the alarm on the MCU.

Section PERFORMANCE_MONITORING

The following flags may be manually added to the [PERFORMANCE_MONITORING] section to modify their default values:

- AUTO_PERFORMANCE_MONITORING=NO

  Enable the Automatic Performance Monitoring. Once the thresholds are for the various error conditions are exceeded, the system issues a fault message (in the *Faults* dialog box) and the MCU status changes from Normal to Minor). For more information see “Appendix C: Performance Monitoring NET-T1/Net-E1” on page C-1.

- PERFORMANCE_MONITORING_TIMEOUT=60

  The performance monitoring time-out.

Section UTIL PASSWORD

The following flags may be manually added to the [UTIL PASSWORD] section to modify their default values:

- PSOS_NET_UTIL = YES

  PSOS (OS) Utilities Tasks (Shell, FTP & Telnet), Can be used in case customer prefers to disable FTP & Telnet due to security issues. (Applicable only for pSos and not for XPEK.

- FTP_LOGIN = NO

  When set to YES, enables password verification for FTP Sessions, otherwise, a password is not required.

- IPTERMINAL_LOGIN = NO

  Enable Password for IP Terminal. In the IP Terminal type login then password (in the same command line).

- ALLOW_ORDINARY_OPERATOR_TO_CHANGE_ITS_OWN_PASSWORD = YES

  When set to YES enables the Operator with "ordinary permission" to change his own password. The Operator with "superuser permission" can change all operator's passwords.
  When the flag is set to NO, no operator will be able to change passwords, only delete and create new ones.

- STRONG_PASSWORD=NO

  Add this flag and set it to YES to enable the Strong Password mechanism.

Section XPEK

The following flags may be manually added to the [XPEK] section to modify their default values:

- CREATE_DUMP_FILE_WHEN_EXCEPT = YES

  Used for debugging purposes – start the debugger in case of exception.

- SILENT_MODE = YES

  Set this flag to YES (default) to increase MGC unit security. As a hacking preventive measure, the MCU is set to Silent Mode in order to ignore pings. For more information about Silent Mode, see *"XPEK Silent Mode" on page 5-38*.

Section SNMP

- SNMP = NO

  Enables SNMP for the MCU system.

- SNMP_TRAP_LEVEL = MINOR

  Define Trap level settings according to the type of severity: MAJOR, MINOR, NEVER. For more information about Traps see "Status Trap Content" on page 5-47.

- SNMP_TRAP_INTERVAL = 60

  Defines the interval in seconds between each trap. For more information about Trap Intervals, see *"Status Trap Timer" on page 5-47*.

Section MCU_CLOCKING

Defines the clock source type on the MCU, only one clock source per system is possible, when more than one clock source is defined, the ISDN clock is the default. Four types of clock sources can be implemented on MCU:

- ISDN_CLOCK = YES
- ATM_CLOCK = NO
- INTERNAL_CLOCK = NO
- MPI_CLOCK = NO

The following flag may be manually added to the [MCU_CLOCKING] section to modify their default values:

- SYSTEM_NORMAL_WITH_SINGLE_CLOCK_SOURCE = YES

  Set to this flag to YES allowing the MCU's status to be NORMAL, even if there is only a single clock source.

Section LAN

The following flags may be manually added to the [LAN] section to modify their default values:

- DRIVER_SMC = NO

  The controller auto detects the NIC card type, when a fault is detected the default (flag value = NO) is implemented: NO = SMC Driver, YES = 3COM or Intel Driver.

Section WATCH DOG

The following flags may be manually added to the [WATCH DOG] section to modify their default values:

- WATCH_DOG=YES

  Enables an automatic MCU reset when the MCMS crashes.

Section GENERAL

- PRODUCT_TYPE = 100

  Defines the type of MCU used as a system, the default being set to the MGC-100. Selection of three types is possible: MGC-100 (= 100), MGC-50 (= 50) and MGC-25 (= 25).

- CONFERENCE_ID_MCU_LENGTH = 4

  Defines the number of digits in the Conference Numeric ID that will be assigned by the MCU. Possible values are 1 to 16 digits. Enter 0 to

disable the automatic assignment of numeric IDs by the MCU and let the Operator manually assign them.

- CONFERENCE_ID_USER_LENGTH = 4

  Defines the number of digits that the Operator must enter when manually assigning the Numeric ID to the conference. Possible values are 1 to16 digits. Enter 0 to disable checking of the Numeric ID length.

- RESERVATION_CONFERENCE_ID_UNIQUE = YES

  If set to NO - duplicate NIDs are allowed in reservations. In this case, it's the administrator's responsibility to make sure there is no overlapping reservations with same NID planned for the same time.

- PREFERRED_PORT = 80

  80 - Any port can be used and is the preferred port with XML
  5001 or 1205 - the http port not activated and uses the proprietary API.

- SECURED_PORT_MANDATORY_FOR_API = NO

  When set to YES, API connection is only allowed via SSL secured connection.

- SECURED_PORT_MANDATORY_FOR FILE = NO

  When set to YES, file transfer is only allowed via SSL/TLS secured connection.

- TRADITIONAL_END_POINTS_MODE = YES

  When set to YES, enables support for old endpoints like Swiftsite.

- IGNORE_AIM = YES

  When set to YES, enables the participant to use an external telephone, while the endpoint's audio channel is muted, however, the participant's audio channel status is indicated by the "Mute by Endpoint" icon in the MGC Manager *Monitor* and *Status* panes. Also, when the participant is muted from the endpoint, the participant can use an external telephone to connect to the conference while the endpoint's audio channel is muted.

- MAX_PARTIES_NUMBER_IN_VIDEO_CONF = 100

  The maximum number of participants that can access an video conference. Up to 680 participants are allowed in a video conference, however this requires 128MB of RAM on the control unit.

The following flags may be manually added to the [GENERAL] section to modify their default values:

- CDR = YES

  When set to NO, disables the use of the CDR on the system.

- H0 = NO

  When set to YES, enables H0 network connectivity.

- HIGH_BIT_RATE = YES

  Setting the High Bit Rate flag to YES enables Continuous Presence and Transcoding conferences to be run at up to 1920 Kbps on the standard Video cards. This option should be selected only if all the video cards are of the new version. If the High Bit Rate flag is set to YES and the MCU contains video cards of a version older than 1.43, the MCU's status changes to Major and an appropriate error message is added to the Faults log. If the High bit rate Flag is set to NO, the highest line rate that can be set for the conference is 768 Kbps. The video card that does not support the High Bit Rate is pulled out from the available resources list and it is not used to run conferences.

- HIGH_VIDEO_FRAME_RATE = YES

  If set to YES, the flag enables high Video quality (30 frames per second) for high Line Rates of up to T1/E1 in Transcoding and Continuous Presence conferences.

  If the High Video Frame Rate flag in the system.cfg is set to YES, and the MCU contains video cards of a version older than 1.43, the MCU status changes to Major and an appropriate error message is added to the Faults log. The video card that does not support the High Frame Rate is pulled out from the available resources list and it is not used to run conferences.

- BONDING_DOWNSPEED = YES

  This option enables the bonding of channels.

- MAX_PARTIES_NUMBER_IN_AUDIO_CONF = 860

  The maximum number of participants (default - 860) that can access an *Audio Only* conference.

- PREFERRED_SECURED_PORT = 443

  When mandatory security is enabled from the MGC manager, on first connection after the reset, MCU will automatically use only the preferred TLS/SSL-secured port 443, and the HTTPS protocol./

- AUTO_LAYOUT = YES

  When set to NO, disables the usage of the Auto Layout feature.

- ENABLE_DTMF_VIA_GW = YES

  Enables/disables DTMF Forwarding (user to user) in a gateway sessions.

- ENABLE_LECTURE_SHOW = NO

  When set to YES, enables the Lecture Show feature.

- ALLOW_VIDEO_MUTE=NO

  To disable the Video Mute functionality so that users cannot stop the video channel transmission to the conference.

- NUM_OF_DIGITS_IN_GW_PROFILE=1

  Enter this flag to change the default setting for the number of digits that comprise the GW Profile ID from one to two digits.

Section QOS PARAMS

- DIFF_SERV_AUDIO = 0X88

  The diffserv value for audio packets.

- DIFF_SERV_VIDEO = 0X88

  The diffserv value for video packets.

Section IP MISC FLAGS

- PARTY_MONITORING_REFRESH_PERIOD= 2

  The party monitoring is a request that the MCMS sends to the IP card. This flag helps to determine the load of those request by identifying the number of seconds between each party monitoring request.

- IP_ENABLE_ROUNDTRIPDELAY = YES

  When an endpoint disconnects from the conference, the MCU perceives the endpoint to be connected but not responding. To disconnect the endpoint the MCU sends a Round Trip Delay request to the endpoint. If the endpoint fails to respond, it is disconnected from the MCU.

- IGNORE_STREAM_VIOLATION = NO

  Normally when RTP encounters severe problems in the media streams, it sends STREAM_STATUS_IND to mcms, and as a result mcms moves the sender into Secondary. If this is done in the Nortel environment the agent always be secondary because it always sends overflow. This flag is used to ignore this indication from the card for any state of the call except change mode.

- IGNORE_STREAM_VIOLATION_IN_CHANGE_MODE = NO

  Normally when RTP encounters severe problems in the media streams, it sends STREAM_STATUS_IND to mcms, and as a result mcms moves the sender into Secondary. If this is done in the Nortel environment the agent always be secondary because it always sends overflow. This flag is used to ignore this indication from the card for change mode.

The following flags may be manually added to the [IP MISC FLAGS] section to modify their default values:

- CASCADE_TO_PREVIOUS_VERSION = 0

  When set to 0 you are not able to Cascade conferences with previous MCU software versions. Set to the version number (or earlier) to which cascading is to be enabled.

- CP_REGARD_TO_INCOMING_SETUP_RATE = YES

  When set to YES in a Continuous Presence mode, the MCU checks the Bandwidth requested by the endpoint, if the participant is not connected (only when the participant has capabilities of the defined conference rate).

- SOFTWARE_CP = YES

  This option enables Software Continuous Presence conferences.

- THRESHOLD_BITRATE=100

  Determines the acceptable deviation, in percentage, from the expected channel bitrate as declared and negotiated between the MCU and the endpoint (in the H.245 channel). The threshold is defined in fractions of 1000, therefore, a threshold of 100 defines 10%. Entering zero for a flag disables the flag.

- THRESHOLD_FRACTION_LOSS=5

  Determines the acceptable percentage of the channel Fraction Loss (as it appears in the Channel Status box). The threshold is defined in fractions of 1000, therefore, a threshold of 100 defines 10%. Entering zero disables the flag.

- THRESHOLD_ACCUMULATE_PACKET_LOSS=5

  Determines the acceptable percentage of packets lost since the channel has opened, beyond which the channel quality may be compromised. The threshold is defined in fractions of 1000, therefore, a threshold of 100 defines 10%. Entering zero disables the flag.

- THRESHOLD_INTERVAL_PACKET_LOSS=5

  Determines the percentage of packets that were lost in the last RTP report interval, beyond which the channel quality may be compromised. The threshold is defined in fractions of 1000, therefore, a threshold of 100 defines 10%. Entering zero disables the flag.

- THRESHOLD_ACCUMULATE_OUT_OF_ORDER=5

  Determines the acceptable percentage of packets that arrived out of order since the channel has opened. The threshold is defined in fractions of 1000, therefore, a threshold of 100 defines 10%. Entering zero disables the flag.

- THRESHOLD_INTERVAL_OUT_OF_ORDER =5

  Determines the acceptable percentage of packets that arrived out of order in the last RTP report interval. The threshold is defined in fractions of 1000, therefore, a threshold of 100 defines 10%. Entering zero disables the flag.

- THRESHOLD_ACCUMULATE_FRAGMENTED=5

  Determines the percentage of packets that were fragmented since the channel has opened.

- THRESHOLD_INTERVAL_FRAGMENTED=5

  Determines the percentage of packets that were fragmented in the last RTP report interval. The threshold is defined in fractions of 1000, therefore, a threshold of 100 defines 10%. Entering zero disables the flag.

- THRESHOLD_JITTER=80

  Determines the maximum delay in milliseconds in the expected arrival time (buffer size). The threshold is defined in fractions of 1000, therefore, a threshold of 100 defines 10%. Entering zero disables the flag.

- THRESHOLD_LATENCY=300

  Determines the maximum time it takes a packet to travel from one end to another. The threshold is defined in fractions of 1000, therefore, a threshold of 100 defines 10%. Entering zero disables the flag.

- THRESHOLD_FRAME_RATE=0

  Determines the acceptable deviation, in percentage, from the expected channel frame rate. The threshold is defined in fractions of 1000, therefore, a threshold of 100 defines 10%. Entering zero disables the flag.

- DEFENCE_PERCENT = 95

  Indicates to end point the percentage to send us of the actual bit rate to protect the MCU from bursty end point. 100% means that we are not protecting MGC from bursty end point. The value can be any value 100% or less. Usually 95% is sufficient.

- ACTIVE_PROTECTION_NUMBERING=YES

  YES - Ignores duplicate messages
  NO - Does not ignores duplicate messages

Section IP LOAD FLAGS

The following flag may be manually added to the [IP LOAD FLAGS] section to modify its default value:

- SIP_REGISTER_LOAD = 80

  The amount of resources the process consumes. Measured in 0.1%. Possible values are 1 to 1000.

Section IP CARD MONITORING

- IP_MONITORING_SHOW_FAULTY_MARK = YES
  YES - Show participant monitoring section with a red fault ('!') indication in MGC manager
  NO - don't show any participant indication

Section H323 GK FLAGS

- RRQ_WITHOUT_GRQ = NO

  Must be set to NO for the register as a gateway feature to function properly.
  YES – Registration start with RRQ (Registration Request).
  NO – Registration start with GRQ – Gatekeepers Request)
- H323_ENABLE_CONFERENCE_DIALIN_IDENTIFY = NO

  Set the flag to YES to enable the enhanced cascading mode in which Aliases (conference name and participant name) may be used for H.323 cascading conferences.

  Set it also to YES to enable the RSS 2000 video recording.
- ENABLE_ALT_GK = YES
  YES - Enables use of the alternate gatekeeper when the primary gatekeeper fails.
  NO - Disables use of the alternate gatekeeper.

The following flags may be manually added to the [H323 GK FLAGS] section to modify their default values:

- GATEWAY_DESTINATION_SERVER=YES

  To enable multiple ISDN video endpoints calls over the same MGC gateway to reach the same IP destination.
- PREFIX_TYPE_IS_H323ID = NO

  Enables the Prefix type (for most of GK, it is E.164).When using ECS Gate Keepers need to be set to YES
  YES – H320_GW
  NO – H323_GW
- ARQ_WHEN_CALL_IS_WITH_IP = YES

  When a card is registered with a Gatekeeper, and the participant has a IP address (not alias), an ARQ message is sent to the Gatekeeper.

- MCU_REG_AS_320_GW = YES

  When working in register as GW mode two options are available, H320_GW (YES), or H323_GW (NO). When working with CISCO MCM it is require to register as H320_GW (YES)

- PATH_NAVIGATOR_OLD_VERSION_IN_ROUTED_MODE = NO

  When set to YES the MCU does remove People+Content or Duo Video.

- REMOVE_G722_AND_GENERIC_AUDIO = NO

  If set to YES a VOIP phone cannot always establish a connection when using PathNavigator as the Gatekeeper.

Section IP MEDIA FLAGS

- IP_ENABLE_BACKGROUND_COLOR = NO

  Set to YES, when using *Background Colors* in a *Continuous Presence* Video conference.

The following flags may be manually added to the [IP MEDIA FLAGS] section to modify their default value:

- IP_AUDIO_CONCEALMENT = NO

  Because of RTP demand this flag is used to set the G711 to 30 FPP.

- SIP_G711_FPP = 30

  Enables you change the frame per packet of audio algorithm G.711.

- SIP_G7231_FPP = 30

  Enables you change the frame per packet of audio algorithm G.723.1.

- ENABLE_IP_SLIDE = YES

  When set to YES, H.323 participants can view the video Welcome slide when connecting to an IVR-enabled conference. SIP participants cannot view the Welcome slide.

- IP_PACKETS_FRACTION_LOST = NO

  For future development.

- H323_INTERLACE_MODE = YES

  When set to YES, enables Pro-Motion in H.323.

- RFC2833_DTMF = YES

  YES - Enables the use of RFC2833.
  NO - Disables the use of RFC2833.

Section SIP

- SIP_ENABLE_264_FIXED = NO

  In VSW 264 resolution in SIP environment that doesn't support highest common this flag should be NO.

The following flags may be manually added to the [SIP] section to modify their default value:

- SIP_REINVITE = YES

  YES - Only send one algorithm for each media, 1 for audio and 1 for video is sent.
  NO - All the mcu capabilities for each media is sent.

- SIP_FAST_UPDATE_INTERVAL = 0

  0 = Disables the MCMS fast update requests.
  If not 0 = The interval in seconds between two fast update requests. If the endpoint does not request one, the MCMS initiates a request instead of the endpoint and sends it to the video card.

- SIP_MSG_TIMEOUT = 120

  The value can be 120 and above (120 is the minimum). This value is the time (in seconds) that the MCU will wait for a SIP message before the timer deactivates.

- SIP_USER_AGENT_FPS_FIX =

  UserAgent header contains the string. Possible values: all valid characters.
  1 disables the flag.

- SIP_FPS_FIX_TO =

  New value to set. Possible values: 30, 15, 7.5
  1 disables the flag.

If the system.cfg flags: SIP_FPS_FIX_TO and SIP_USER_AGENT_FPS_FIX=NO are defined in the system.cfg file, adjustments are performed on all remote participants in CP conferences.
Define which User Agents (SIP endpoints using a header in SIP messages) use a fixed frame per second value with CIF resolution.
SIP_USER_AGENT_FPS_FIX = [string]; UserAgent header contains the following string SIP_FPS_FIX_TO = [int]; New value to set
For example:
SIP_USER_AGENT_FPS_FIX = “RTC”
SIP_FPS_FIX_TO = “15”
The Fixed FPS value is set to 15 for all SIP participants with “RTC” character set in User Agent field (or downgraded to 15 FPS for all Windows Messenger users in CIF).
The system.cfg flag SIP_USER_AGENT_FPS_FIX is relevant only if the flags: SIP_FPS_FIX_TO and SIP_FPS_FIX_TO = 0 are present in the system.cfg file.

- SIP_RESET_CHANNEL_ON_HOLD = 0

  1 (for Nortel): When getting HOLD from remote, mcms sends UPDATE_CHANNEL in order to nullify the SSRC and SEQ.
- SIP_USER_AGENT_FLOW_CONTROL =

  YES (For Nortel), Offer signaling DTMF in SDP.
- SIP_USER_AGENT_FLOW_CONTROL_RATE = 64,128,192,256,384,512,768

  Describe spare buffers for overflow from remote (for Nortel “8,64,128,256,384,512,768 “).
- SIP_LUCENT_CDR = NO

  YES = In dial out the special private headers for Lucent CDR are added. The default for Lucent is YES.
- SIP_CONF_WATCH_CONTROL=NO

  Set to YES to enable the SIP-CX environment for the MCU.
- AD_HOC_PROFILE_ MSFT=

  Enter the name of the Profile (Profile name must be written in CAPS) that will be used for conference definition, hence setting the Entry Queue to which it is assigned as Microsoft enabled. For example, if the flag is

set to AD_HOC_PROFILE_ MSFT=OCMR, the conference parameters will be taken from the Profile named OCMR.

- MSFT_IP_SERVICE_NAME_PREFIX=*IP network service name*

  To designate a SIP-CX enabled IP Network Service enter the flag with the prefix of the IP network service name. For example, if you enter the prefix MICROSOFT as follows: MSFT_IP_SERVICE_NAME_PREFIX=MICROSOFT, the IP Network service whose name starts with MICROSOFT (MICROSOFT1, MICROSOFT2, etc.) will be considered by the system as SIP-CX enabled.

Section IP_BOARD_PARAMETERS

- JITTER_BUF_SIZE = 2

  The size of the minimum Jitter Buffer in 10 msec increments.

  The possible values are 2-8 (20-80msecs).

- SIP_VIDEO_DRAFT = 5

  The SIP Video draft version. '5' is the newer one. (3 for Nortel Environment)

- SIP_CAP_DTMF_BY_INFO = NO

  If YES, offer signaling DTMF in SDP.

The following flags may be manually added to the [IP BOARD PARAMETERS] section to modify their default value:

- H245_TUNNELING = NO

  Enables H.245 tunneling.

- SIP_NORTEL = NO

  This flag enables/disables specific changes done for the Nortel environment. (YES for Nortel Environment)

- FILTER_MEDIA_BY_IP = YES

  If set to YES, we drop packets that don't come from the address specified when the channel was opened. For Cisco this flag should be set to NO.

Section IP_3G_FLAGS

The following flags may be manually added to the [IP_3G_ FLAGS] section to modify their default value:

- ENABLE_H323_PSTN = NO

  YES - Enable Ericsson 3G support
  NO - Disable Ericsson 3G support

- USE_ISDN_NUMBER_FOR_H323_DIALING = NO

  YES - Uses an ISDN number for H.323 dialing.
  NO - An ISDN number is not used for H.323 dialing.

- H323_MOBILE_PHONE_RATE = 0

  Available values 0 - 128.
  52 is for Ericsson only.

- SEARCH_FOR_H323_DEFINED_PARTY = YES

  YES - Enables an MCU search for define participant.
  NO - The MCU does not search for defined participant.

Section IP_AUDIO

- G729 = NO

  When set to YES, enables G729 audio algorithm.

The following flags may be manually added to the [IP_AUDIO] section to modify their default value:

- G722 = YES

  When set to YES, enables G.722 in H.323.

- G728 = YES

  When set to YES, enables G.728 in H.323.

- G7231 = YES

  When set to YES, enables G.723.1 in H.323. Requires Audio card *H/W Version 4.0* or higher, or the *Audio+* card.

- G722_1 = YES

  When set to YES, enables G.722.1 in H.323. Requires Audio card *H/W Version 4.0* or higher, or the *Audio+* card.

- SIREN7 = YES

  When set to YES, enables SIREN7 in H.323.

- SIREN14 = NO

  When set to YES, enables SIREN14 in H.323.

Two flags from the AUDIO PLUS FLAGS section must be set as follows: PDC_MODE=YES and AUDIO_PLUS_FREQUENCY=WB.

Section H320_AUDIO

- SIREN14_320 = NO

  When set to YES, enables SIREN14 in H.320. Requires the *Audio+* card.

The following flags may be manually added to the [H320_AUDIO]section to modify their default value:

- G722_1_320 = YES

  When set to YES, enables G.722.1 in H.320. Requires Audio card *H/W Version 4.0* or higher, or the *Audio+* card.

- H320_G722 = YES

  When set to YES, enables G.722 in H.320. Requires Audio card *H/W Version 4.0* or higher, or the *Audio+* card.

- SIREN7_320 = YES

  When set to YES, enables SIREN14 in H.320. Requires Audio card *H/W Version 4.0* or higher, or the *Audio+* card.

Section H263

- IP_H263 = YES

  Set to YES to enable H.263 video format in H.323 call.

- H263 = YES

  Set to YES to enable H.263 video format in H.320 call.

The following flags may be manually added to the [H323]section to modify their default value:

- GW_H263 = YES

  Set to YES to enable H.263 video format in Gateway calls.

- H263_ANNEX_F = YES

  Set to YES to enable H263 Annex F.

- H263_ANNEX_N = YES

  Set to YES to enable H263 Annex N.

- H263_ANNEX_P = YES

  Set to YES to enable H263 Annex P.

- H263_ANNEX_L = NO

  Set to YES to enable Annex L in 60 FIELDS (NTSC).

- H263_VGA_SVGA_XGA_NTSC = YES

  Set to YES to enable custom video formats with H.263 video format.

- H263_4CIF = YES

  Set to YES to enable 4CIF.

- H263_16CIF = YES

  Set to YES to enable 16CIF.

- H320_VIDEOSWITCHING_VIDEOPROTOCOL_SELECTION_AUTOMODE_H263 = YES

  When using H.263, H.320 is automatically selected for a video connection.

- IP_VIDEOSWITCHING_VIDEOPROTOCOL_SELECTION_AUTOMODE_H263 = YES

  When using H.263, H.323 is automatically selected for a video connection.

- PROMOTION_FIELD_DROP = YES

  Polycom proprietary Pro-Motion capability, which improves the video quality of fast-motion video, especially when using the 384 Kbps line rate.

  When set to YES, the encoder reverts momentarily to 30 frames/sec. video when detecting fast frame movements (a lot of changes between consecutive frames).

- LIMIT_AUTO_VSW_H263_FORMAT = NO

  Set to YES to prevent the opening of H263 4CIF and higher resolution in Highest Common conferences.

  When set at NO, no limits are placed on H.263 resolution in highest common mode.

- DBC_2=YES

  Set to No to disable DBC-2 that provides error concealment and recovery for multipoint VSW and CP conferences and gateway calls.

Section CHAIR/FECC

- FECC_GW = YES

  YES - Enables FECC capabilities in all gateway calls.
  NO - Disables FECC capabilities in all gateway calls.

The following flags may be manually added to the [CHAIR/FECC] section to modify their default value:

- FECC = YES

  YES - Enables FECC conferencing.
  NO - Disables FECC conferencing.

- WAIT_FOR_CHAIR_VIDEO_TYPE_NEW = 1

  When a conference is set to wait for the chairperson and participants connect to the conference before the chairperson, the participants are placed on hold until the chairperson joins the conference.
  1 - While on hold the participants can view each other and their audio is muted.
  0 - While on hold the participants view the Welcome slide and hear background music.

- ENABLE_FECC_EQ=YES

  Set to NO to disable FECC support in Entry Queues.

Section T120

The following flags may be manually added to the [T120]section to modify their default value:

- T120 = YES

  When enabled, activates T.120 for ISDN participants.

- H323_T120 = YES

  When enabled, activates T.120 for IP.

Section FREE SERVICES

The following flag may be manually added to the [FREE SERVICES] section to modify its default value:

- FREE_SERVICES = NO

  Enables Net Service Hunting (H.320) in case the first Net Service over-exceeds its maximum capacity.

Section CUSTOMER_PERMISSIONS

The Customer Permissions section defines feature availability according to customer purchase and is not accessible to the user.

Section DELAYS

The following flags may be manually added to the [DELAYS] section to modify their default value:

- DELAY_BETWEEN_DIAL-OUT_PARTY = 1

  To define the delay between dial-out participants for automatic dial-out to a large number of participants when routers and switches cannot handle the instant traffic load. The delay between participants is specified in seconds, and the system default is set to one second.

- CHANNEL_DELAY = 2

  Channel Delay in H221 calls in .01 seconds.

- BONDING_CHANNEL_DELAY = 0

  Fine tuning the Bonding process with correlation with downspeeding.

- BONDING_6_CHANNELS_DELAY = AUTO

  Fine tuning the Bonding process with correlation with downspeeding.

- BONDING_REDIAL_DELAY = 0

  Fine tuning the Bonding process with correlation with downspeeding.

- DELAY_BETWEEN_DIAL-OUT_AUDIO_PARTY = 25

  To define the delay between dial-out participants for automatic dial-out to a large number of audio participants when routers and switches cannot handle the instant traffic load. The delay between audio only participants is specified in seconds, and the system default is set to twenty-five seconds.

- MUX_BOND_REDUCED_LATENCY = YES

  Decreases system latency by enabling the MUX and the Bonding processes to be conducted on the MUX card.

- ENABLE_IP_REDIAL = NO
  YES - Enables re-dialing when H.323/SIP dialout calls fail.
  NO - Disables H.323 re-dialling.

  ALWAYS - extends the automatic re-dialing to the ongoing conference.

- NET_PSTN_DELAY = 0

  Delay in hsync (10ms) before the 1st command.

- NET_PSTN_DELAY2 = 0

  Delay in hsync (10ms) before the 2nd command

- NET_PSTN_DELAY3 = 0

  Delay in hsync (10ms) before the 3rd command

- NET_PSTN_CMD_ORDER = 0

  1 - the old order (alert, connect, TS)
  0 - new order (TS, alert, connect)

Section GREET_AND_GUIDE\IVR

- MESSAGE = YES

  Set to YES, to enable the Message I/O daughter card. For more information see, the MGC Hardware & Installation Manual, Greet & Guide Hardware Kit.

- MUSIC = NO

  Set to YES, to enable the Music I/O card. For more information see, the MGC Hardware & Installation Manual, Input/Output Cards.

- DTMF_FORWARDING = YES

  Set to YES to enable a roll over feature where DTMF codes are forwarded between one conference to another.

- DEFAULT_PASSWORD_LENGTH = 6

  Value for the default password setting. Valid values 1-16.

- MAX_PASSWORD_LENGTH = 16

  The MCU does not accept reservations with passwords longer than the above value (through API or DTMF). Valid values 1-16.

- MIN_PASSWORD_LENGTH = 4

  The MCU does not accept reservations with passwords shorter than the above value (through API or DTMF). Valid values 1-16.

- QUICK_LOG_IN_VIA_ENTRY_QUEUE = NO

  Enables the Chairperson to enter only the chairperson password as both conference and chairperson passwords (provided the appropriate option is also configured in the IVR Service).

- VISUAL_NAME_CONVENTION = 0

  0 - The participants visual name is not changed.
  1 - The participants visual name is changed and has counter (n+1), for example Dan 001, Dan 002.

- AUTOMATIC_ALLOCATION_OF_CONFERENCE_CHAIR_PASSWORD = YES

  YES = The conference password and chairperson password are allocated by the system when the field is left blank
  NO = Conference password and chair person password are not allocated by the system when the field is left blank.

- ROLL_CALL_CONFIRMATION = NO

  Set to NO to not play the Roll Call Confirm Record message to participants.

- EVENT_ICON_TEXT=2

  Defines the type of visual indication:

  0 - Text only, no icon

  1 - Icon only, no text

  2 - Text & icon (system default)

  Note: If 1 (Icon, No Text) is selected, the End of Conference icon is displayed twice: x minutes before the conference is about to end (where x is defined in the Conference Settings) and one minute before conference end.

- TEXT_EVENT_MEDIA=2

  Defines the use of audio and/or visual indications:

  0 - Audio indication only

  1 - Visual indication only

  2 - Audio & visual indication (system default)

The following flags may be manually added to the [GREET_AND_GUIDE\IVR] section to modify their default value:

- LEADER_WAITING_TIME_OUT = 20

  The amount of time that the system waits for the chairperson to join the conference. If the chairperson does not join the conference within the predefined time, the conference is terminated (applies only to conferences that require a chairperson to start the conference).

- LEADER_RECOVERY_TIME = 60

  A time-out measured in seconds after which the system terminates a conference when the chairperson leaves. The time-out enables the chairperson to re-connect prior to conference termination.

  nd enable directly logging in to the conference.

- TCS4_INFO = NO

  Set to YES to allow the field in the video ISDN end points to be configured as the Numeric ID/Chairperson password and enable direct logging in to the conference.

- Q&A=YES

  When enabled provides the Q&A feature for conferences (audio only).

- START_IVR_VIDEO_DELAY_TIME = 6

  When a participant connects to a video conference, sets the amount of time (in seconds) prior to activating the IVR Messaging Service.

- INVITE = YES

  Set to YES to enable the conference chairperson to invite participants during an on going audio only conference.

- EVENT_DISPLAY_DURATION=5

  Establishes the length of time (in sec.) the indication is displayed. The possible values are: 5 (system default), 10 and 15 seconds.

- AD_HOC_EQ_DIRECT_ONGOING_CONF=YES

  By default, the system is configured to validate the participant's right to start a new on going conference without checking if the conference is already running (flag is set to NO).

  When setting the flag to YES, the system validates the participant's right to start a new on going conference only after checking if the conference is already running

- USE_CLI_AS_PWD_FOR_EXT_DB=YES

  By default, the system is configured to validate the participant's right to join a conference using a Password or PIN code for authentication with the external database application (flag is set to NO).

  When set to YES, the system uses the participant's CLI for authentication with the external database application.

Section AUDIO PLUS FLAGS

- VTX = NO

  Set to YES to enable VTX 1000 users to connect to conferences with wide band resources.

- AUTO_AUDIO_PLUS_LOGGER_ON_CARD_STARTUP = YES

  Set to YES to enable the Auto AudioPlus Logger On Startup. An AudioPlus log file is automatically created on each and every system startup.

- AUDIO_PLUS_FREQUENCY = MB

  A parameter for Time Slot Calculation that determines the Audio Algorithm bandwidth settings for the MCU.

  — NB - Narrow Band.

  — MB - Medium Band. In this mode, Siren14 audio algorithms in unavailable.

  — WB - Wide Band. In this mode, Siren14 audio algorithm is available. It decreases the number of audio ports per MCU when set to this mode.

  In order to enable SIREN14 - this flag should be set to WB, with the SIREN14 and PDC_MODE Flag set to YES. When setting this flag to WB, for all standard Audio boards (not Audio+) the MCU activates a system alarm - Major.

- SINGLE_PARTY_HEARS_MUSIC = YES

  When enabled, if the first participant to enter the conference is the only connected participant, s/he hears background music.

- AUDIO_PLUS_CM_FLASH_SIZE = 49152000

  The following flags must be added manually to change their default values:

  AUDIO_PLUS_CM_MSG_32 = 36

  AUDIO_PLUS_CM_MSG_16 = 24

  AUDIO_PLUS_CM_MSG_8 = 172

  AUDIO_PLUS_CM_MSG_4 = 438

  AUDIO_PLUS_CM_MSG_2 = 360

  This group of flags determines the number of audio files for the messages and voice prompts that can be stored in the system’s memory,

sorted in groups according to their duration. There are five duration categories: 2-second, 4-second, 8-second, 16-second and 32-second groups.

Currently, the Audio+ card can store up to 4000 seconds of voice prompts (about 66 minutes). As the voice prompts are stored per duration category there may be redundancies in storage capacity as a 6-second voice prompt will have to be stored under the 8-second category.

The following flags may be manually added to the [AUDIO PLUS FLAGS] section to modify their default value:

- AUTO_AUDIO_PLUS_LOGGER = NO

  Set to YES to enable the Auto AudioPlus Logger. When an AudioPlus unit failure occurs an AudioPlus log file is automatically created.

- AUDIO_PLUS_YES_NO = YES

  Set to YES to enable Audio Plus in the MCU configuration.

- PDC_MODE = YES

  If YES, enables SIREN14 on the system.

- MAXIMUM_AUDIO_PLUS_UNITS_NUMBER = 126

  Set this value to 126 for the MGC-100, 84 for the MGC-50 as an internal parameter for time slot calculation.

  Enter 0 to disable this parameter.

- MUSIC_VOLUME_RATIO = 7

  Determines the volume level of a message played to a participant listening to music. The volume of the message can range from 0-10, where 10 is the maximum. Default setting is 7 (recommended).

- AGC = YES

  If set to YES, activates the Auto Gain Control algorithm for all conferences run on this MCU.

- NOISE_LINE_DETECTION = 0

  Noisy Line Detection analyses the participant's line signal in order to detect a noisy line and notify the operator. This flag activates the SilenceIT algorithm, and is based on the measurement of the audio energy, and based on this measurement, fine-tune the system usage of the SilenceIT algorithm. The audio energy measurements are done by

connecting an endpoint to an ongoing conference, and using the IP Terminal to detect the noise/speech level. The values measured are then compared to the values listed in Table 5-9 on page 5-35. Based on the range of these values the user locates the corresponding parameter. This value is entered here, as the new flag setting.
Setting the flag value to **0** disables the SilenceIT mechanism.

- AUDIOP_TONE_GAIN = 4

  Controls the volume of the bridge tones (for example: entry/exit tones), 0 being the lowest and 10 the highest possible volume for a tone.

Section VIDEO PLUS FLAGS

This section describes the flags available with the Video+ board.

- VIDEO_PLUS_YES_NO = YES

  YES enables the video+ board.

- 4CIF_THRESHOLD = 512

  Possible values - All natural numbers not greater than 1920. This parameter is minimal endpoint call rate in Kbps, whenever possible the encoder transmits H.263 4CIF format.

- COP_SINGLE_ENABLE_QCIF = NO

  Set to YES to allow participants with QCIF only capabilities to join the conference on a single port.

- COP_SINGLE_LINE_RATE_THRESHOLD = YES

  Set to YES to restrict the minimum line rate of the participants joining the conference on a single port. Participants below this threshold connect as secondary (i.e., Audio Only). Otherwise there is no limitation on the line rate to join the Conference On Port.

  The threshold values are taken from a hard-coded table within the MCMS:

Rate	Threshold
1920-1472	768
768	384
512	256
384-192	128
128-64	0

- PARTY_NAME_ALWAYS_ON = NO

  Flag must be set to YES, when requiring the display of participant's names during a conference.

The following flags may be manually added to the [VIDEO PLUS FLAGS] section to modify their default value:

- ENABLE_CLICK_AND_VIEW_SPLASH = YES

  Set to YES to enable the splash screen to be displayed after connecting to an enabled Click & View conference.

- DISPLAY_PARTY_NAME = YES

  When the flag is set to YES, enables the display of participant names during a conference. During *Conference Properties - Settings* definition with any H.320 participant you are required to set the *Chair Control* parameter to **Auto** in order to activate the feature.

- CP_4CIF = YES

  YES - Depending on the call rate endpoint resolution and layout type, the encoder transmits in H.263 4CIF.
  NO - The encoder does not transmit H.263 4CIF.

- CP_HIGH_RES_GRAPHICS = YES

  YES - Enables the support of high resolutions (XGA/SVGA/4CIF/VGA) in CP, COP or Transcoding conferences on the Video+ card.

Section PEOPLE PLUS CONTENT

- ENTERPRISE_PEOPLE_CONTENT = YES

  Enables People+Content for Polycom and iPower endpoints.

- H239 = YES
  YES = Enables H239 Calls.
  NO = Disables H239 Calls.

- GW_EPC_H239 = YES
  YES = Enables H.239 in gateway calls (if both endpoints support People+Content or H.239), with People+Content/H239 conferences.
  NO = Disables gateway calls in People+Content/H239 conferences.

The following flags may be manually added to the [VIDEO PLUS FLAGS] section to modify their default value:

- PEOPLE_AND_CONTENT = YES

  Enables People and Content V0 for PictureTel endpoints.

- ENABLE_IP_DUO_VIDEO = YES

  Enables an IP based Duo Video conference.

- ENABLE_DUO_VIDEO = YES

  Enables a Duo Video conference.

- ENABLE_VISUAL_CONCERT_PC = YES

  Enables the connection of Polycom Visual Concert PC endpoints using both Video and Content streams.

- ENABLE_VISUAL_CONCERT_FX = YES

  Enables the connection of Polycom Visual Concert FX endpoint using both content and video streams.

- CUSTOM_FORMATS_IN_H323_DUO_VIDEO = NO

  Set to YES to enable the custom format of Tandberg H323 Duo Video participants.

- CIF_RESOLUTION_IN_H323_DUO_VIDEO = YES

  Set to YES to enable the declaration of CIF in the content capabilities of Tandberg H323 Duo Video participants.

- ENABLE_H239_EQ=YES

  Set to NO to disable H.239 support in Entry Queues.

- ENABLE_AUTO_1x1_LAYOUT_FOR_CASCADED_LINK=YES

  Set to YES to automatically set the cascaded link to Full Screen (1x1) in CP, forcing the speaker in one cascaded conference to display in full window in the video layout of the other conference. For more details, see the MGC User's Guide, Volume II, Chapter 1.

- H263_ANNEX_T=YES

  Set to NO to send the Content stream without Annex T and enable Athera and Tandberg endpoint that do not support Annex T to process the Content.

Section T1-CAS-PARAMETERS

- T1CAS_WINKSTART_TIMER2 = 1

  Delay before sending WinkStart for dial-in in T1-CAS party; 0 - 10 (0 means no delay, 10 means 100 ms)

- DT_PARAMS = 1,300,600,10,1

  Defines the general characteristics of the dial tone. Continuous flag, Frequency 1, Frequency 2, Time tolerance, Tone order

- DT_CADENCE = 100,300

  Define the dial tone's cadence in pairs - t1_on, t1_off, t2_on, t2_off...

- B_PARAMS = 1,300,600,10,1

  Defines the general characteristics of the busy tone. Continuous flag, Frequency 1, Frequency 2, Time tolerance, Tone order.

- B_CADENCE = 100,300

  Define the busy tone's cadence in pairs - t1_on, t1_off, t2_on, t2_off...

- FB_PARAMS = 1,300,600,10,1

  Defines the general characteristics of the fast busy tone. Continuous flag, Frequency 1, Frequency 2, Time tolerance, Tone order

- FB_CADENCE = 100,300

  Define the fast busy tone's cadence in pairs - t1_on, t1_off, t2_on, t2_off...

- IDLE_CODE_T1_CAS = 0X55

  This is an Idle code (silent), which decides that no more DTMF (the phone number for T1CAS) will be received, and time-out is invoked.

- T1CASDTMFTIMER2 = 3

  The time (in seconds) the MCMS waits after 1 DTMF is received, before it decides that no more DTMF (the phone number for T1CAS) will be received, and time-out is invoked.

- T1CAS_PHONE_LEN = 4

  Enables the MCU to reduce the delay during T1-CAS dial-in connection. When this flag is set to 4 (default), the system assumes that the fourth DTMF code received completes the phone number sent by the endpoint and continues the connection process. When this flag is set to 0, the system ignores this flag and allows a longer delay. Possible values are 0 to 10.

The following flags may be manually added to the [T1-CAS-PARAMETERS] section to modify their default value:

- ALLOW_T1_CAS_PARTICIPANTS_IN_VIDEO_CONFERENCE = NO

  Set this flag to YES to allow T1-CAS, Audio Only participants to join a video conference in a unified (mixed media) MCU. In this case, all video conferences will run on the Audio+ card and not on the Standard Audio. If set to NO (default), T1-CAS participants will not be able to join a video conference.

- AUTOMATICALLY_ALLOCATE_DIAL-IN_NUMBERS_IN_MEET_ME_CONFERENCE_FOR_T1-CAS_SERVICE = YES

  Set this flag to YES (default) to allow the system to automatically allocate T1-CAS dial-in numbers to Meet Me Per Conferences or Meeting Rooms in addition to ISDN numbers. This flag is required only in a unified (mixed environment) MCU. If this flag is set to NO, you can still manually allocate T1-CAS dial-in numbers (in the Meet Me Per Conference tab).

Section NET8_PARAMETERS

- COUNTRY_CODE = COUNTRY_NIL

  Enter the name of the country in which the MCU is located.

- IDLE_CODE_T1 = 0X13

  This is the Idle code (silent), which is transmitted on the ISDN T1 B channels, when there is no transportation on the channel.

- IDLE_CODE_E1 = 0X54

  This is the Idle code (silent), which is transmitted on the ISDN E1 B channels, when there is no transportation on the channel.

- NUMBER_OF_DIGITS = 9

  When using ISDN Overlap sending dialing mode, this field holds the number of digits to be received by the MCU.

- NET8_DEFAULT_TYPE = ISDN or T1-CAS

  This flag is required to select the default network type, as it is not possible to mix an ISDN Network Service and a T1-CAS on the same Net-2/Net-4/Net-8 Network Interface card.

- SILENT_CHNL_TS = 127

  Silent TS for idle pattern (0-127) for T1CAS. TS is TimeSlot. 1 TDM has 128 TS on it.

- SILENT_CHNL_LINE = 15

  Silent TDM for idle pattern (0-15) for T1CAS.

- MIN_TX_WINK = 20

  For T1-CAS, minimum time (in msec) to transmit Wink after receiving Setup. Possible values 0 to 255.

- MAX_TX_WINK = 29

  For T1-CAS, maximum time (in msec) to transmit Wink after receiving Setup. Possible values 0 to 255.

- SETTLING_TIME = 4

  For T1-CAS. DIAL OUT- end of DTMF sending till expected reception of tones. Possible values 0 to 255.

- NO_ASNWER_TONE = 40

  For T1-CAS. Disconnection time-out (in sec.) in case of no answer or no tone. Possible values 0 to 255.

- MIN_RX_WINK = 10

  For T1-CAS, minimum time (in msec) to receive Wink after sending Setup. Possible values 0 to 255.

- MAX_RX_WINK = 35

  For T1-CAS, maximum time (in msec) to receive Wink after sending Setup. Possible values 0 to 255.

- PARTIAL_DIAL_TO = 10

  For T1-CAS. In DIAL IN-How long (in sec) do we wait to the next digit till we decide that this is a partial dialing and therefore an unsuccessful dial in call and resources can be freed. Possible values 0 to 255.

Section ENCRYPTION

- ALLOW_ENCRYPT_IN_PARTY_LEVEL

  YES - Enables encrypted participants in non-encrypted conference.
  NO - Disables encrypted participants in non-encrypted conference.

The following flags may be manually added to the [ENCRYPTION] section to modify their default value:

- SIZE_OF_ENCRYPTION_KEY_DATABASE_FOR_POLYCOM_ISDN = 200

  The size values (200-600) for the database.

- SIZE_OF_ENCRYPTION_KEY_DATABASE_FOR_IP = 200

  The size values (200-600) for the database.

- SIZE_OF_ENCRYPTION_KEY_DATABASE_FOR_TANDBERG_ISDN = 200

  The size values (200-600) for the database.

Section H264

- ENABLE_HD_SD_IN_FIXED_MODE = NO

  If this flag is set to YES, H.264 Standard Definition (SD), High Definition (HD) and VSX 8000 (version 8.0) HRR resolutions are supported in Video Switching conferences.

- H264 = YES

  YES - Supports H.264 on the MCU
  NO - H.264 is not supported by the MCU

- GW_H264 = NO

  YES - Gateway support for H.264 participants on the MCU.
  NO - H.264 gateway capabilities are not supported on the MCU.

- H264_UPPER_LIMIT = 384

  The maximum Line Rate that can be supported with H.264.

- UPGRADE_TO_H264 = NO

  YES - The Auto protocol settings for a video switching conference implement H.264 after using H263 or H261.
  NO - The Auto protocol video switch conference will not change to H264 (after it changed to H263/H261).

- H264_VSW_AUTO = YES

  If set to NO, Video Switching conferences are set to fixed mode. In VSW 264 resolution in SIP environment that doesn't support highest common this flag should be NO.

Section RESOURCE_REPORT_LOGGER

The following flags may be manually added to the [RESOURCE_REPORT_LOGGER] section to modify their default value:

- RESOURCE_REPORT_MECHANISM = NO

  YES - Enables the resource report mechanism.
  NO - Disables the resource report.

- MAX_NUMBER_OF_RR_FILES = 100

  Maximum number of files. The default is set to 100.

- TIME_RETRIVING_INTERVAL_FOR_RR_FILES = 5

  Interval in minutes for data retrieval.

- RESOURCE_REPORT_MAX_TIME_FILE_TO_LIVE = 120

  The time range in minutes.

Section MUX PLUS FLAGS

The following flag may be manually added to the [MUX PLUS FLAGS] section to modify its default value:

- AUTO_MUX_PLUS_LOGGER = YES

  YES - Enables the automatic creation of MUX+ Logger diagnostic file when the unit fails.
  NO = Disables automatic creation of MUX+ Logger diagnostic file.

Section EXTERNAL DB FLAGS

- ENABLE_EXTERNAL_DB_ACCESS = NO

  If YES, the bridge will try to connect to an external database application.

- EXTERNAL_DB_IP = 0.0.0.0

  The IP address of the external application server.

- EXTERNAL_DB_PORT = 80

  The Database Server port used by the MCU to send and receive XML requests/responses to the external application server.

- EXTERNAL_DB_LOGIN = POLYCOM

  The Database Server login, that is, the user name defined in the external application for the MCU.

- EXTERNAL_DB_PASSWORD = POLYCOM

  The Database Server password, that is, the password associated with the user name defined for the MCU in the external database application.

- EXTERNAL_DB_DIRECTORY= ““

  The Database Server directory which holds the translation script.

- AUTHENTICATE_USER = NO

  If the flag is set to YES then the MCU validates the user that is trying to connect to the MCU (through the MGC Manager or other application) with an external database rather than validating with its internal users list.

Section SIP REFER PREFIX AND PHONES

These flags are only needed when working with SIP CX – Microsoft. These flags are used to parse a REFER message. The system decides where to call according to the prefix and if there is no prefix the default is PSTN.

- NUM_OF_DIGITS_IN_PREFIX_NUMBER = 0

  Defines the length of the SIP_REFER_XXX_PREFIX for all network types.

- SIP_REFER_ISDN_PREFIX = 0

  The prefix that routes the call to the ISDN network.

- SIP_REFER_H323_PREFIX = 0

  The prefix that routes the call to the H.323 network.

- SIP_REFER_PREFIX = 0

  The prefix that routes the call to the SIP network.

- SIP_REFER_MPI_PREFIX= 0

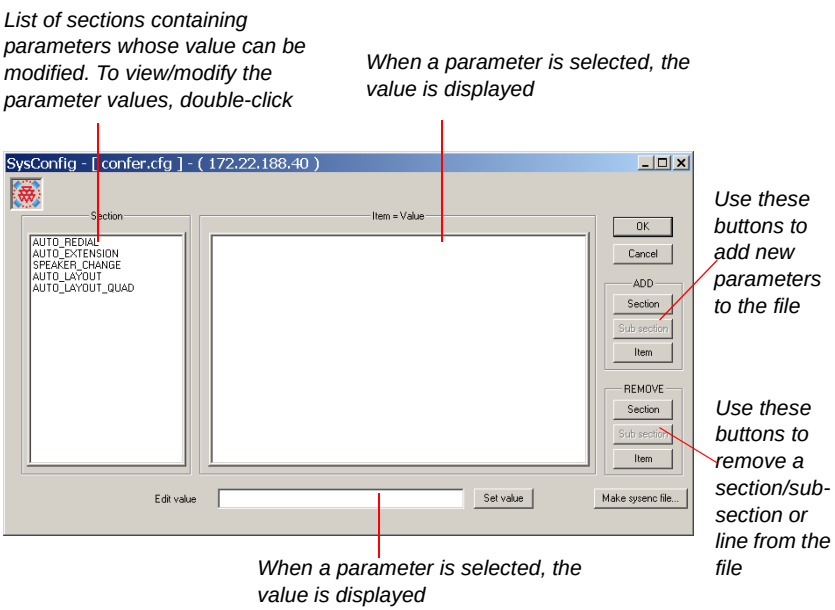
  The prefix that routes the call to the MPI network.

Edit "confer.cfg"

The "confer.cfg" file is used to modify automatic re-dialing parameters, the automatic extension of the conference duration and the Auto Layout parameters.

To modify the "confer.cfg" file:

1. On the *MCU Utils* sub-menu, click **Edit "confer.cfg"**.
   The *SysConfig* dialog box opens.



2. In the *Section* box, double-click the section you want to change.

   The parameter names and values are displayed in the *Item=Value* box.
3. In the *Item=Value* box, click the value to be modified.

   The item's value is placed in the *Edit value* text box.
4. In the *Edit value* text box, edit the value.
5. Click the **Set Value** button to apply the new value to the file.
6. Click **OK**.

Confer.cfg Flags

Section AUTO_REDIAL

- NUM_REDIAL_TIMES = 3

  The number of times the system redials when a participant is disconnected.

- REDIAL_INTERVAL_IN_SECS = 30

  The interval between system redial attempts when a participant is disconnected.

Section AUTO_EXTENSION

The end time of a conference can be automatically extended without operator intervention. The following parameters are defined at the MCU level and they apply to all the conferences that will be run on this MCU. Whether the automatic extension of conference duration will apply to a specific conference is determined by enabling the End Time Alert Tone, in the *Conference Properties – Settings* dialog box.

- ENABLE_AUTO_EXTENSION

  Defines whether the automatic extension is enabled and if it can be applied to conferences. Select **YES** to enable the auto extension mode for conferences, or **NO** to disable it.

- MAX_EXTENSION_TIME

  The maximum accumulative number of minutes to be added to the predefined conference duration. For example, if the conference duration is set to 3 hours and this flag is set to 45 minutes, the total number of minutes that can be added to a conference (in multiples defined in the Extension Time Interval field) is 45 minutes, totaling a conference duration of 3 hours and 45 minutes.

- EXTENSION_TIME_INTERVAL

  The number of minutes that the conference will be extended by each time the system checks and identifies that at least one participant is still connected to the conference.

Section SPEAKER_CHANGE

- SPEAKER_CHANGE_TIME_INTERVAL = 0

  The amount of time a speaker is displayed before the system starts checking if there is a new speaker. The minimum time that a speaker has

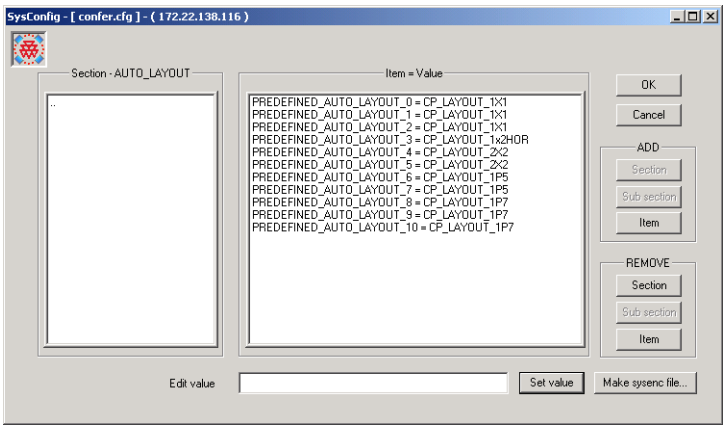
to speak to become the main speaker is set per conference in the *Talk Hold Time* field, in the *Conference Properties – Settings* dialog box.

Sections AUTO_LAYOUT and AUTO_LAYOUT_QUAD

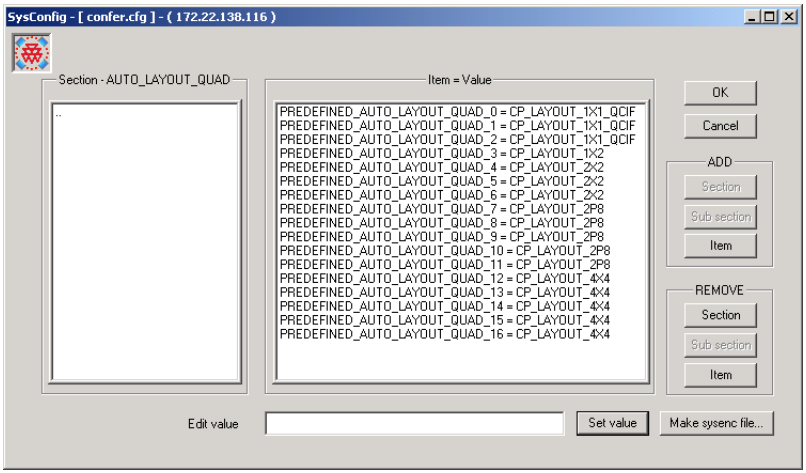
Layout selection for each number of video participants is defined in the "confer.cfg" file. These values can be modified.

The flags are divided into two sections:

- AUTO_LAYOUT contains the layout definitions for Continuous Presence – Classic



- AUTO_LAYOUT_QUAD contains the layout definitions for Continuous Presence – Quad Views.



To modify these values, enter the appropriate name of the layout.

Table 5-15details the names of Continuous Presence – Classic layouts that can be entered in the “confer.cfg” to modify the automatic layout selection.

Table 5-15: Continuous Presence – Classic Layout Names

Layout #	Layout Name in “confer.cfg”	Layout
1	CP_LAYOUT_1X1	
2	CP_LAYOUT_1X2	
3	CP_LAYOUT_2X1	
4	CP_LAYOUT_2X2	
5	CP_LAYOUT_3X3	

Table 5-15: Continuous Presence – Classic Layout Names (Continued)

Layout #	Layout Name in "confer.cfg"	Layout
6	CP_LAYOUT_1P5	
7	CP_LAYOUT_1P7	
8	CP_LAYOUT_1x2VER	
9	CP_LAYOUT_1x2HOR	
10	CP_LAYOUT_1P2VER	
11	CP_LAYOUT_1P2HOR	
12	CP_LAYOUT_1P3HOR	
13	CP_LAYOUT_1P3VER	
14	CP_LAYOUT_1P4HOR	
15	CP_LAYOUT_1P4VER	
16	CP_LAYOUT_1P8CENT	

Table 5-15: Continuous Presence – Classic Layout Names (Continued)

Layout #	Layout Name in "confer.cfg"	Layout
17	CP_LAYOUT_1P8UP	
18	CP_LAYOUT_1P2HOR_UP	
19	CP_LAYOUT_1P3HOR_UP	
20	CP_LAYOUT_1P4HOR_UP	
21	CP_LAYOUT_1P8HOR_UP	

Table 5-16details the names of Continuous Presence – Quad Views layouts that can be entered in the "confer.cfg" to modify the automatic layout selection.

Table 5-16: Continuous Presence – Quad Views Layout Names

Layout #	Layout Name in "confer.cfg"	Layout
22	CP_LAYOUT_4X4	
23	CP_LAYOUT_2P8	
24	CP_LAYOUT_1P12	
25	CP_LAYOUT_1X1_QCIF	

When a conference set to both Auto Layout and Presentation Mode is run on the Standard Video card the definition of the layouts selected for Auto Layout changes to the following video layouts:

1 participant = 1X1;
2 participants = 1X1;
3 participants = 1X2;
4 participants = 2X2;
5 participants = 2X2;
6 participants = 2X2;
7 participants = 3X3;
8 participants = 3X3;
9 participants = 3X3;
10+ participants = 3X3

Automatic re-dialing During the Conference

The automatic re-dialing during the connection process can be extended to the duration of the on-going conference. If a dial-out IP (H.323 or SIP) participant disconnects from the conference for any reason, the MCU will automatically redial to that participant, hence saving the need to call the operator (if one is available), or connecting as dial-in (if the conference number is known).

The MCU will not redial the participant's endpoint when the participant's endpoint was disconnected or deleted from the conference by the operator

To enable the automatic re-dialing during the conference, in addition to the system.cfg flag ENABLE_IP_REDIAL that should be set to ALWAYS, the following flags must be set in the confer.cfg file:

Table 5-17: confer.cfg Flags Values

Flag Name	Value	Description
REDIAL_INTERVAL_IN_SECS	30 (default), 60	Defines the interval, in seconds, between redialing attempts.

Table 5-17: confer.cfg Flags Values (Continued)

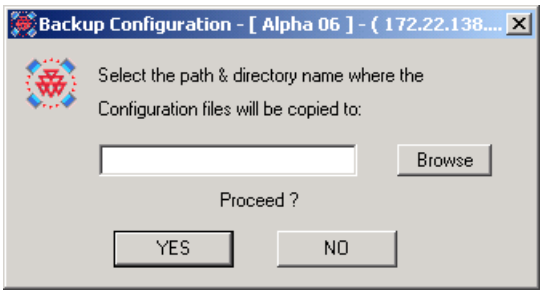
Flag Name	Value	Description
NUM_REDIAL_TIMES	2 (default), 10	Defines the number of times the MCU will attempt to dial out to the participant during the conference.
	Auto	Setting this flag to Auto forces the MCU to continue re-dialing to the endpoint until the end of the ongoing conference.

Backup Configuration

This utility is used to backup the MCU's various configuration files.

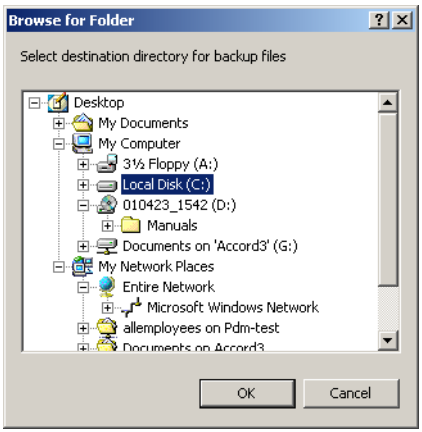
To backup the configuration files:

1. From the *MCU Utils* sub-menu select **Backup Configuration**. The *Backup* dialog box opens.



2. Type the name and path of the destination folder for the backup files, or click the **Browse** button to select the destination folder.

If you have selected Browse, the *Browse for Folder* dialog box opens, enabling you to select the destination folder.



Select the destination folder and click **OK**.
The system returns to the *Backup* dialog box.

3. Click **YES** to copy the files to the destination folder or **NO** to cancel the operation.
   A progress indicator is displayed, listing the files being copied to the destination directory.

   At the end of the backup process, the system displays a completion message.

4. Click **OK**.
   The system stores the configuration files in the selected directory, in a folder whose name is derived from the MCU name. Under this folder two new folders are created:

   — *CFG Files* - contains the configuration files

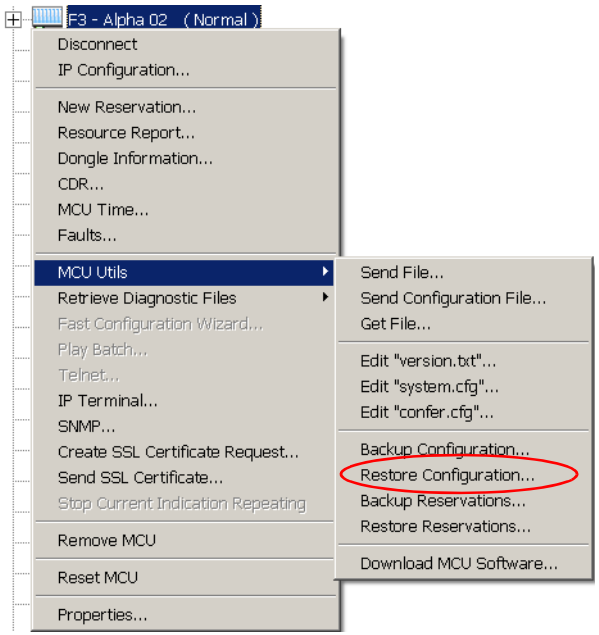
   — *Msg Files* - contains the audio and video files used in the Greet and Guide mode, and in the IVR Service

Restore Configuration

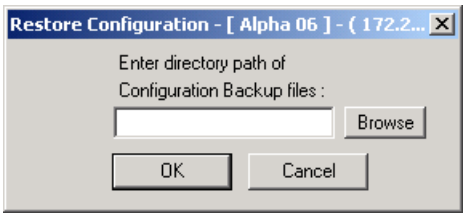
This utility is used to restore the MCU's various configuration files that were saved to disk and the default IVR Service provided with the installation CD. This utility is used when there are problems with the MCU's configuration files and you want to reinstall them, or when you want to install or restore the default IVR Message Service, Entry Queue Service or Default Gateway Session Profiles. For instructions on installing and restoring the default IVR Message Service see *Chapter 2, "Manual Installation of the Default Message Services" on page 2-30*.

To restore the configuration files:

1. On the *MCU Utils* sub-menu, click **Restore Configuration**.



The *Restore Configuration* dialog box opens.



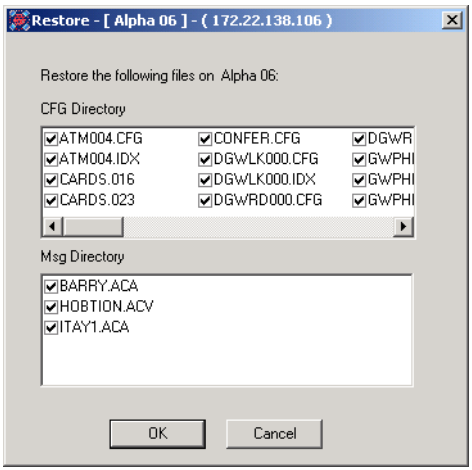
2. Type the configuration files path to be installed, or click the **Browse** button to locate them.

   If you have selected Browse, the *Browse for Folder* dialog box opens, enabling you to select the source folder.

   Select the folder in which the backed up configuration files were stored (this folder has the MCU name and contains the sub-folders with the configuration files) and click **OK**.
   The system returns to the *Restore* dialog box.

3. Click **OK** to continue.

   The *Restore* dialog box is displayed.



The system lists the configuration files (*CFG Directory* box) and the audio and video files (*Msg Directory* box) used in the Greet and Guide mode that were backed up to your disk. By default, all the files are

checked. To cancel the copy of a certain configuration file, clear its check box.

4. Click **OK** to install the configuration files on the MCU.

Reservations Backup and Restore

You can backup reservations and meeting rooms to files stored on any disk on the network. However, Reservations are automatically restored after software upgrade and you therefore do not need to *Restore* the reservations. It is recommended that you backup reservations using the Reservations Backup utility. Reservation backups **are not** compatible between versions, therefore you should backup reservations before and after any version or software upgrade.

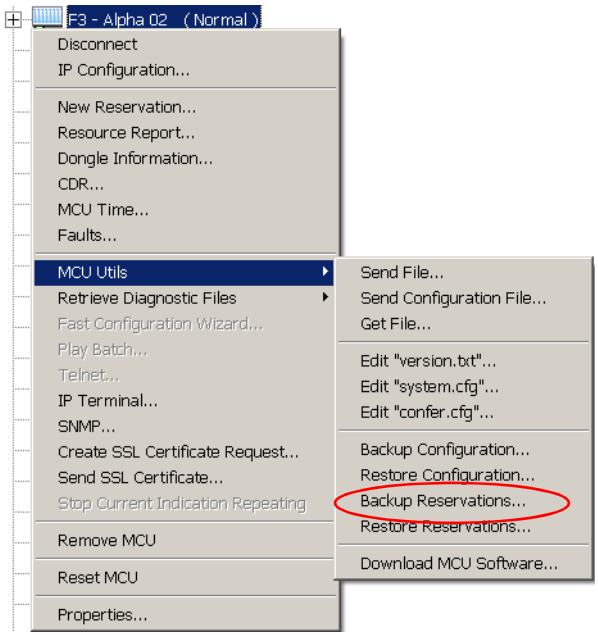
Reservations and meeting rooms can be restored back to the MCU. This option is useful when you upgrade from one version to another, or when you modify certain settings in the MCU, which could result in the loss of reservations.

Backing up Reservations

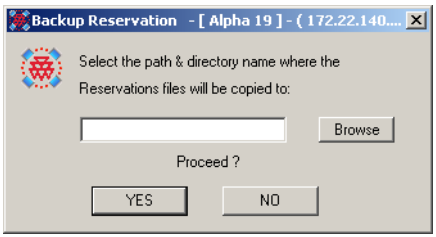
When you upgrade the new software, the existing reservation files are automatically restored and converted to the new version format. It is essential to back up reservations with the new version format.

1. Connect to the MCU whose reservations need to be backed up.

2. Right-click the MCU's icon, click **MCU Utils,** and then click **Backup Reservations**.



The *Backup Reservations* dialog box opens



3. Enter the path of the destination folder where the backed-up Reservation and Meeting Room files will be stored, or click the **Browse** button to select the destination folder from the *Browse for Folder* dialog box.
4. Select the drive and folders using the standard Windows conventions, and then click **OK**.

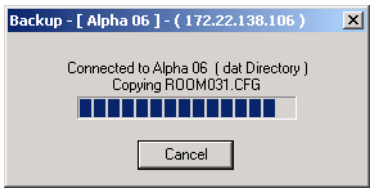
5. The selected path appears in the *Backup Reservations* dialog box. The system automatically creates a sub-folder in the selected path using the MCU's name in the following convention:

   drive:\selected folder\ MCU name

   For example, if the MCU name is ALPHA6 and the selected path is D:\ Personal, the actual path will be: D:\ Personal\ALPHA6.

6. Click **YES** to proceed (**NO** will cancel the operation).

   The *Backup* progress indicator opens, displaying the names of the files being copied to the selected destination.



   When the backup process is completed, the *Finished* message box opens.

7. Click **OK**.

   A subdirectory named *dat* is created in the selected destination folder. This directory contains the backup files *cfg* and *idx*.

   Backup files are of the following type:

   — *Rsrv xyz.cfg* – Reservations data files

   — *Rsrv xyz.idx* – A binary index file that contains the reservation name, and an offset to retrieve the details from the data file

   Meeting Room files are of the following type:

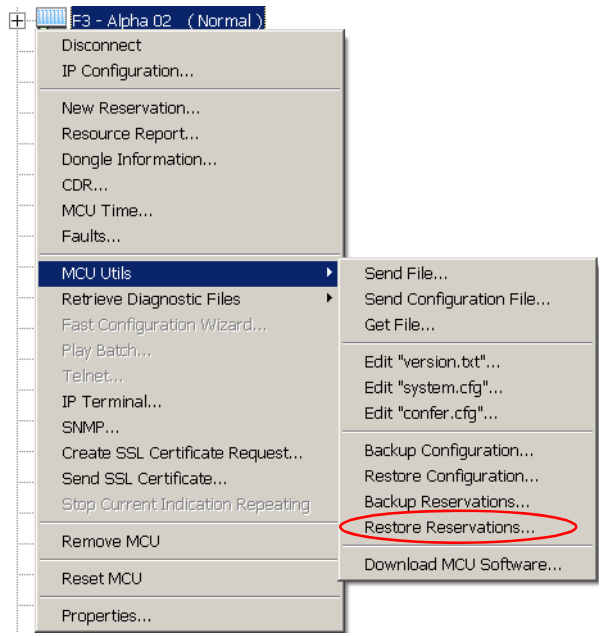
   — *Room xyz.cfg* – Meeting data file

   — *Room xyz.idx* – A binary index file that contains the meeting room name, and an offset to retrieve the details from the data file

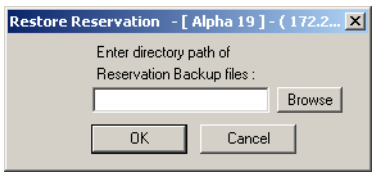
Where *xyz* represents the MCU's internal version number at the time the reservation was scheduled. You will therefore have a new set of files whenever the MCU's version is updated.

Restoring Reservations and Meeting Rooms

1. Connect to the MCU to which the reservations and meeting rooms are to be restored.
2. Right-click the *MCU* icon, click **MCU Utils**, and then click **Restore Reservations**.



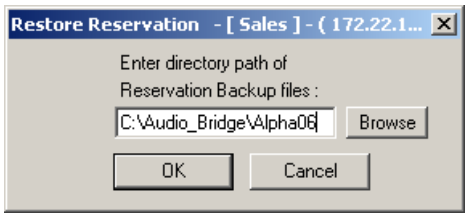
The *Restore Reservation* dialog box opens.



3. Enter the path of the source folder where the backup files are stored, or click the **Browse** button, to select the folder from the *Browse for Folder* dialog box.
4. Select the drive and folders using the standard Windows convention, and then click **OK**.

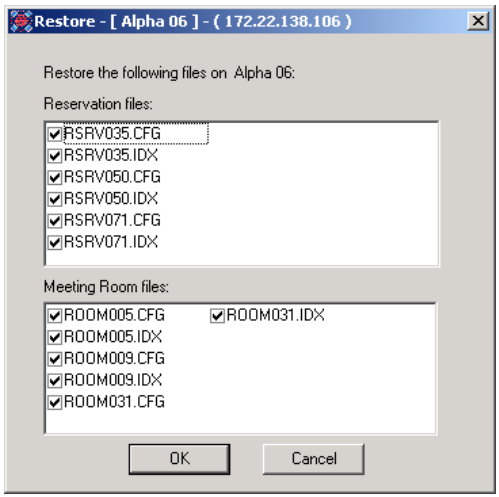
   Note that the files are stored under the.dat directory.

   The selected path appears in the *Restore Reservation* dialog box.



5. Click **OK**.

   The *Restore* dialog box opens.



   The *Restore* dialog box displays all the Reservation and Meeting Room files that are currently stored in the selected path.

   The system lists the reservation files (*RSR*) and the meeting room files (*ROOM*) used in the Greet and Guide mode that were backed up to your disk. By default, all the files are checked.

6. To restore a file, check the check box next to the file name.

   To cancel the copy of a certain configuration file, clear its check box.

7. Click **OK**.

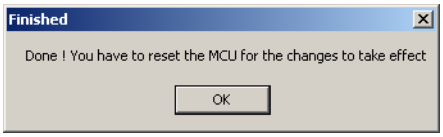
   A warning message is displayed, prompting you to either abort the procedure, or to continue.

During the restoring process, the system overwrites all reservations that are currently saved on the MCU whose MCMS version is the same as those being restored.
It is possible to restore reservations to a different MCU provided the same MCMS version is loaded on both MCU's.

8. Click **Yes** to continue.

   The *Restore* progress indicator opens, displaying the files that are being restored.

   When all the files have been restored, the *Finished* message box is displayed.



9. Click **OK**.

The *Restore* dialog box closes. You need to reset the MCU for any changes to take effect.

When restoring reservations to an MCU with a newer MCMS version that contains additional parameters, the additional parameters (which are not included in the restored reservations) are set to their default values. If a parameter no longer exists in the new MCMS version, it will be removed from the reservations being restored.
The reservation data is related to the MCMS S/W version – i.e. to the MCMS parameters used to set up a conference and each MCMS S/W has its own unique identifier (for example Rsrv025 relates to MCMS S/W version 25).

Download MCU Software

The MCU installation utility is used to update or reinstall the software on an MCU. The files are copied from the appropriate drive on the operator workstation to the MCU. This procedure is described in detail in *Chapter 2, "MGC Unit Software Installation" on page 2-22.*

Retrieving Diagnostic Files

There are numerous MCU tools to debug and trace suspended tasks. These tools are:

- System Diagnostic Files
- System Dump Files
- IP Card Diagnostic Files
- Video+ Diagnostic Files
- Logger Diagnostic Files
- Audio+ Diagnostic Files
- MUX+ Diagnostic Files

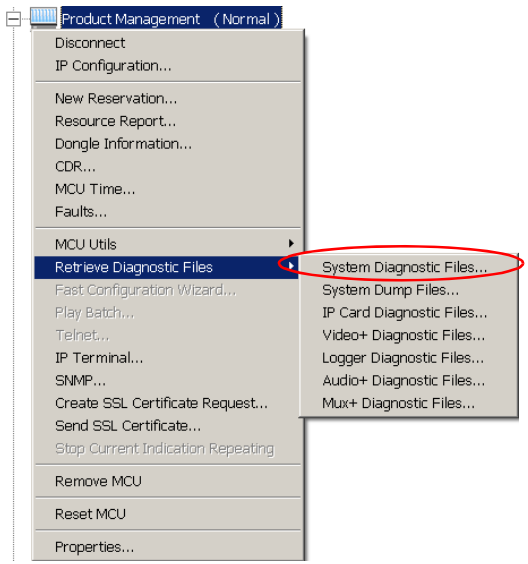
System Diagnostic Files

This utility is a debugging tool that traces a problem in the system and captures the relevant details to a file, allowing the problem to be analyzed. This feature records the traces that follow the specific task that became suspended due to an exception.

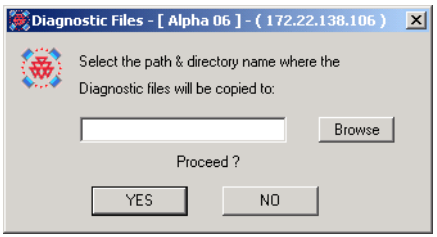
The trace includes the content of that task's stack, making it possible to track all the addresses to which the task had been, until the exception occurred. For more information on the Trace-Capture function, see *"IP Terminal" on page 5-29*.

To back up the exception files:

1. Right-click the *MCU* icon, click **Retrieve Diagnostic Files**, and then click **System Diagnostic Files**.

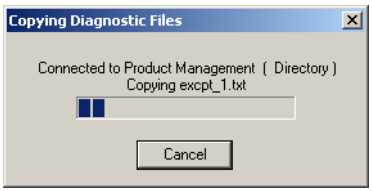


The *Diagnostic Files* dialog box opens.



2. Enter the destination path name to where you want to copy the diagnostic files, or click the **Browse** button and select a destination folder from the *Browse for Folder* dialog box.
3. Click **YES** to proceed.

A progress indicator opens displaying all the files being copied to the destination directory.



Once all the exception files have been copied to the destination directory, the *Finished* message box opens.

4. Click **OK**.

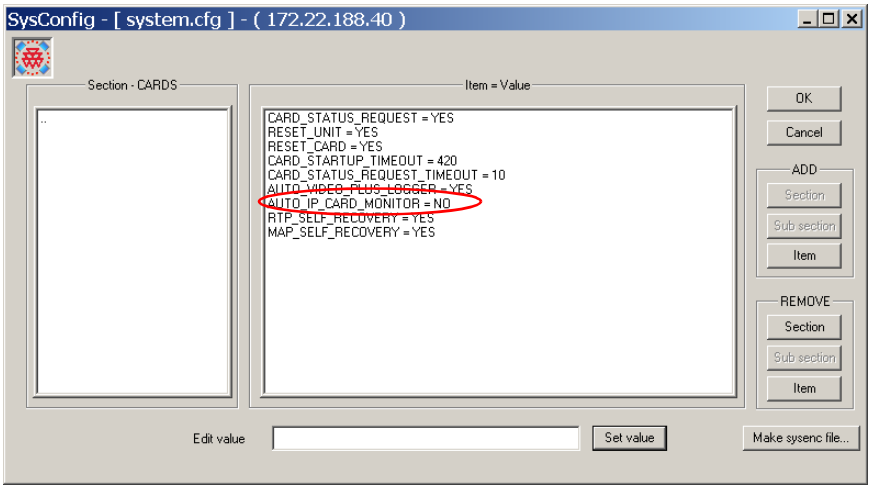
   The exception files are stored in the <*MCU Name*>/diagnos sub-folder of the selected destination folder

IP Card Diagnostic Files

When an error occurs on the IP, a trace-capture may be created automatically (if the appropriate option is selected in the system.cfg) or manually via IP terminal. The IP trace-capture file created when an error occurs in the IP card is saved on the MCU in the directory **7.256/mcu/cardmntr** and can be retrieved using the *IP Card Diagnostic Files* utility. The file can then be analyzed to determine the problem.

To automatically create a trace-capture file when there is a problem with the IP card:

The automatic creation of the IP trace-capture file is controlled by a flag in the “system.cfg” in the *CARDS* section: AUTO_IP_CARD_MONITOR.



For details of flag modification in the “system.cfg” see *“Edit “system.cfg”” on page 5-64*.

This flag may be set to one of the following options:

- **NO** (no automatic monitoring – only manual monitoring is available)
- **UNIT** (traces will be automatically saved for each unit failure)
- **CARD** (traces will be automatically saved for each card failure)

If *Unit* or *Card* are selected, a file containing the trace information for each failure will be created using the name format **crdmn_nn.txt**, where nn is a number between 00 and 19. The files are created sequentially, cyclically, when the 20th file overwrites the first file and so on. Recommended mode is NO (manual card monitor).

The IP card diagnostic file stored on the system saves the following traces to the diagnostic file:

- Messages between tasks
- Tasks error messages

- The timer and TDM tasks workflow by 10 milliseconds time stamps
- Running tasks and their last action
- Tasks status: idle, running, wait
- Queues status: full, empty
- Registers

To manually create an IP diagnostic file:

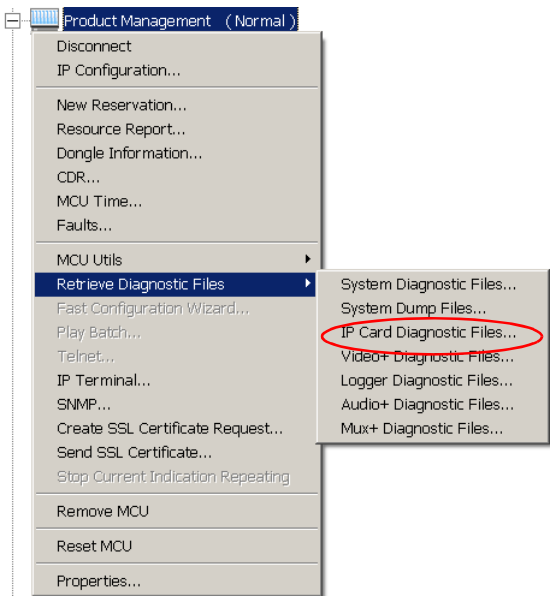
In the *IP Terminal* window, type the command:
card_monitor <board_id> <file_name>

Where <*board_id*> is the IP board slot number (for example, 4), and <*file_name*> is the text file name (for example, Crdmntr1.txt), under which the information will be stored.
For example, type **card_monitor 4 crdmntr1.txt**

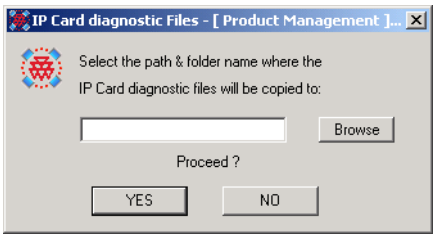
The file is stored in the MCU under the directory **7.256/mcu/cardmntr**. This folder is automatically created by the system if it does not exist on the MCU.

To retrieve the H.323 trace-capture files:

1. Right-click the *MCU* icon, click **Retrieve Diagnostic Files**, and then click **IP Card Diagnostic Files**.



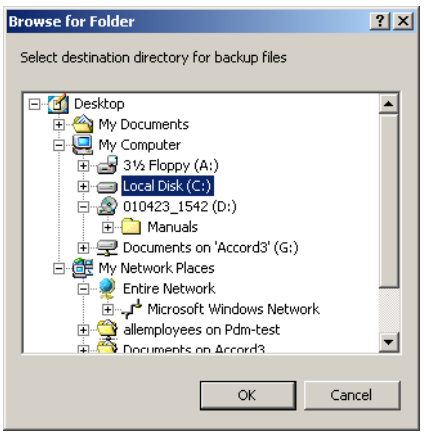
The *IP Card Diagnostic Files* dialog box opens.



2. In the *Local path* box, type the path of the destination directory where the diagnostic file will be stored, or click **Browse**.

   The *Browse for Folder* dialog box opens.

3. Select the destination folder and click **OK**.



   The selected folder is displayed in the *H323Card Monitoring Files* dialog box.

4. In the *H323Card Monitoring Files* dialog box, click **Yes** to proceed.

   The files are stored in the <MCU *Name*>/cardmntr sub-folder of the selected destination folder.

Retrieving the H.323 diagnostic file resets the H.323 card. Make sure that there are no conferences running on the card when the card monitor command (creating the H.323 diagnostic file) is executed.

Video+ Logger

The Video+ Logger is a utility that records diagnostic information about the Video+ cards. This information is used by Polycom personnel to identify problems on the card.

When an error occurs on the Video+ card, a trace file may be created automatically (if the appropriate option is selected in the system.cfg), or manually via IP terminal. The Video+ trace file is automatically stored on the MCU and can be retrieved using the *Retrieve Diagnostic Files* utility. The file can then be analyzed to determine the problem.

Video+ Logger File Structure

The files are stored under the folder: **7.256\mcu\vp_log.** This folder is automatically created by the system if it does not exist on the MCU.

The Video+ card diagnostic file header contains the following fields:

- Date and Time
- MCMS Version Number
- Board ID, component ID
- Video+ component versions
  - MNG_FILE (card manager)
  - VIDEO_PLUS_PROCESSOR_FILE (map)
  - VIDEO_PLUS_FPGA_FILE (bcod)

The log data is comprised of Card Manager data and/or map log from a faulty unit. Each logger file can be up to 72KB, including header.

Creating the Video+ Logger Files

The Video+ logger file may be created automatically or manually.

Automatic creation of the Video+ logger files

The automatic creation of the Video+ trace-capture file once a failure occurs is enabled in the "system.cfg" in the *CARDS* section, by setting the flag AUTO_VIDEO_PLUS_LOGGER to **YES**. When setting this flag to **NO**, the

The files are created sequentially, cyclically, when the 100^{th} file overwrites the first file and so on. Recommended mode is **NO** (manual card monitor).

The file names are generated automatically, with the following components:

- Text: **vp_logger**
- Board ID number
- Unit ID number
- A serial number between 0 and 99, ascending sequentially

For example, a file could be named: **vp_logger 4 2 03** where **4** is the Board ID number, **2** is the Unit ID number and **03** is the serial number.

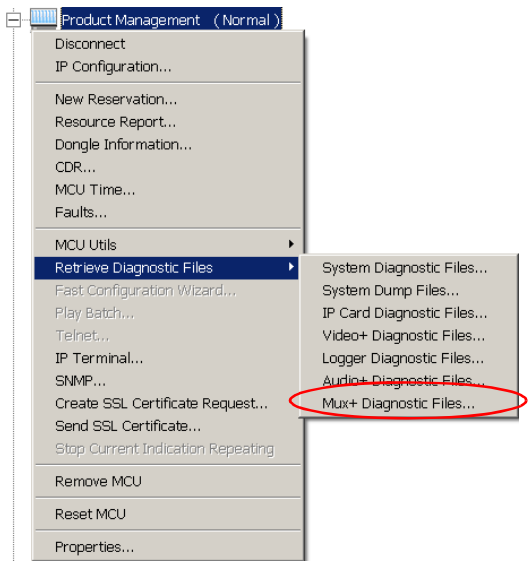
Manual creation of the Video+ logger files:

- In the *IP Terminal* window, type the command:
  vp_logger <board_id> <unit_id>

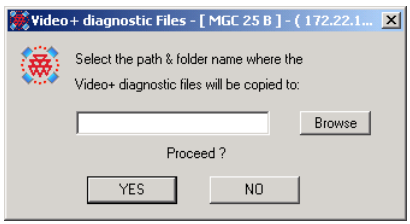
  Where <*board_id*> is the Video+ board slot number (in the MGC 25, the "logical" slot number as appears in the MGC Manager) and <*unit_id*> is the mapped unit ID (0 for Card Manager).
  For example, type **vp_logger 5 0.**

Retrieving the Video+ Logger files

1. Right-click the *MCU* icon, click **Retrieve Diagnostic Files**, and then click **Video+ Diagnostic Files**.



The *Video+ Diagnostic Files* dialog box opens.

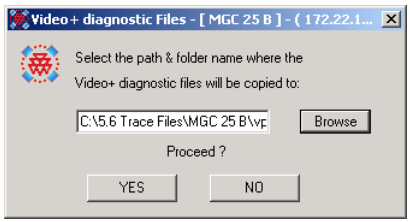


2. In the *Local path* box, type the path of the destination directory where the diagnostic file will be stored, or click **Browse** to select the destination folder.

   The *Browse for Folder* dialog box opens.

3. Select the destination folder and then click **OK**.

   The selected folder is displayed in the *Video+ Diagnostic Files* dialog box.



4. In the *Video+ Diagnostic Files* dialog box, click **Yes** to proceed.

   The Video+ diagnostic file is saved in the <*MCU Name*>/vp_log sub-folder of the selected destination folder.

Logger Diagnostic Files

The Logger utility is a troubleshooting tool that continually records MCU system messages and saves them to files in the hard drive of the MCU. For each time interval defined in the system, a different data file is created. New files are created until the maximum size allowed for messages (usually most of the hard drive free disk space) is reached. When the maximum file size limit is exceeded, the system overwrites the old files in a cyclical order (that is, the new file overwrites the first file). The files may be retrieved from the hard drive for off-line analysis and for debugging purposes. The files to which the messages are saved are compressed in order to conserve space and allow the maximum number of system messages to be stored.

The Logger utility is activated at the MCU startup. The Logger is disabled when the MCU is Reset manually (from the MCU unit), or when there is a problem with the Logger utility (such as a problem in the hard drive where the files are saved). In such cases, the data is lost.

When the MCU is reset from the MGC Manager, the files are saved on the MCU hard drive.

The Logger Files

The following files are saved to the MCU hard drive:

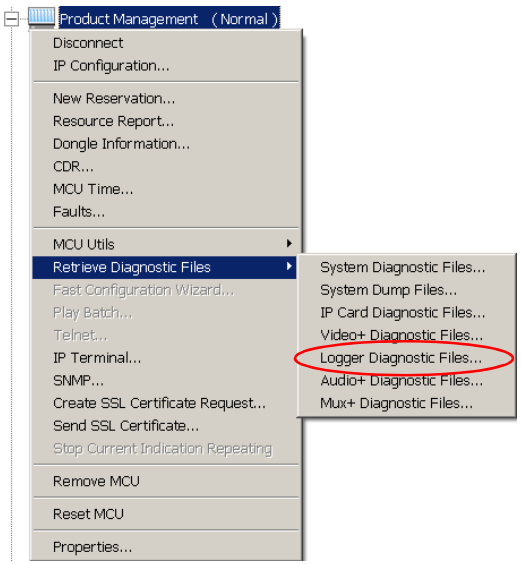
- Data files - These files contain the messages generated by the system in a given time interval. The default time interval is 10 minutes. The file is named using the following format: logNNNNN.log where NNNNN represents the file's sequential order in the creation cycle, for example, log00011.log is the eleventh file to be created.
- Index file - This file contains a list of all the data files currently saved to the MCU hard drive, the time and date of the first message and the time and date of the last message included in each file.

The Logger Utility must be enabled in the system.cfg. For details, see *"Edit "system.cfg"" on page 5-64*.

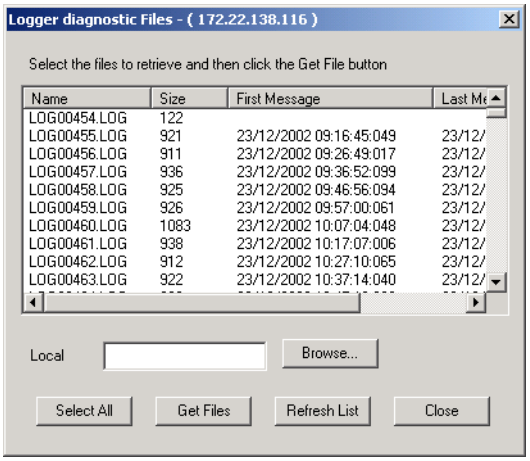
Retrieving the Logger Files

You can easily retrieve the files stored on the MCU and then save them to your PC or another location on your network.

1. Right-click the *MCU* icon, click **Retrieve Diagnostic Files**, and then click **Logger Diagnostic Files**.



The *Logger Diagnostic Files* dialog box opens.

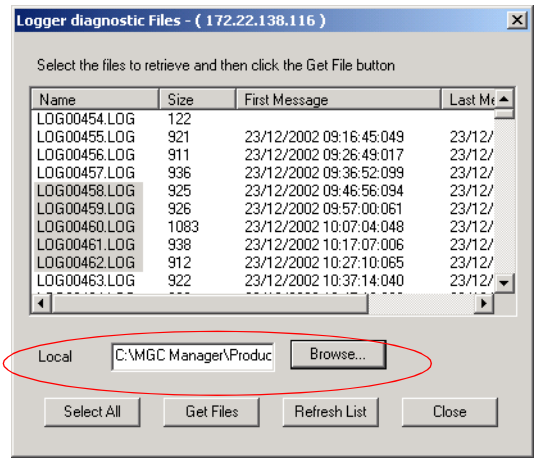


2. Select the files to retrieve or click the **Select All** button to retrieve all the files currently stored on the MCU's hard drive.

The trace files are saved periodically, so you can access them according to their time frame. However, if you want to examine the messages generated in the hard drive in the latest time interval, it is possible that the file has not yet been saved to the hard drive. To force the system to close a data file and save it, use the **IP Terminal** utility and enter **stop_logger** in the command line.
To resume the Logger utility activity (once it was forced to stop logging), use the **IP Terminal** utility and enter **start_logger** in the command line.

3. Click the **Browse** button to select the destination folder to store the retrieved files.
   The *Browse for Folder* dialog box appears.
4. Select a folder and click **OK**.

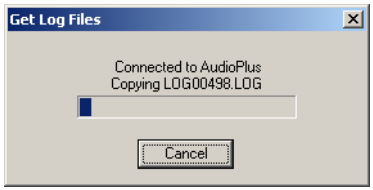
   The destination path is listed in the *Local* field.



Sometimes the list of Logger data files may not be updated and some of the files may be missing. In such a case, exit and re-access the MGC Manager application.

5. Click the **Get Files** button.

The *Get Log Files* dialog box appears while retrieving the selected files files.

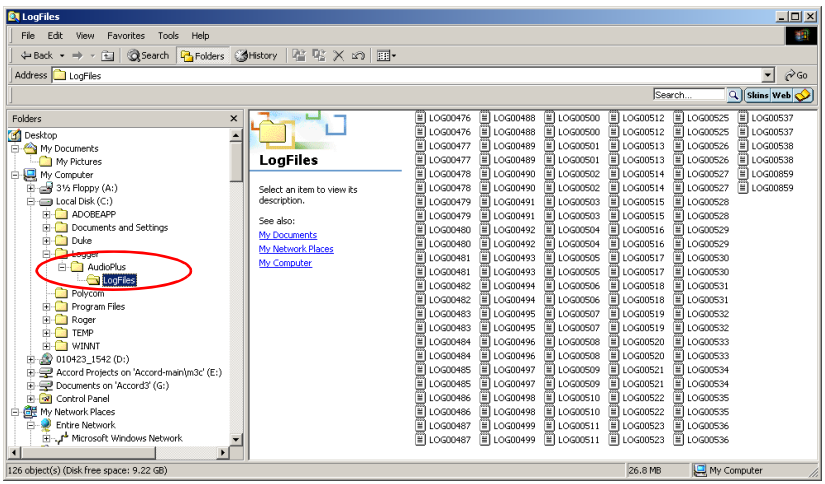


The files are saved in the <*MCU Name*>/logfiles sub-folder of the selected destination folder.

Displaying the file contents

To analyze the messages generated by the system, open the text files retrieved from the MCU using any text editor such as Notepad, or Microsoft Word.

1. In Windows Explorer, browse to the folder containing the log files.



2. Using a text editor application, open the Logger data file to analyze its contents or send the file(s) to your next level of support.

Sometimes the data file cannot be opened in the text editor application. In such a case, close the MGC Manager application used to retrieve the Logger data files.

Audio+ Logger

The Audio+ Logger is a utility that records diagnostic information about the Audio+ cards. This information is used by Polycom personnel to identify problems on the card.

The Audio+ Logger is available in the MGC-50/100, but not in the MGC-25.

A trace file may be created manually via IP terminal. The Audio+ trace file is automatically stored on the MCU and can be retrieved using the *Retrieve Diagnostic Files* utility. The file can then be analyzed to determine the problem.

Audio+ Logger File Structure

The files are stored under the folder: **7.256\mcu\ap_log**

The Audio+ card diagnostic file header contains the following fields:

- Date and Time
- MCMS Version Number
- Board ID, component ID
- Audio+ component versions
  - MNG_FILE (card manager)
  - AUDIO_PLUS_CONTROLLER_FILE
  - AUDIO_PLUS_UNIT_FILE

The log data is comprised of Card Manager data. Each logger file can be up to 72KB, including header.

Creating the Audio+ Logger Files

The Audio+ logger file may be created automatically or manually.

Automatic creation of the Audio+ logger files

The automatic creation of the Audio+ trace-capture file is controlled by the AUTO_AUDIO_PLUS_LOGGER_ON_CARD_STARTUP flag in the “system.cfg” in the *AUDIO PLUS FLAGS* section.

The flag may be set to one of the following options:

- **NO** (Logger mechanism is not activated automatically on card startup)
- **YES** (Logger mechanism is activated automatically on card startup)

In addition, the AUTO_AUDIO_PLUS_LOGGER flag must be set to NO:

- **NO** (Logger mechanism is activated only as a response to IP Terminal command)

The files are created sequentially, cyclically, when the 100th file overwrites the first file and so on. Recommended mode is **NO** (manual card monitor).

The file names are generated automatically, containing the following components:

- Text: **ap_logger**
- Board ID number
- Unit ID number
- A serial number between 0 and 99, ascending sequentially

For example, a file could be named: **ap_logger 4 2 03** where **4** is the Board ID number, **2** is the Unit ID number and **03** is the serial number between 0 and 99.

Manual creation of the Audio+ logger files:

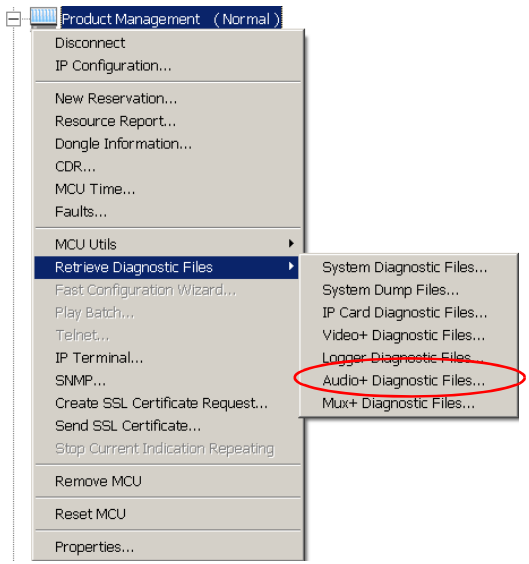
In the *IP Terminal* window, type the command:
ap_logger <board_id> <unit_id>

Where <*board_id*> is the Audio+ board slot number and <*unit_id*> is the mapped unit ID (0 for Card Manager).
For example, type **ap_logger 5 0**

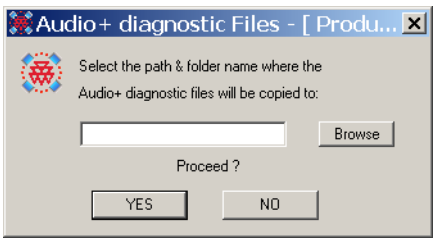
The file is stored in the MCU under the directory **7.256\mcu\ap_log**. This folder is automatically created by the system if it does not exist on the MCU.

Retrieving the Audio+ Logger files

1. Right-click the *MCU* icon, click **Retrieve Diagnostic Files**, and then click **Audio+ Diagnostic Files**.



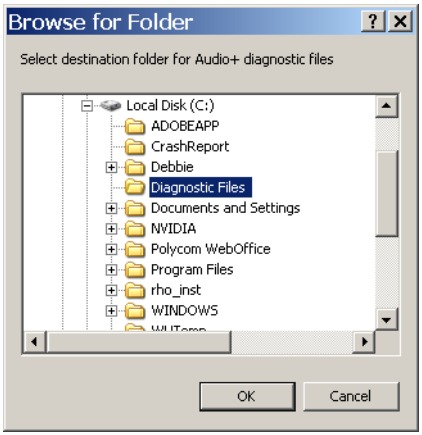
The *Audio+ Diagnostic Files* dialog box opens.



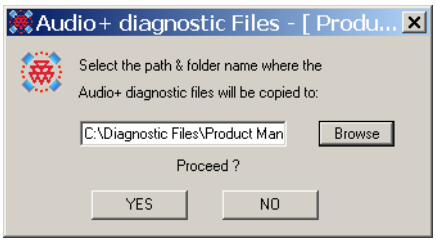
2. In the *Local path* box, type the path of the destination directory where the diagnostic file will be stored, or click **Browse** to select the destination folder.

The *Browse for Folder* dialog box opens.

3. Select the destination folder and then click **OK**.



The selected folder is displayed in the *Audio+ Diagnostic Files* dialog box.



4. In the *Audio+ Diagnostic Files* dialog box, click **Yes** to proceed.

   The Audio+ diagnostic file is saved in the <*MCU Name*>/ap_log sub-folder of the selected destination folder.

MUX+ Logger File

When an error occurs on the MUX+ card, a trace file is created automatically (if the appropriate option is selected in the system.cfg), or manually via IP terminal. The MUX+ trace file is automatically stored on the MCU and can be retrieved using the *Retrieve Diagnostic Files* utility. The file can then be analyzed to determine the problem.

MUX+ Logger File Structure

The files are stored under the folder: **7.256\mcu\muxp_log.** The MUX+ card diagnostic file header contains the following fields:

- Date and Time
- MCMS Version Number
- Board ID, component ID
- MUX+ component versions
  - — MNG_FILE (card manager)
  - — MUX_PLUS_PROC_FILE (processor)

The log data is comprised of Card Manager data and/or map log from a faulty unit. Each logger file can be up to 72 KB, including the header.

Creating the MUX+ Logger Files

The MUX+ logger file may be created automatically or manually.

Automatic creation of the MUX+ logger files:

The automatic creation of the MUX+ trace-capture file once a failure occurs is set in the “system.cfg” in the *MUX PLUS FLAGS* section, by setting the flag AUTO_MUX_PLUS_LOGGER to YES.
When setting this flag to NO, the automatic Logger utility is deactivated. The Logger files are created sequentially, cyclically, when the 100^{th} file overwrites the first file and so on. The file names are generated automatically with the following components:

- Text: **mpl**
- Board ID number (2 digits)
- Unit ID number (1 digit)
- A serial number between 0 and 99, ascending sequentially (2 digits)

For example, a file could be named: **mpl04203** where **04** is the Board ID number, **2** is the Unit ID number and **03** is the serial number.

Manual creation of the MUX+ logger files:

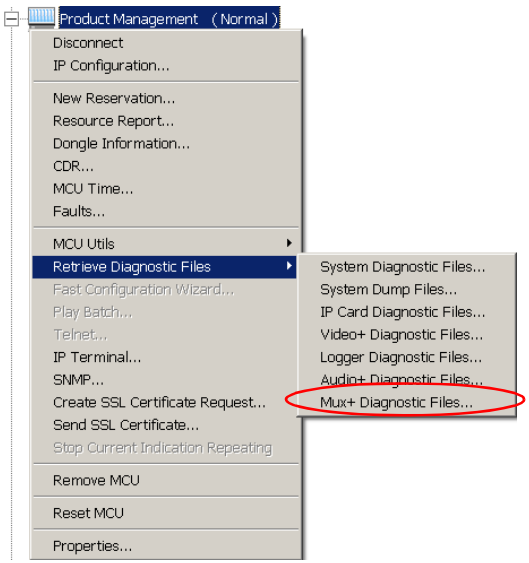
In the *IP Terminal* window, type the command:
mp_logger <board_id> <unit_id>

Where <*board_id*> is the MUX+ board slot number (in the MGC 25, the "logical" slot number as appears in the MGC Manager) and <*unit_id*> is the mapped unit ID (0 for Card Manager).
For example, type **mp_logger 3 2.**

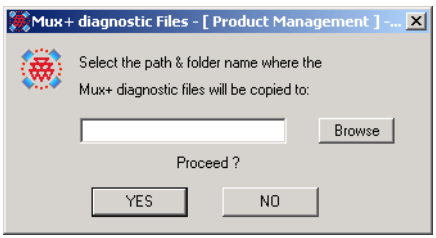
The file is stored in the MCU under the directory **7.256\mcu\muxp_log**. This folder is automatically created by the system if it does not exist on the MCU.

Retrieving the MUX+ Logger files

1. Right-click the MCU icon, click **Retrieve Diagnostic Files** and then click **Mux+ Diagnostic Files**.



The *Mux+ diagnostic Files* dialog box opens.

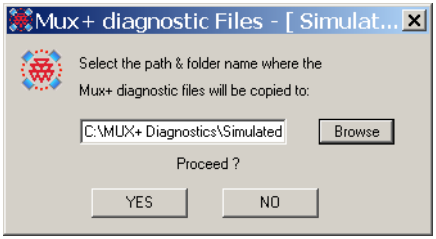


2. In the *Path* box, type the path of the destination directory where the diagnostic file will be stored, or click **Browse** to select the destination folder.

   The *Browse for Folder* dialog box opens.

3. Select the destination folder and then click **OK**.

   The <*MCU Name*>/muxp_log sub-folder of the selected destination folder is displayed in the *Mux+ Diagnostic Files* dialog box.



4. In the *Mux+ diagnostic Files* dialog box, click **Yes** to proceed.

   The MUX+ diagnostic file is saved in the <*MCU Name*>/muxp_log sub-folder of the selected destination folder.

Clocking

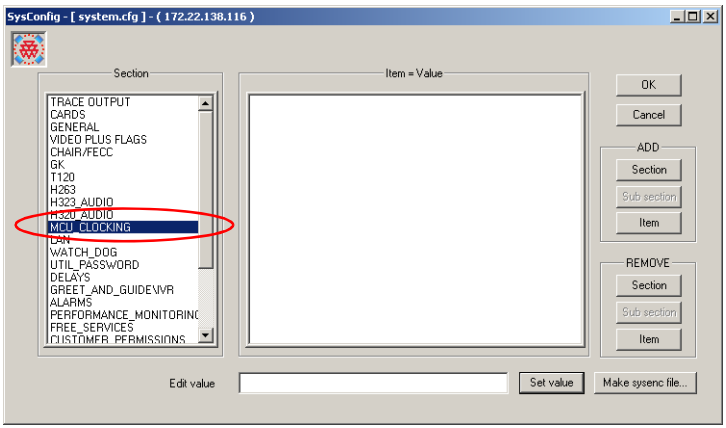
To be able to work with the network connected to the MCU you need to synchronize the system clock with the network clock. This is done in two steps:

- Selecting the network type according to which the system clock will synchronize. Only one system type may be selected for clocking.
- Selecting the spans of the selected network that will act as primary and backup clocks. The primary and the backup clock must be set on spans of the same network type.

Selecting the network type for clocking:

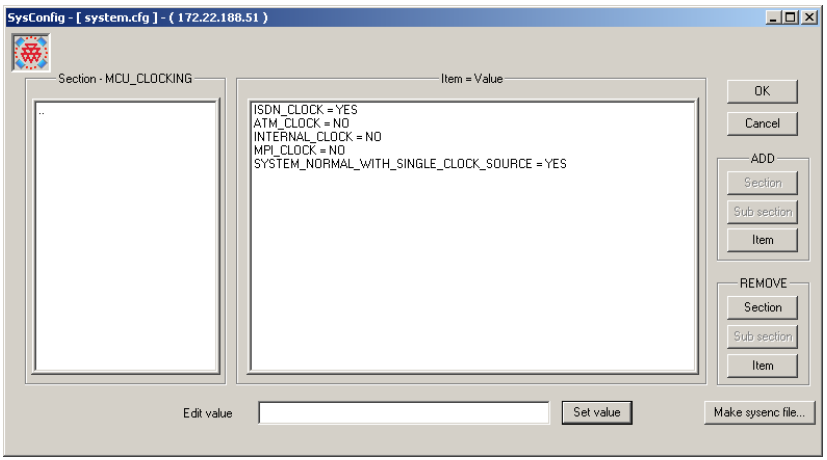
The network type to be used for clocking is selected in the "system.cfg" file.

1. Right click the MCU icon, click **MCU Utils** and then click **Edit "system.cfg"** from the cascading menu.
   The *SysConfig* dialog box opens.



2. In the *Section* box, double-click **MCU_CLOCKING**.

The list of network types that can be connected to the MCU is displayed in the *Item=Value* box.



3. Click on the network type to be used for clocking in the *Item = Value* box. The following table describes which network type should be selected for clocking when the MCU is connected to various networks.

Table 5-18: Clocking Options

Networks connected to the MCU	Network selected for clocking	Notes
ISDN only or ISDN with any of the following networks: ATM, H.323, MPI	ISDN	The primary and the backup clock must be set on spans of the same network type.
ATM only	Internal Clock	
H.323 only	Internal Clock	

Table 5-18: Clocking Options (Continued)

Networks connected to the MCU	Network selected for clocking	Notes
MPI only	MPI	The network clock is enabled only when the span coming from the DCE to the MCU is active (i.e. handles a call). Therefore, the spans defined as primary and backup clock must be connected first when starting a conference, and disconnected last when terminating the conference.
ATM and MPI	MPI	The network clock is enabled only when the span coming from the DCE to the MCU is active (i.e. handles a call). Therefore, the spans defined as primary and backup clocks must be active at all times (i.e. leased mode).

Only one Network type can be set for clocking.

4. In the *Edit Value* field, enter **YES** to enable it and click the **Set Value** button to apply it to the field.
5. Click **OK** to update the MCU with the changes.

For information about setting the primary and backup clocks, see "Assigning the ISDN Network Service to the Net-2/Net-4/Net-8 Card" on page 3-34.

Clocking in Serial Environment

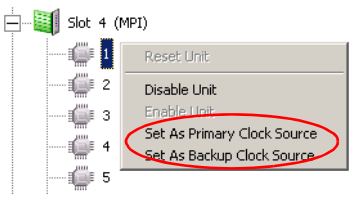
When the MCU is connected directly to both ISDN lines and serial lines, the MCU synchronizes its clock with the ISDN network clock.

In a serial only environment, the DCE, which is connected to a T1/E1 line, synchronizes its clock with the ISDN network clock. This clock is transferred via the serial connection to the MCU, but only when the serial connection is active (i.e. when it transfers a call to/from the MCU). Therefore, when starting a conference, the participant whose span is set as the primary clock must be connected first and disconnected last when terminating the conference as this participant provides the clocking signal for the system.

In a serial only environment, you must define one span as **Primary** clock and another span as **Backup** clock.

1. Connect to the MCU.
2. In the *Browser* pane click the plus [+]icon next to the *MCU* icon, to list its options.
3. Double-click the **MCU Configuration** icon, or click on the plus [+] icon next to the *MCU Configuration* icon, to list the *Configuration* options.
4. Double-click the *Cards* icon or click the plus [+]icon next to the *Cards* icon to list the MCU slots.
5. Double-click the slot containing the module you want to configure, or click the plus [+] icon next to the card icon.

   The MPI units are displayed in the *Browser* pane and in the *Status* pane.
6. Right-click the unit you want to configure, and then click the desired option.
   Select **Set As Primary Clock Source** or **Set As Backup Clock Source** according to the desired configuration.



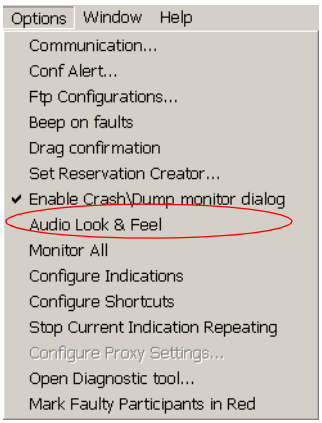
Audio Look & Feel

The MGC Manager controlling MGC units that are used for Audio Only conferences can be set to **Audio Look & Feel** to hide all video associated functions and show the Audio Only mode default settings.

When **Audio Look & Feel** is selected, the MGC Manager displays only Audio Only parameters. In all other configurations, the operator will be able to see both VoicePlus (Audio Only) and Video features.

To implement the Audio Only User Interface Settings:

- On the *Options* menu, click **Audio Look & Feel**.



A check mark appears next to **Audio Look & Feel**, indicating that this mode is active. All video related functions and dialog boxes are hidden.

To cancel the *Audio Look & Feel* mode and display the video parameters:

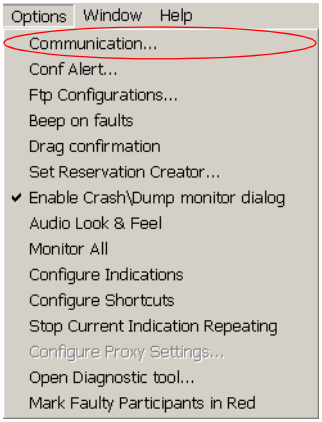
- On the *Options* menu, click **Audio Look & Feel**.

Setting the Default Communications Parameters

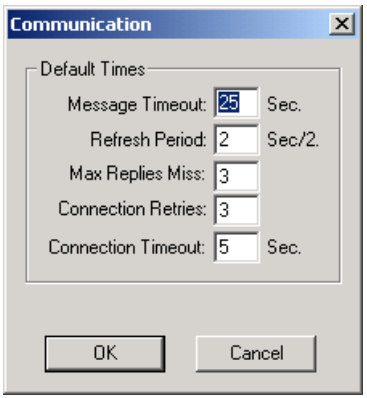
You can change the parameters that control the communication between the MGC Manager and the MCUs.

To set up the default communications parameters:

1. On the *Options* menu, click **Communication**.



The *Communication* dialog box opens.



2. Fill in the dialog box as follows:

Table 5-19: Communications Properties

Parameter	Description
Message Timeout	If no message is received from the MCU for the time period specified in this field, an error is triggered. The default value is 25 seconds. A higher value should be entered when the connection is slow or all the slots in the MCU are occupied. In these cases, the recommended value is 120 seconds.
Refresh Period	The frequency at which the MCU information in the MGC Manager screen is updated. The refresh rate is half of the seconds entered here. The default value is 2, which means that the information is refreshed every second (2/2=1).
Max Replies Miss	The number of messages that are sent and not received before a connection problem is triggered and the system considers the connection as lost.
Connection Retries	The number of times the MGC Manager attempts to establish a connection with an MCU following a disconnection, or connection loss. Minimum value should be 1.
Connection Timeout	The number of seconds the MGC Manager will wait after each connection attempt for connection confirmation. Default value is 5. Recommended value is 25.

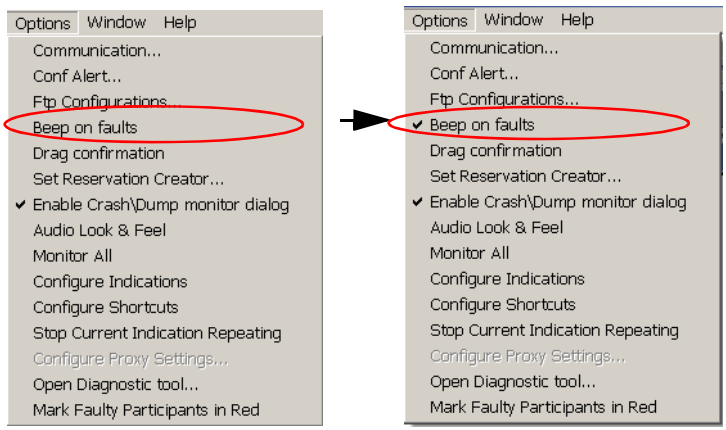
3. Click **OK**.

Faults Alert

You can set the operator workstation to beep continuously whenever a fault is detected. The system stops beeping once the fault is corrected. By default, this option is disabled.

To enable continuous beeping whenever a fault exists:

- On the *Options* menu, click **Beep on faults**.



A check mark appears next to the **Beep on faults** the next time you open this menu.

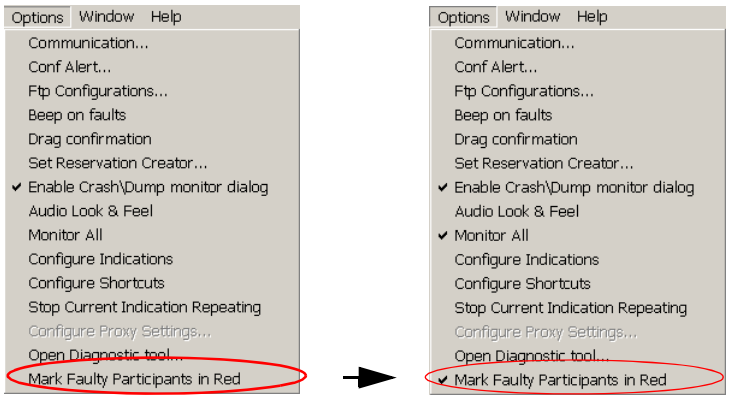
If no check mark appears next to the **Beep on faults** menu item, the feature is disabled.

Displaying Faulty Participants in Red

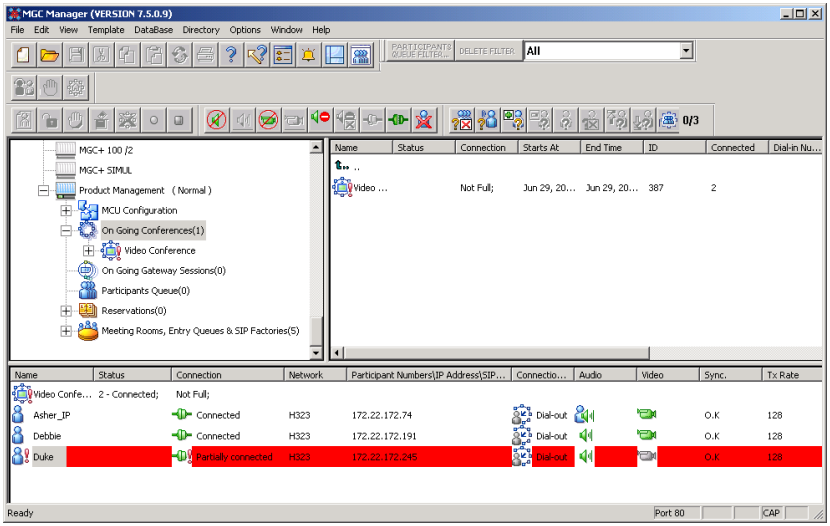
You can set the MGC Manager to highlight in red all participants that have a problem with their connection and require operator assistance.

To mark faulty participants in red:

- On the *Options* menu, click **Mark Faulty Participants in Red.**



A check mark appears next to the **Mark Faulty Participants in Red** the next time you open this menu. In the MGC Manager all participants requiring operator assistance are highlighted in red, as shown in the *Monitor* pane.



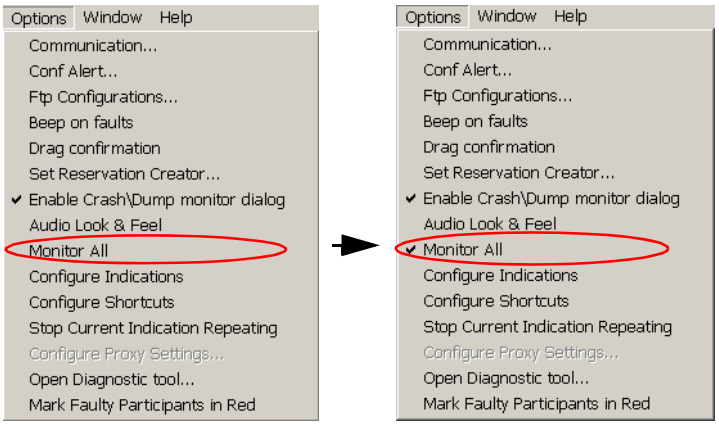
Monitoring All Conferences

You can set the MGC Manager to continuously monitor the participants that require the operator's assistance in all On Going Conferences.

The participants are monitored according to the last selected monitoring filter options for any of the On Going Conferences monitored by this operator.

To enable continuous monitoring of participants in all On Going Conferences:

- On the *Options* menu, click **Monitor All**.



A check mark appears next to the **Monitor All** the next time you open this menu.

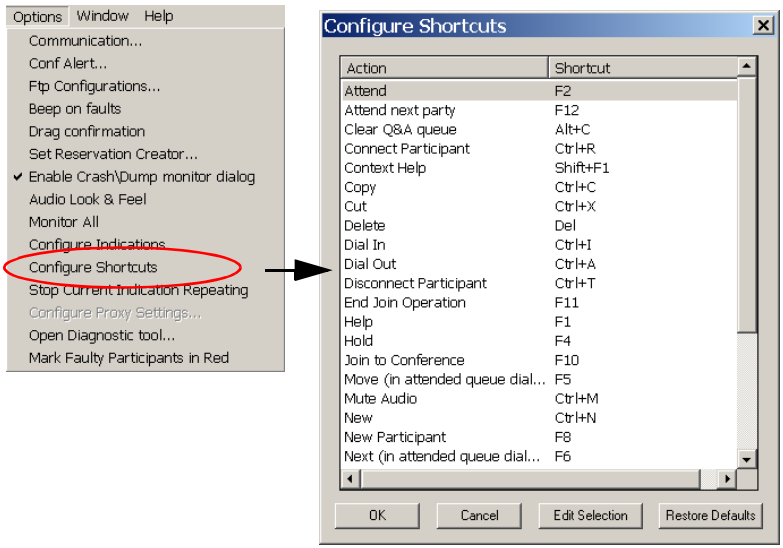
To modify the filter options, right click any *On Going Conference* icon and the click **Monitor Filter**.
The *Participants Monitoring Filter* dialog box opens. For details, see the *MGC Manager User's Guide, Volume I, Chapter 5, "Monitor Filter"*.

Configurable Shortcut Keys

MGC Manager user can configure the MGC Manager command shortcut keys for their convenience and usage. The list of shortcut keys may be sent to printer, file or clipboard (to be used with other applications). You may restore shortcut keys settings to their default values.

To configure command shortcuts:

On the *Options* menu, click **Configure Shortcuts**.
The *Configure Shortcuts* dialog box opens.



The following columns are displayed, listing the current settings in a table format.:

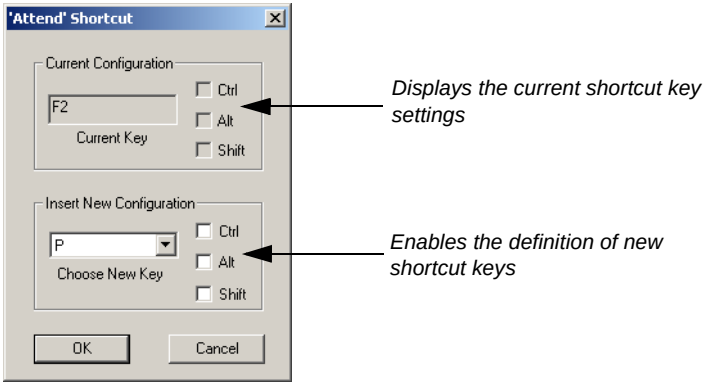
Table 5-20: Configure Shortcuts Dialog Box Columns

Column	Description
Action	Displays the list of features for which shortcuts can be configured.
Shortcut	Displays keyboard keys used to activate the functions.

4. In the *Configure Shortcuts* dialog box, highlight the shortcut to configure and click the **Edit Selection** button**.**

   Alternatively, double-click the shortcut to configure.

   The <*function name*> *Shortcut* dialog box opens.



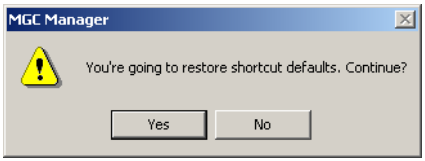
5. To define a new combination of keys, select a key from the *Choose New Key* drop-down list and add any combination of command keys (*Ctrl*, *Alt* or *Shift)*. Alternatively, you can type the appropriate key in the *Choose New Key* box and then select the appropriate command keys (*Ctrl*, *Alt* or *Shift*).

6. Click **OK**.
   The <*function name*> *Shortcut* dialog box closes and the new shortcut is displayed in the *Configure Shortcuts* dialog box.

To Restore the Shortcut Default Settings:

You may restore all Shortcut keys to their default settings in one operation.

1. In the *Configure Shortcuts* dialog box, click **Restore Defaults**.
   A confirmation dialog box opens.



2. Click **Yes**, to restore to the shortcut key to their default settings or **No** to retain current settings.

Audio Alert Event Indications

An audio alert event indicates to the operator that a particular event has occurred. The audio alert may be played repeatedly by the MCU until stopped by the operator.

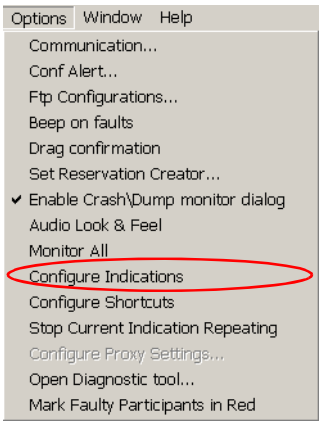
The first time the event occurs, the *Indications Log* window opens and records the event. The indications log can be saved to file.

Configuring Event Indications

You define for which MCUs the Event Indications are played. The *Indications Log* window displays all the events that occurred in all the connected MCUs for which the Event Indications are enabled.

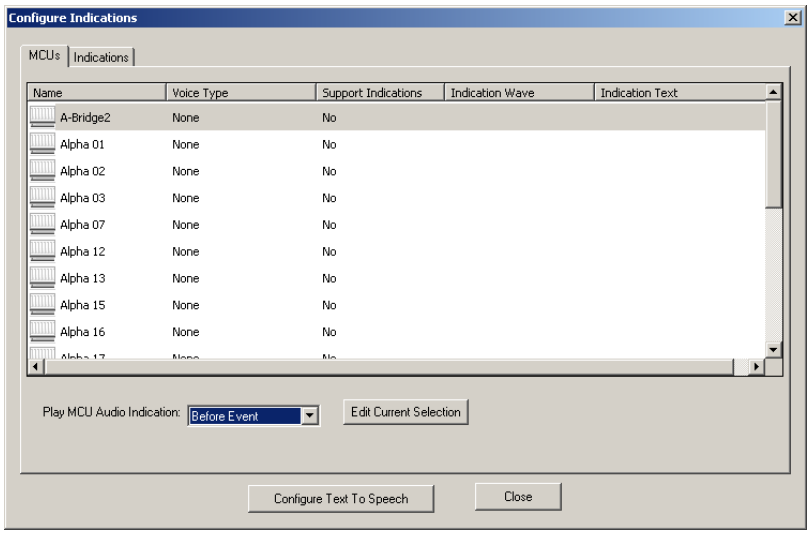
Enabling Event Indications:

1. On the *Options* menu, click **Configure Indications**.



Alternatively, click the *Configure Indications* button on the toolbar.

The *Configure Indications* dialog box opens.



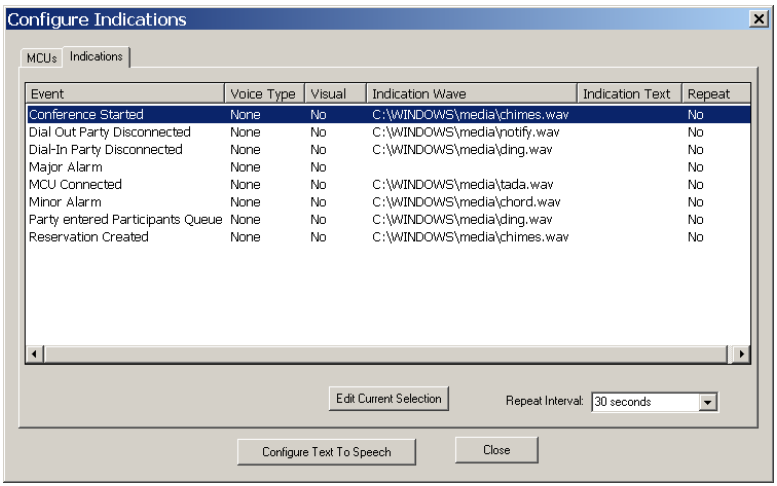
This window contains two tabbed dialog boxes:

- **MCUs** - enables you to determine the MCUs for which the Event Indication set defined in the Indications tab will be enabled. You can also add an MCU-specific indication that will be added before or after the event the Event Indication.
- **Indications** - enables you to define the set of Event Indications that will be played for the selected MCUs.

You can start the configuration process by first defining the Event Indications set and then selecting the MCUs for which the indications will be enabled, or you can start with the MCUs and continue with the Event Indications. The result will be the same at the end of the process.

2. Click the *Indications* tab to set the indications that can be played for the listed events.

The *Configure Indications–Indications* dialog box opens and all indications are displayed.



This dialog box lists in a table format the events for which the system currently supports audible indications.

For each event, the following information is displayed:

Table 5-21: Indications Window Columns

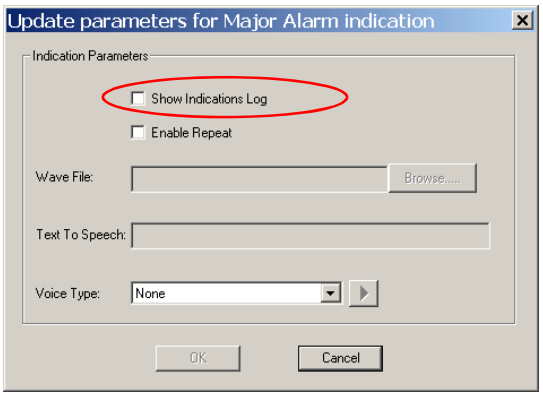
Column	Description
Event	Displays the list of events for which indications are supported. The following events are supported: • *MCU Connected* - The MGC Manager is connected to the MCU. • *Major Alarm* - The MCU status is Major and the Operator's attention is required. • *Minor Alarm* - The MCU status is Minor. • *Party Entered Participants Queue* - A participant entered the Participants Queue and requires the Operator's assistance. • *Dial Out Participant Disconnected* - A dial-out participant is disconnected from the conference and you may need to reconnect the participant to the conference.

Table 5-21: Indications Window Columns (Continued)

Column	Description
Event (cont.)	• *Dial In Participant Disconnected* - A dial-in participant is disconnected from the conference. • *Conference Started* - The conference has started. This notification may be important when a scheduled conference (reservation) has started at its pre-defined date and time. • *Reservation Created* - The system has added the requested reservation to memory.
Voice Type	Indicates whether an audio indication will be played and if yes, which type of audio indication. The following options are displayed: • *None* - No audio indication will be played when the event occurs. However, the event will be recorded in the event log file. • *Wave File* - A wave file will be played when an event occurs. The wave file is indicated in the *Indication Wave* column. • *Text To Speech* - To speak the text entered in the Indication Text field as the Event Indication. The voice parameters, speed and other options for text-to-speech translation is defined by clicking the **Configure Text To Speech** button.
Visual	Indicates whether the event will be recorded in the Indications Log and whether the Indications Log window will be displayed. If No is displayed, the event will not be recorded to the log file and the Indications Log window will not open when the event occurs.
Indication Wave	Displays the name and path of the wave file that will be played when the event occurs.
Indication Text	Displays the text that will be translated into voice.

3. In the *Indications* table, double-click the event for which you want to update parameters. Alternatively, select the entry and then click **Edit Current Selection** button.

   The *Update Parameters for <Event> Indication* dialog box opens.



4. Click the **Show Indication Log** check box to enable the Indication for the requested event. When enabled, each time the event occurs the system automatically opens the Indications Log window on top of all other windows, enabling you to view all the events that are recorded to the log file.
5. To play the indication repeatedly (until stopped by the operator), select the **Enable Repeat** check box.
6. In the *Voice Type* drop down list, select one of the following options:
   - **None** - to indicate that no audible alarm will be played and the event will only be recorded to the log file. If this option is selected, the *Wave File* and *Text-To-Speech* fields are disabled.
   - **Wave File** - to play a wave file when the event occurs. The wave file is selected in the *Wave File* field. If you select this option, the *Wave File* field is enabled and the *Text-To-Speech* field is disabled.
   - **Text to Speech** - to translate the text that you enter in the *Text-To-Speech* field into voice according to the translation parameters configured in the Text-to-speech utility parameters. If you select this option, the *Text-To-Speech* field is enabled and the *Wave File* field is disabled.

7. If the *Wave File* option is selected in the *Voice Type*, select the wave file that will be played when the event occurs.

   The *Wave File* field displays the default wave file assigned to the event. This file is taken from the Windows default wave files directory. To select another wave file, enter the path and name of the wave file to be used, or click the **Browse** button to select the file from the list.

   If you have selected the **Browse** button, the *Open* dialog box appears. Use Windows conventions to select the appropriate wave file.

8. If the *Text-To-Speech* option is selected in the *Voice Type*, in the *Text-To-Speech* field enter the text that will be translated into voice and spoken when the event occurs.

9. To play either the wave file or the text translated into voice (preview), click the **Play** button next to the *Voice Type* field.

10. Click **OK** to complete the Event Indication definition and return to the *Configure Indications–Indications* dialog box.

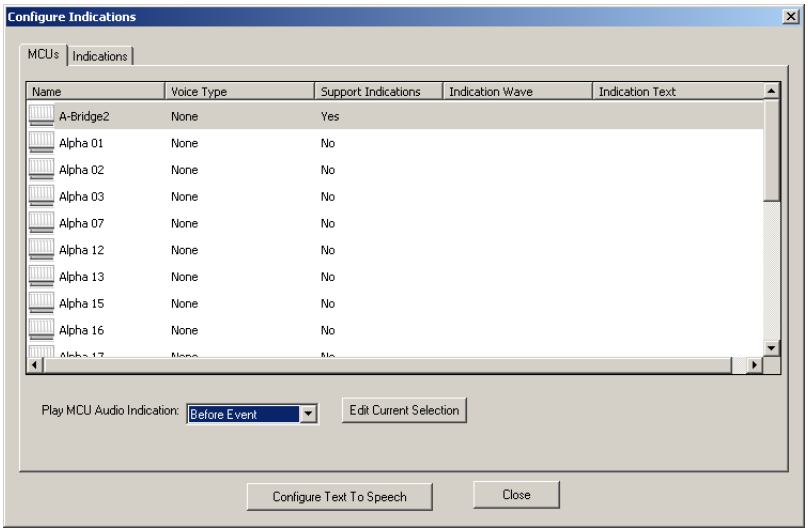
    The Indications table is updated accordingly.

11. Repeat steps 3 to 10 to define additional indications.

12. Select the **Enable Repeat Indications** check box to enable the Repeat interval field.

13. In the *Repeat Interval* drop down list, select the interval between the played indications.

14. Click the **MCU** tab to define the MCUs for which the Event Indications set, defined in the Indications dialog box, is enabled.



This dialog box lists in a table format whether the Event Indications set is enabled for the MCU and whether a specific MCU indication is added to the Event Indication. The following columns are displayed:

Table 5-22: MCU Indications Columns

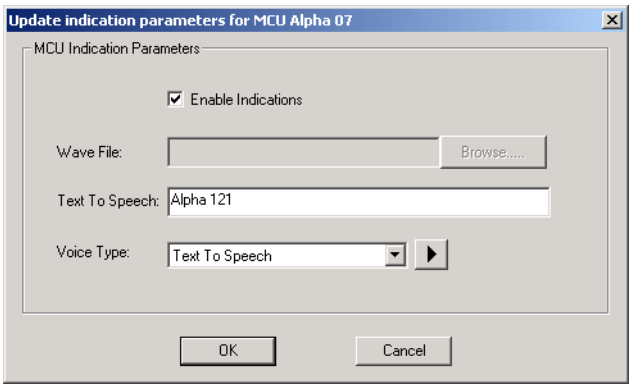
Column	Description
MCU	Displays the list of all MCU currently defined in the MGC Manager (connected and disconnected).

Table 5-22: MCU Indications Columns (Continued)

Column	Description
Voice Type	Indicates whether an MCU-specific audio indication will be played as the MCU indicator and, if yes, which type of audio indication. The following options are displayed: • *None* - No MCU-specific audio indication will be played when an event occurs. • *Wave File* - A wave file will be played as the MCU indicator when an event occurs. The wave file name is displayed in the *Indication Wave* column. • *Text To Speech* - To speak the text entered in the Indication Text field as the MCU indicator. The voice parameters, speed and other options for text-to-speech translation are defined by clicking the **Configure Text To Speech** button.
Support Indications	Indicates whether the Event Indications set is enabled or disabled for the MCU. When disabled, no event will be recorded and no audible indication will be played for this MCU.
Indication Wave	Displays the name and path of the wave file that will be played as the MCU indication when an event occurs.
Indication Text	Displays the text used as this MCU indicator that will be translated into voice and spoken when an event occurs.

15. To enable the Event Indications set for an MCU, click the MCU entry and then click the **Edit Current Selection** button. Alternatively, double-click the MCU entry.

The *Update Indication Parameters for MCU <MCU name>* dialog box opens.



16. Click the **Enable Indications** check box to enable the event Indications set for the selected MCU.
17. To add an MCU specific indication before or after the event indication, in the *Voice Type* drop down list, select one of the following options:
    - **None** - No MCU-specific audio indication will be played when an event occurs on this MCU. If this option is selected, the *Wave File* and *Text-To-Speech* fields are disabled.
    - **Wave File** - To play a wave file as an MCU indicator when the event occurs on this MCU. The wave file is selected in the *Wave File* field. If you select this option, the *Wave File* field is enabled and the *Text-To-Speech* field is disabled.
    - **Text To Speech** - To translate the text that you enter in the *Text-To-Speech* field into voice as an MCU indicator according to the translation parameters configured in the Text-to-speech utility parameters. If you select this option, the *Text-To-Speech* field is enabled and the *Wave File* field is disabled.
18. If the *Wave File* option is selected in the *Voice Type*, select the wave file that will be played as this MCU indicator when the event occurs on this MCU. Either enter the path and name of the wave file to be used in the *Wave File* field, or click the **Browse** button to select the file from the list.

    If you have selected the **Browse** button, the *Open* dialog box appears. Use Windows conventions to select the appropriate wave file.

19. If the *Text-to-speech* option is selected in the *Voice Type*, in the *Text-To-Speech* field enter the text that will be used as this MCU indicator and translated into voice when the event occurs on this MCU.
20. To play (preview) either the wave file or the text translated into voice, click the **Play** button next to the *Voice Type* field.

21. Click **OK** to complete the MCU Indication definition and the return to the *Configure Indications–MCU* dialog box.

    The MCUs table is updated accordingly.
22. Repeat steps 15 to 21 to define indications for additional MCUs.
23. In the *Play MCU Audio Indication* list, select whether the MCU indication will be played **Before** the Event indication or **After** the Event indication. The indication that will be played is composed of two parts: The MCU indication + The Event indication. For example, if the *Play MCU Audio Indication* option is set to *Before Event*, the voice-to-speech option is selected in the Voice type and you have entered the name of the MCU (such as Demo MCU) as text, the system will play “Demo MCU” first and then will play the Event Indication.
    This selection applies to all the listed MCUs.

To configure the voice parameters, speed and other options for the text-to-speech translation, click the **Configure Text To Speech** button to open the Speech Properties dialog box. Refer to Windows documentation or on-line help for additional information.

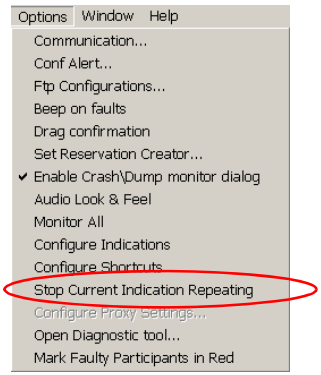
Click **Close** to complete the Event indications configuration.

To stop Repeated indications:

Event indications which are not repeated, are played once. Repeated indications will be played until stopped by the operator or when the event is no longer occurring. You can stop all the repeated indications for all connected MCU’s or you can stop the indications per MCU. When a new event occurs the indication is played again.

To stop all repeated Event Indications for all MCU's:

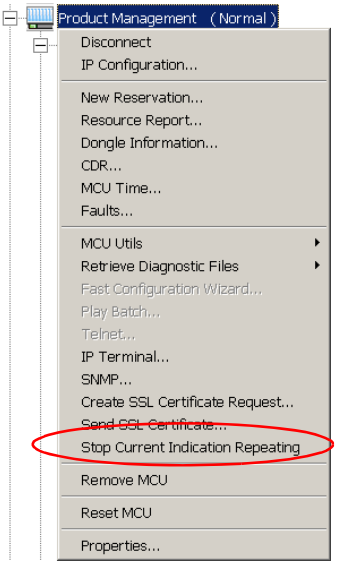
- On the *Options* menu, click **Stop Current Indication Repeating**.



All repeated indications are halted.

To stop all repeated Event Indications per MCU:

- In the *Browser* pane, right-click the MCU and then click **Stop Current Indications Repeating**.



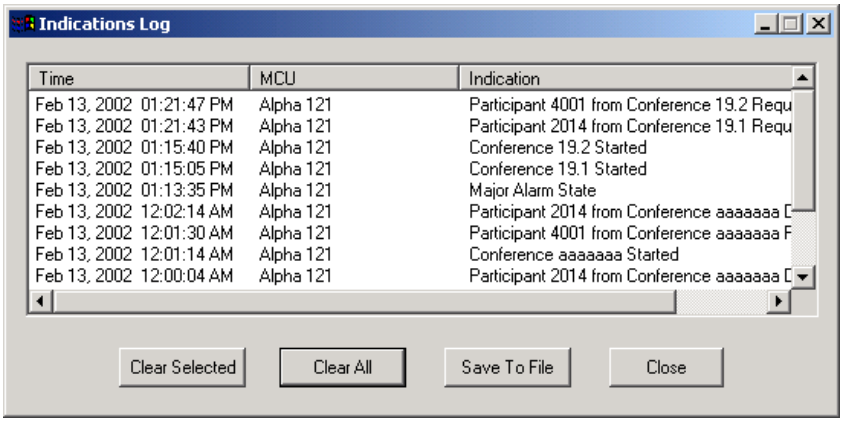
Repeated indications relevant to this MCU are stopped.

Viewing the Event Indications in the Indication Log Window

The *Indication Log* window automatically opens when an event occurs.

To manually open this window after it was closed, click **Indications Log** on the *View* menu or click the *Indications Log* button on the toolbar.

The *Indications Log* window opens.



The following columns are displayed:

Table 5-23: Indications Log Columns.

Column	Description
Time	The date and time on which the event occurred.
MCU	The name of the MCU on which the event occurred.
Indication	The event that has occurred with event details according to the event type, such as the conference name, participant name or MCU name.

Saving the Events Log to File

1. To save the event log to file, click the **Save Log File** button.
   The *Save As* dialog box opens.

2. Select the destination folder and define the file name.
   All files are saved in Text (*.txt) format and can be opened in any word processor application.

Clearing the Events Log

- To clear one entry in the Events Log, click the entry and then click the **Clear Selected** button.
- To clear all the events from the Events Log (after you have saved the events to file), click the **Clear All** button.

When closing the MGC Manager application, all the Event Indications will be deleted from the Indications Log and lost unless you save them to file before closing the application.

6

Defining Operators

The MGC Manager supports three levels of operators:

- Attendant
- Ordinary
- Superuser

Attendant operators can only define and manage new conferences, gateway sessions, meeting rooms, and participants. The Attendant operator does not have access to the MCU Configuration icon and MCU Utilities.

Ordinary operators can perform all the tasks an Attendant operator does. In addition, Ordinary operators can also view the configurations of the modules in the MGC-100 and the MGC-50.

Superuser operators can perform all the tasks Attendant and Ordinary operators do. In addition, Superuser operators can define and delete other operators, and define Network Services. While Ordinary operators can view the configurations of the modules in the MGC-100 and the MGC-50, only the Superuser operator can modify the configuration of a module.

You can verify which operators are defined in the system. This feature is available to both Superuser and Ordinary operators. Neither operator can view the operator passwords.

Working with operators involves the following:

- Listing the operators who are currently defined in the system
- Defining new operators
- Deleting operators

Note that every MCU is defined with a default operator, called POLYCOM, whose password is POLYCOM. You can log into any MCU using the POLYCOM operator. However, once you have defined other authorized operators, it is recommended to remove the default operator. Make sure that at least one operator defined as Superuser remains in the operator's list when removing operators.

Listing the Operators Defined in the System

You can view the list of operators that are currently defined in the system and the operators that are logged into the system.

To view the operators currently defined in the system:

1. In the *Browser* pane of the main window, double-click on the name of the MCU whose operators you wish to list.

   A list of options appears below the MCU's icon.

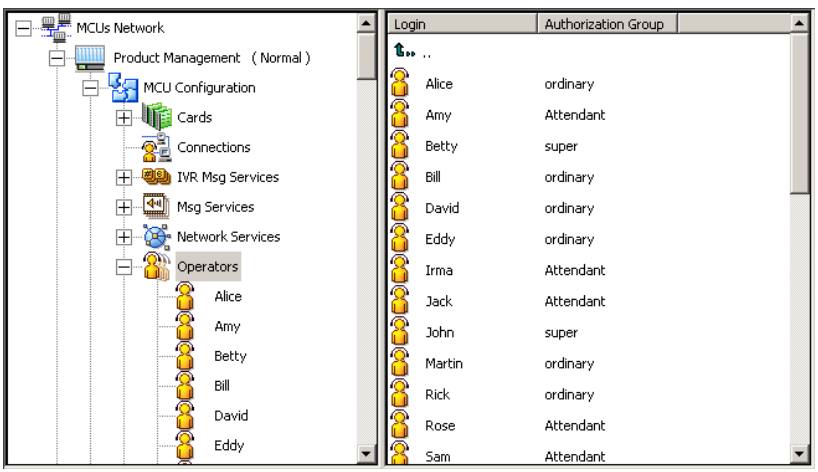
2. Double-click on the *MCU Configuration* icon, or click on the plus [+] icon next to the *MCU Configuration* icon to display the cascading list.

   A list of configuration options appears below the MCU Configuration icon.

3. Double-click on the *Operators* icon or click on the plus [+] icon next to the *Operators* icon.

   A list of operators appears below the *Operators* icon. Each operator is identified by his or her login name.

The operator's authorization level is displayed in the *Status* pane of the main window.



Adding a New Operator to the System

To add a new operator to the system:

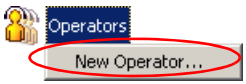
1. In the *Browser* pane of the main window, double-click the name of the MCU to which you want to add an operator.

   A list of options appears below the MCU's icon.

2. Double-click the *MCU Configuration* icon, or click the plus [+] icon next to the *MCU Configuration* icon to display the cascading list.

   A list of configuration options appears below the MCU Configuration icon.

3. Right-click the *Operators* icon, and then click **New Operator**.

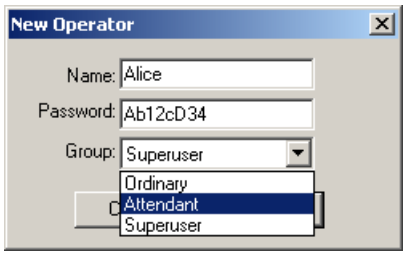


   The *New Operator* dialog box opens.

   In the *Name* text box, type the name of the new operator. The name you specify here is the login name used by the operator when logging into the system.

4. In the *Password* text box, type the new operator's password. The operator uses this password when logging into the system.

5. In the *Group* box, select the type of operator you are defining from the drop-down list.



   There are three types of operators:

   - *Attendant* - Can only perform the following tasks:

     —Define new conferences, gateway sessions, and meeting rooms

     —Define new participants

—Manage On Going Conferences

- *Ordinary* - In addition to all the tasks that can be performed by the Attendant operator, the Ordinary operator can also:

  — View the configurations of the modules in the MGC-50/100

- *Superuser* - In addition to all the tasks that can be performed by Attendant and Ordinary operators, the Superuser can:

  —Define and delete other operators

  —Define Network Services

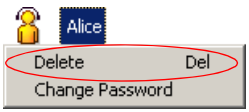
  —Modify the configuration of a module

6. Click **OK**.
   The *New Operator* dialog box closes and the new operator is added to the system. An icon for the new operator appears under the *Operators* icon.

To add a new operator, you must be a Superuser operator.

Deleting an Operator

1. Double-click the *Operators* icon or click on the plus [+] icon next to the *Connections* icon.
   A list of participants appears below the *Operators* icon. All operators currently connected to this MCU appear in the list.
2. Right-click the name of the operator to be deleted, and then click **Delete**.



   A confirmation message is displayed.
3. Click **Yes** to confirm or **No** to cancel the operation.
   If you select *Yes*, the operator name and icon are removed from the system.

To delete an operator, you must be a Superuser operator.

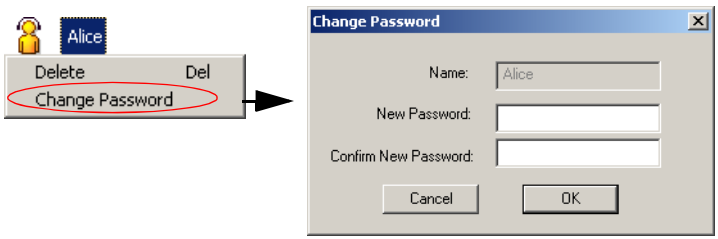
Changing an Operator's Password

A Superuser operator can change his/her own password and other operators' passwords. An Ordinary operator can change his/her own password.

Enable the "system.cfg flag" in the UTIL PASSWORD section ALLOW_ORDINARY_OPERATOR_TO_CHANGE_ITS_OWN_PASSWORD = YES prior to changing an Operators password. For more information, refer to Chapter 5, "Edit "system.cfg"" on page 5-64.

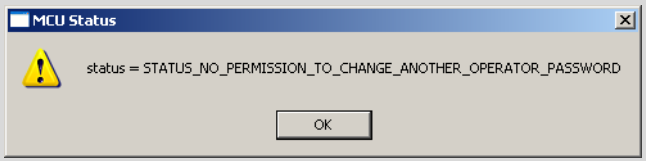
To change an operator's password:

1. Double-click the *Operators* icon or click on the plus [+] icon next to the *Connections* icon.
   A list of participants appears below the *Operators* icon. All operators currently connected to this MCU appear in the list.
2. Right-click the name of the operator to be deleted, and then click **Change Password**.
   The *Change Password* dialog box appears.



3. In the *New* text box, enter the new operator's password.
4. In the *Confirm New* text box, type confirm the new operator's password. Click **OK**.

When an ordinary operator attempts to change the password of another operator the following error message is displayed:



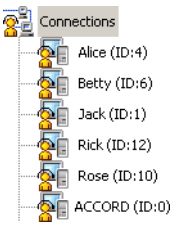
Operator Connections

In the MGC Manager you can list the operators who are currently logged into the MCU.

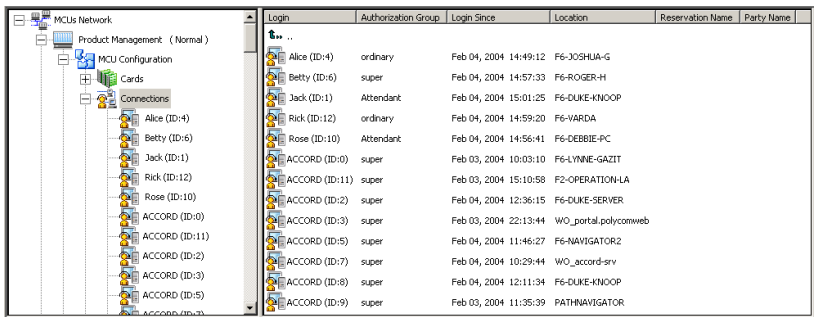
Viewing Operator Connections

To list the operators who are currently connected to the system:

1. Expand the MCU tree.
   A list of options appears below the MCU's icon.
2. Expand the *MCU Configuration* tree.
3. Expand the *Connections* tree.
   The list of operators currently connected to this MCU appears.



4. Click the *Connections* icon to display the operators details in the *Status* pane of the main window.



The information includes:

— The operator's login name and an ID number issued by the MCU. The ID is a sequential number starting with 0 allocated to each operator according to the order in which they logged in. The ID numbers are reset whenever the MCU is reset.

— The operator's authorization level (Ordinary, Attendant or Superuser)

— The time the operator logged in

— The location of the operator, which is the name by which the MCU identifies the operator's computer

Remote Operator Alert

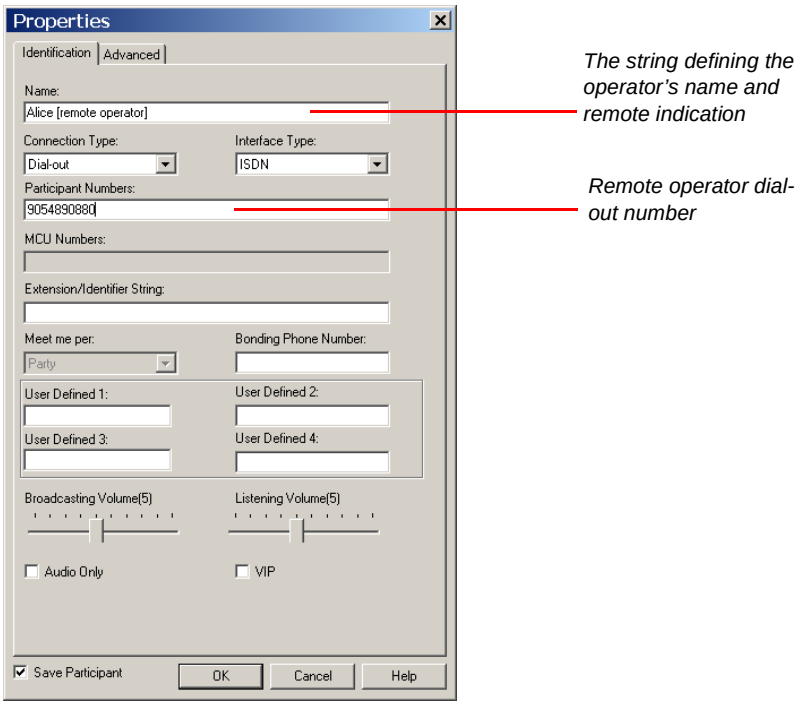
The system can be configured to contact an operator by dialing a phone number at a remote location when no operator is present at a local MGC Manager station. When a participant requests assistance or fails to logon, the participant enters the participants queue and waits to be assisted by the operator. Then, if configured, the MCU automatically dials out to the remote location.

The Remote Operator Alert requires the configuration of an Operator conference including the definition of a "participant". In this case the participant is an operator whose's name contains a string attached to the name that indicates to the system that the operator needs to be contacted at a remote location. The MCU dials out to the remote operator and a connection is established between the participant and operator.

Configuring a Remote Operator Alert Location:

1. Right-click the *Reservations* icon or *On Going Conferences* icon, and then click **New Operator Reservation** or **New Operator Conference**. The *Conference Properties - General* dialog box is displayed.
2. Define an *Operator* conference and click the **Participants** tab. The *Conference Properties - Participants* dialog box is displayed.

3. To define the participant, click the **New** button.
   The *Properties - Identification* dialog box opens.



   The string **name[remote operator]** as displayed in the *Name* field consists of the following format: <Free name text> [remote operator]. Each section of the string is explained below:

   — Text Field—Participant's name

   — Brackets [ ]—Brackets indicating a format string. Brackets are context sensitive and only this type of format can be used: [ ]

   — remote operator—This field is context sensitive and must be exactly presented as shown: **[remote operator]**

4. Finish the conference definition.

5. When a participant enters the *Participants Queue*, the system routes the call to the remote operator.

7

Configuring the Gateway

Overview

The GW-25/GW-45 Gateway is a network element within the H.320 and H.323 communications network. It provides connectivity across different physical networks and translates multiple protocols for point-to-point rich media communications.

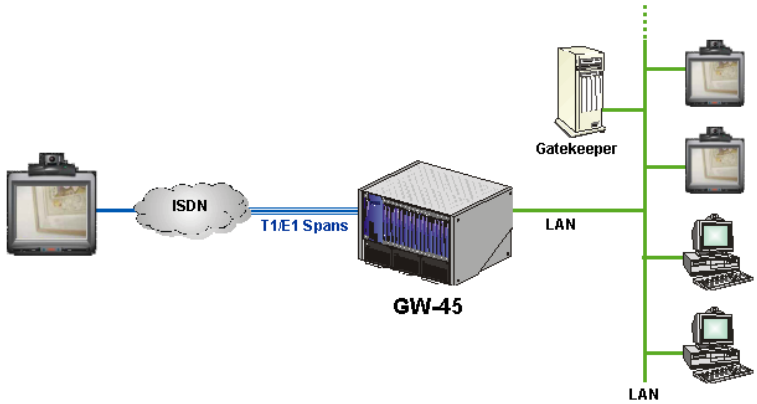


Figure 7-1: Typical Single Gateway Configuration

The GW-25/GW-45 can be connected to both H.320 (ISDN) and H.323 (IP) networks. The gateway configuration supports H.323-to-H.320, H.320-to-H.323 and H.323-to-H.323 point-to-point calls.

The GW-25/GW-45 supports the widest range of video and audio algorithms. It allows sites with different frame rates, connection speeds, audio algorithms, video resolutions and network protocols to transparently connect with one another. The transcoding abilities of the GW-25/GW-45 allow each endpoint to connect at its optimal capabilities.

The GW-25/GW-45 technology and system architecture are the same as those used in the MGC-50/MGC-100. The gateway can be configured on either an 8-slot (GW-25) or 16-slot (GW-45) chassis in a standalone gateway

configuration or as a combined MCU/Gateway configuration. The system can be configured to support a secured firewall gateway that can coexist with other gateway and MCU services on the same platform.

System administration of the MCU and the gateway are accomplished using the same MGC Manager application. This management application enables the system operator to view all the system resources for both the MCU and the gateway. The gateway can also be monitored via the network using SNMP.

The GW-45

The GW-45 is a 16-slot chassis that allow up to 48 concurrent point-to-point sessions in bandwidths ranging from 56 Kbps (audio only) to E1 (1920 Kbps). The GW-45 is a Carrier Class gateway that also provides a NEBS Level-3 compliance solution.

The GW-25

The GW-25 is an 8-slot chassis that allow up to 24 concurrent point-to-point sessions in bandwidths ranging from 56 Kbps (audio only) to E1 (1920 Kbps).

GW-25/GW-45 Main Features

The GW-25/GW-45, main features are:

- The gateway may be configured as standalone or in a shared resource configuration with the MCU
- Scale up to 48 Gateway sessions per gateway
- Connections speed up to E1 (1920 Kbps)
- Can be configured with ISDN/IP network interface supported (ISDN E1/T1 up to 1920 Kbps and Ethernet 10/100)
- Supports ITU video conferencing standards for video and audio
- Can provide a firewall gateway solution
- Can be monitored via the network using SNMP
- Supports Direct Inward Dialing (DID), routing H.320 incoming calls to H.323 endpoints
- Video Transcoding (when needed, requires additional hardware)
- BONDING standard
- Once configured, the Gateway works seamlessly without operator intervention
- Enables the operator to view the list of On Going Gateway sessions and assist participants if required
- H.239/People+Content support

An MCU that is configured as a gateway can forward DTMF tones. The DTMF support in Gateway Sessions is enabled in the system.cfg file in the GENERAL SECTION, by setting the ENABLE_DTMF_VIA_GW flag to YES.

System Specifications

The GW-25/GW-45 conforms to the following standards:

- Audio standards: G.711a, G.711u, G.722, G.723 (H.323 only), G.728, SIREN7, SIREN14
- Video standards: H.261, H.263, H.264
- Video resolution: CIF, QCIF
- Communication Standards: H.320, H.323
- Call setup standards: H.245 (H.323) and H.221 (H.320)
- Content standard: H.239
- Data Rates: Up to E1 (1920 Kbps)

Minimum Requirements

- MGC or Gateway
- H.323 Card (2 Cards required for IP to IP Gateway communications)
- ISDN Net Card (Requires minimum 1 PRI with a range of DID numbers)
- MUX Card
- Audio Card
- Video Card (Optional - for Transcoded calls)

Software Requirements

- MGC Version 4.00.XXX or above
- MGC Manager Version 4.00.XX or above

Network Requirements

- ISDN PRI line for H.320 Participants
- ISDN PRI line should have a range of 10 - 20 DID numbers available for Gateway communications
- Switched Ethernet connection to each H.323 card in the MCU
- 10/Half Ethernet connection for management of the MGC/Gateway
- Static IP address for the MGC/Gateway management port
- Static IP address for each H.323 Card installed on the system

Peripherals

You will need a Gatekeeper of some type: Polycom, Radvision, Cisco, MXM, etc. including:

- H.320-compliant Endpoints
- H.323-compliant Endpoints

Network Alias

- E.164 (Numeric Only)
- H.323 ID (Alpha-Numeric)

Protocol Requirements

The following table summarizes protocol requirements for Gateway communications.

Table 7-1: Protocol Requirements

Protocol/ Component	**H.323**	**H.320**
Call control	H.225.0	Q.931
System control	H.245	H.242/H.243
Multiplex	H.225.0	H.221
Audio	G.711, G.722, G.722.1, G.723.1, G.728, Siren7, Siren14	G.711, G.722, G.722.1, G.723.1, G.728, Siren7
Video	H.261 QCIF, H.263, H.264	H.261 QCIF, H.263, H.264
Dual Stream Mode	H.239	—

Calling Methods Using a Single Gateway

The GW-25/GW-45 gateway configuration supports H.323-to-H.320, H.320-to-H.323 and H.323-to-H.323 point-to-point calls. When an endpoint calls another endpoint, the dial-in number depends on the network used by the call initiator and on the method used to route the call. The Routing Method depends on the gateway configuration.

H.320 to H.323 Calls

A H.320 - H.323 gateway provides inter-working by providing the conversion of audio, video, data and control protocols as specified in the H.323 and H.320 system specifications.

When the H.320 endpoint calls the H.323 endpoint, three different methods may be used to reach the same endpoint: Destinations, Address Book and Forwarding Service.

Destinations

In the Destinations method, the carrier allocates the dial-in numbers to the MCU/Gateway. Usually the carrier only transfers part of the number (the last digits from the end of the number) to the gateway for example, 1501 to 1600. Each dial-in number is assigned to a specific destination H.323 endpoint. The destination H.323 endpoints will have to be configured according to the dial-in numbers allocated to the gateway using aliases in E.164 format. For example, if the dial-in number 1501 is allocated to an H.323 endpoint, the endpoint alias will have to be configured as 1501 in E.164 format. Each of the H.323 endpoints must register with the gatekeeper using its E.164 alias.

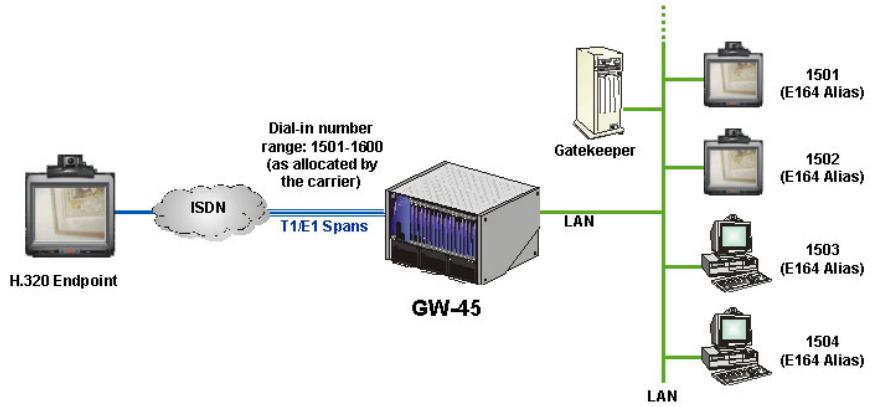


Figure 7-2: System Configuration Using Destinations

Using this method, the H.320 endpoint dials a number that is comprised of the gateway access number and the H.323 endpoint alias in E.164 format (step 1 in Figure 7-3). For example, when the H.320 endpoint dials 9251501, the digits 925 represent the gateway access number and 1501 represent the alias in E.164 format of the destination H.323 endpoint.

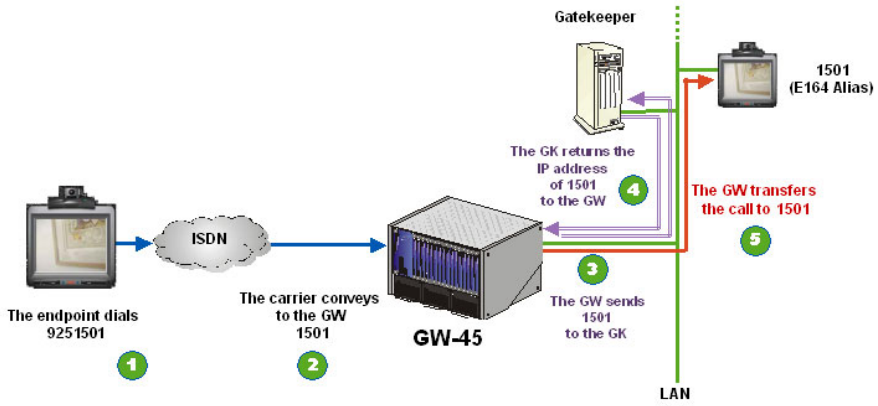


Figure 7-3: Destinations Call Flow

The carrier conveys the dial-in number to the gateway - 1501 in the example (step 2 in Figure 7-3). The gateway sends the dial-in number to the gatekeeper in order to locate the endpoint's IP address (step 3 in Figure 7-3). The

gatekeeper returns the IP address of the destination endpoint to the gateway (step 4 in Figure 7-3), which in turn transfers the call to the appropriate H.323 endpoint (step 5 in Figure 7-3).

Using this method, each configured endpoint has its own direct dial-in number; therefore the gateway requires the use of many dial-in numbers (at least as many as the number of H.323 endpoints). In addition, this method requires the presence of a Gatekeeper for address translation (E.164 alias to an IP address). If the H.323 endpoints were configured prior to the configuration of the gateway, the system administrator has to change the configuration of each endpoint and define a new alias according to the dial-in numbers allocated to the gateway by the carrier.

Address Book

In the Address Book method, the gateway includes a conversion table in which each DID number is assigned an alias or IP address of an H.323 endpoint. The carrier allocates the dial-in numbers to the MCU/Gateway, for example, 1701 to 1800. In Figure 7-4, “System Configuration Using Address Book”, the dial-in number 1721 is assigned to an H.323 endpoint whose alias is 501.

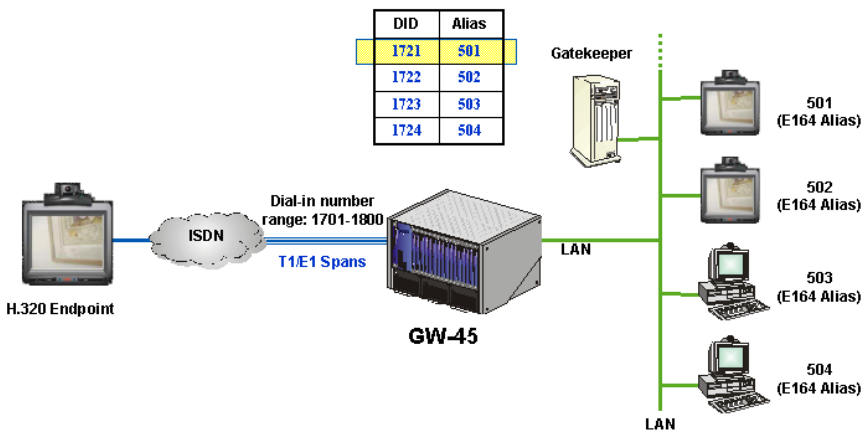


Figure 7-4: System Configuration Using Address Book

Using this method, the H.320 endpoint dials a number that is comprised of the gateway access number and the number that represents an entry in the Address Book; for example, 9251721, where 925 is the gateway access number and 1721 is the entry in the Address Book (step 1 in Figure 7-5, “Call

Flow Using the Address Book"). The carrier conveys the dial-in number to the gateway - 1721 in the example (step 2 in Figure 7-5).

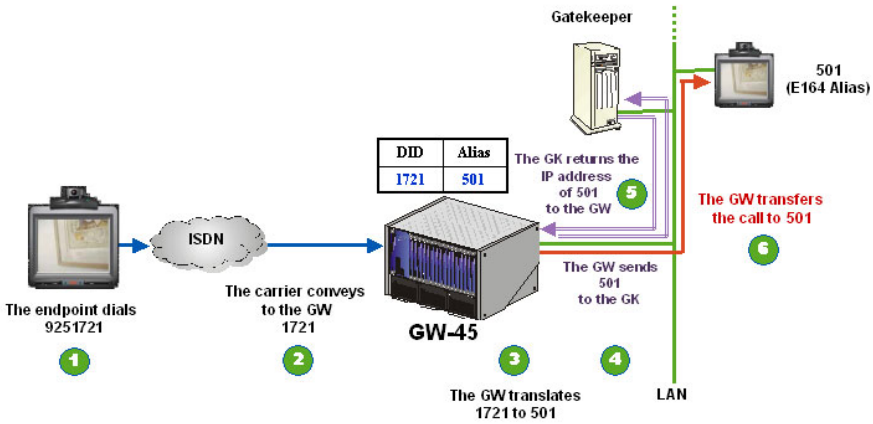


Figure 7-5: Call Flow Using the Address Book

The Gateway finds the appropriate entry in the Address Book (step 3 in Figure 7-5). If the Address Book contains the IP address of the destination endpoint, the call will be routed to the appropriate endpoint directly (step 6 in Figure 7-5). If the Address Book contains the alias of the endpoint for example, 501 in E.164 format, the alias is sent to the gatekeeper for address translation (step 4 in Figure 7-5). The gatekeeper returns the IP address of the endpoint to the gateway (step 5 in Figure 7-5). The gateway then routes the call to the appropriate endpoint.

In this method, each dial-in number is an entry in the speed dial table; therefore, the gateway will require the use of many dial-in numbers. If the conversion table includes the IP address of the endpoint, the gateway can route the call without the presence of a gatekeeper. To use the endpoint's alias, a gatekeeper must be present in the network. However there is no need to change the configuration of any of the H.323 endpoints.

Forwarding Service

In the Forwarding Service method, the administrator allocates a few dial-in numbers (from the range of dial-in numbers received from the carrier) to the MCU/Gateway, for example, 1815 to 1825; therefore, there cannot be an assignment between endpoints and dial-in numbers. Instead, the H.320

endpoint dials one number to access the gateway, and then enters the H.323 endpoint number (in E.164 format) using the TCS4 method.

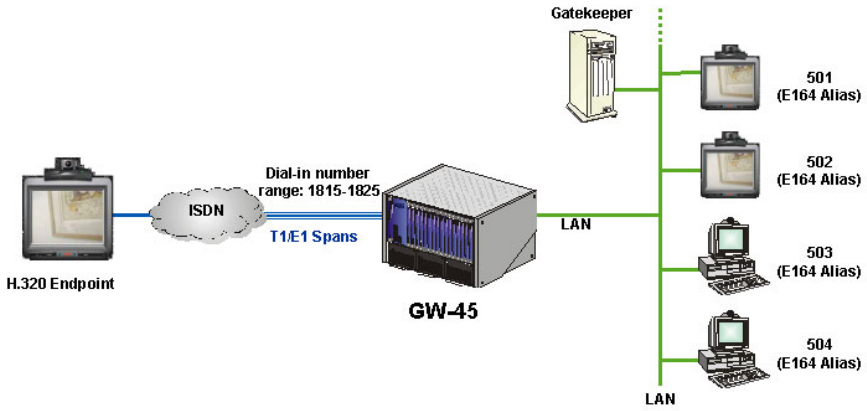


Figure 7-6: System Configuration Using Forwarding Service

Using this method, the H.320 endpoint dials a number that is comprised of the gateway access number, the forwarding service session identifier, the TCS4 indicator and the alias (in E.164 format) of the H.323 endpoint. For example, 9251815 (Note: On some H.320 endpoints there is a special TCS4 field where you add the 501 dial string, beside the phone number as shown in step 1 in Figure 7-7, “Call Flow Using Forwarding Service” where 9251815 represents the gateway access number. The TCS4 information is sent by the endpoint after its first channel synchronizes with the gateway.

The gateway identifies the TCS4 number 501 as the H.323 endpoint number and sends it to the gatekeeper for address translation (step 4 in Figure 7-7). The gatekeeper returns the IP address of the endpoint to the gateway (step 5 in Figure 7-7), which then transfers the call to the appropriate H.323 endpoint (step 6 in Figure 7-7).

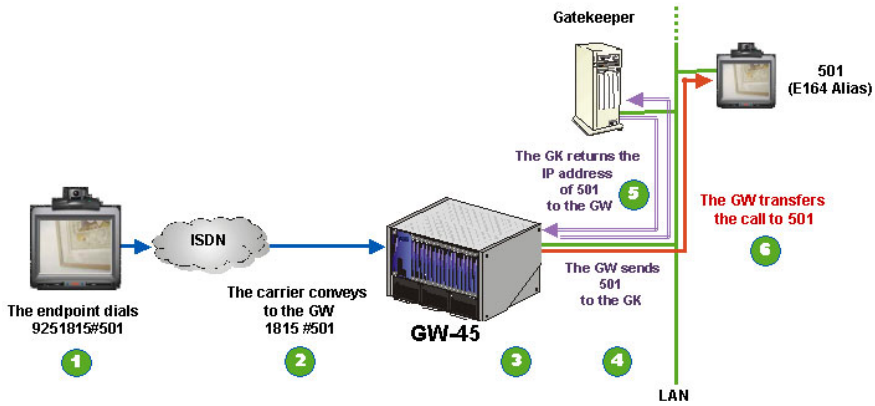


Figure 7-7: Call Flow Using Forwarding Service

In this method, only a few dial-in numbers (as little as one) may be used to access the gateway. One dial-in number may serve many H.323 endpoints. It does not require any additional configuration of the endpoints or the gateway. However, this method can only be used with H.320 endpoints that support TCS4. To use the endpoint's alias, a gatekeeper must be present in the network and the H.323 endpoints must register with the gatekeeper using their numeric aliases (E.164 format).

ISDN-IP Methods Summary

Table 7-2 summarizes the different methods that can be configured for the Gateway.

Table 7-2: ISDN-to-IP Methods Summary

	Destinations	Speed Dial	Forwarding Service
Method	Each dial-in number is assigned to one destination H.323 endpoint.	Each dial-in number is assigned to an entry in the speed dial table which is then translated to the H.323 endpoint address.	One single dial-in number may be used for all the gateway calls. The H.323 endpoint number is entered using TCS4.
Endpoint configuration	The system administrator must configure the H.323 endpoint aliases according to the dial-in numbers. Useful for new network installations.	No need to change the configuration of the H.323 endpoints. The conversion is done via the speed dial table. Useful for existing network installations.	No need to change the configuration of the H.323 endpoints. Useful for existing network installations.
Dial-in Numbers requirement	Requires the user to purchase many dial-in numbers.	Requires the user to purchase many dial-in numbers.	The user can purchase a dial-in number and many PRI lines.

H.323 to H.320 or H.323 Calls

When an H.323 endpoint calls an endpoint (H.323 or H.320), two different methods may be used to reach the same endpoint: Forwarding Service (H.323 to H.320) or Address Book.

With the Address Book method, the Gateway includes a conversion table in which each E.164 ID number is assigned either the phone number of an H.320 destination endpoint or an IP address or Alias of an H.323 endpoint. The Gateway also includes a table of Session Profiles. Each Session Profile describes the call parameters such as the network service to be used to dial to the destination endpoint, the line rate and the transcoding mode. Each entry in the table is identified by an E.164 format ID. When the call originator dials the E.164 ID, the gateway converts this ID to the destination endpoint dial number or IP address/Alias. The call parameters such as Line Rate, Restricted (ISDN only) and Transcoding Method are indicated by a Session Profile ID.

Address Book IP-to-ISDN

This method is used when an "Internal" IP endpoint calls an external ISDN number. It enables speed dialing as the IP endpoint only enters the endpoint ID in the table and does not have to enter the whole number (many digits). With the Address Book method, the Gateway includes a conversion table in which each E.164 ID number is assigned a destination H.320 (ISDN/PSTN) number. In this method, the destination endpoint details are taken from the Address Book table, enabling speed dialing from H.323 endpoints to ISDN endpoints.

In the following examples, the number 83 represents the H.323 Network Service prefix defined for the MCU and that is registered with the Gatekeeper. It is used by the Gatekeeper to identify the MCU and network cards that should be used to handle the call.

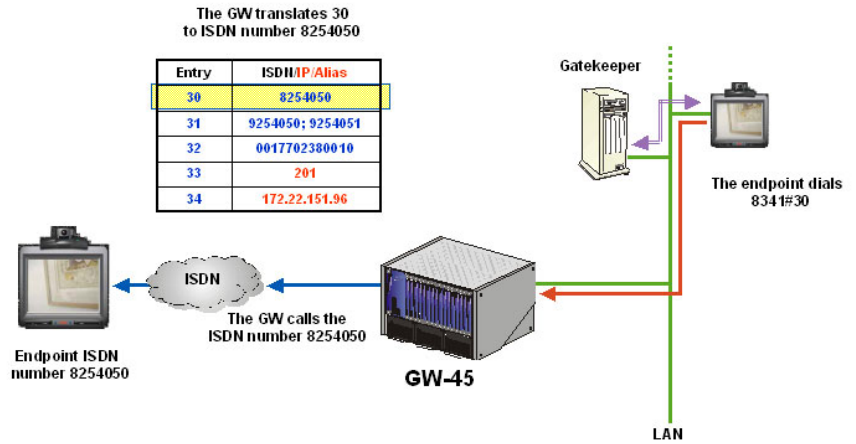


Figure 7-8: IP-to-ISDN System Configuration Using Address Book

For example, when the H.323 endpoint dials 8341#30 (step 1 in Figure 7-9, “IP-to-ISDN Call Flow Using Address Book”), the MCU Network Service prefix (as registered with Gatekeeper) is sent to the gatekeeper where the digits 83 are identified as the gateway prefix (step 2 in Figure 7-9) and the digits 41 as the Session Profile. The gatekeeper translates the prefix to the IP address of the gateway (step 3 in Figure 7-9). The call is transferred to the gateway with the digits 41and #30 (step 4 in Figure 7-9).

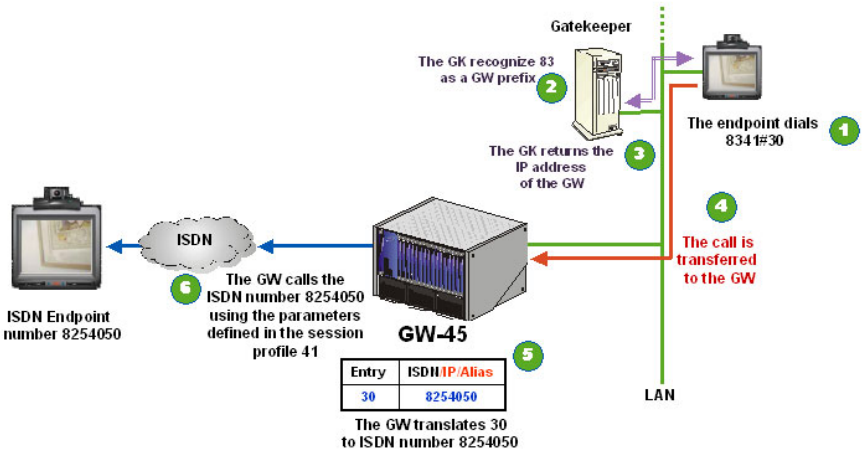


Figure 7-9: IP-to-ISDN Call Flow Using Address Book

The gateway uses 41 to identify the Session Profile to be used for calling the ISDN endpoint. It determines the call line rate, restricted and transcoding settings. The gateway identifies #30 as an entry in the Address Book table and translates this entry to 8254050 (step 5 in Figure 7-9). The gateway calls the number 8254050 using the parameters defined in the Session Profile identified by the digits 41and connects both endpoints (step 6 in Figure 7-9). Using this method, a gatekeeper must be present for address translation of the prefix and Session Profile to the gateway IP address.

Address Book IP-to-IP

In the Address Book method, the gateway includes a conversion table in which each E.164 ID number is assigned a destination alias or IP address. In this method, the destination endpoint details are taken from the Address Book table. It is used when an internal IP endpoint calls an external IP address through a firewall.

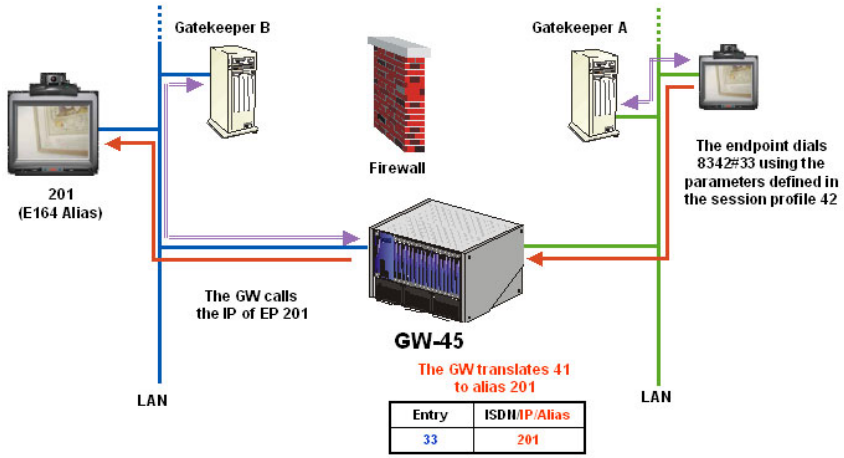


Figure 7-10: IP-to-IP System Configuration Using Address Book

For example, when the H.323 endpoint dials 8342#33 (step 1 in Figure 7-11, "IP-to-IP Call Flow Using Address Book"), the number is sent to the gatekeeper A where the digits 83 are identified as the gateway prefix (step 2 in Figure 7-11). Gatekeeper A translates the prefix to the IP address of the gateway (step 3 in Figure 7-11) and sends this address to the endpoint. The call is transferred to the gateway with the digits 42#33 (step 4 in Figure 7-11).

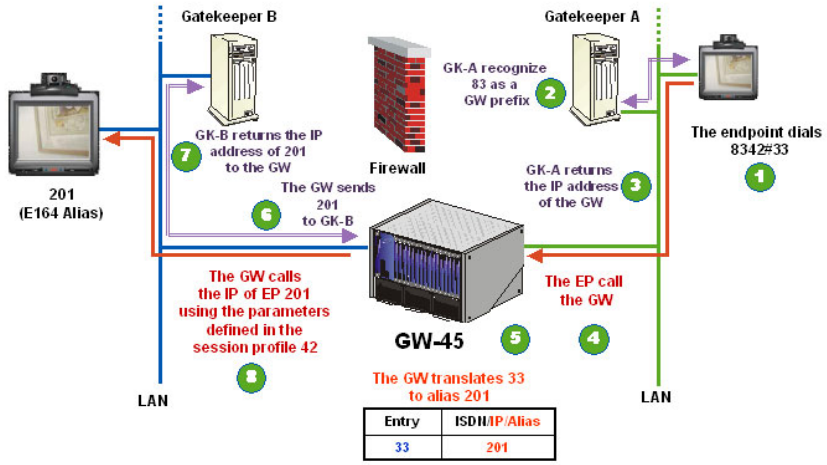


Figure 7-11: IP-to-IP Call Flow Using Address Book

The gateway identifies #33 as an entry in the Address Book table and translates this entry to alias 201 (step 5 in Figure 7-11). The gateway sends the alias 201 to gatekeeper B for address translation (step 6 in Figure 7-11). Gateway B returns the IP address of the endpoint to the gateway (step 7 in Figure 7-11) using the parameters defined in the Session Profile 42. The gateway calls endpoint 201 and connects the endpoint to the video conference (step 8 in Figure 7-11).

In this method, all H.323 endpoints on the network can call any H.323 endpoint when two gatekeepers (one in each zone) are present. The H.323 endpoints must register with the gatekeepers using their numeric aliases (any selected format). This enables gateway sessions over firewalls without changing the organization network configuration or compromising its security.

Session Profile IP-to-ISDN

In this method, the destination endpoint number and the gateway session configuration details are transferred to the gateway in the dialed number.

The H.323 endpoint dials the gateway prefix and the H.320 number (step 1 in Figure 7-12, "IP-to-ISDN Call Flow Using Session Profile"), for example, 8390*8254050.

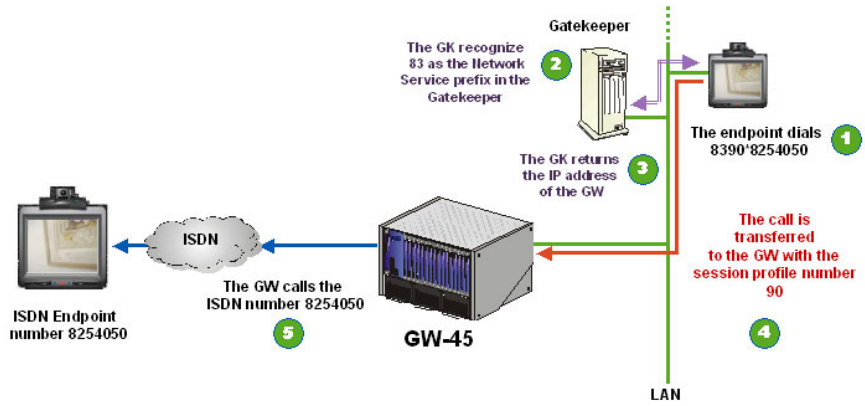


Figure 7-12: IP-to-ISDN Call Flow Using Session Profile

The Prefix 83 needs to be configured in the Gatekeeper and is listed in the H.323 Network Service as the prefix. The indicated asterisk (*) is the delimiter and the digits 8254050 represent the destination endpoint ISDN number. The number is sent to the gatekeeper where the digits 83 identify the gateway (step 2 in Figure 7-12**)**. The gatekeeper returns the IP address of the gateway (step 3 in Figure 7-12) to the endpoint. The call is then routed to the gateway (step 4 in Figure 7-12) including the ISDN number of the destination endpoint. The gateway dials the ISDN number and connects the endpoint to the conference (step 5 in Figure 7-12) using the call parameters defined in the Session Profile whose ID is 90.

Session Profile IP-to-IP

In this method, endpoint details are transferred to the gateway in the dialed number. It is used when an internal H.323 endpoint calls an external IP address.

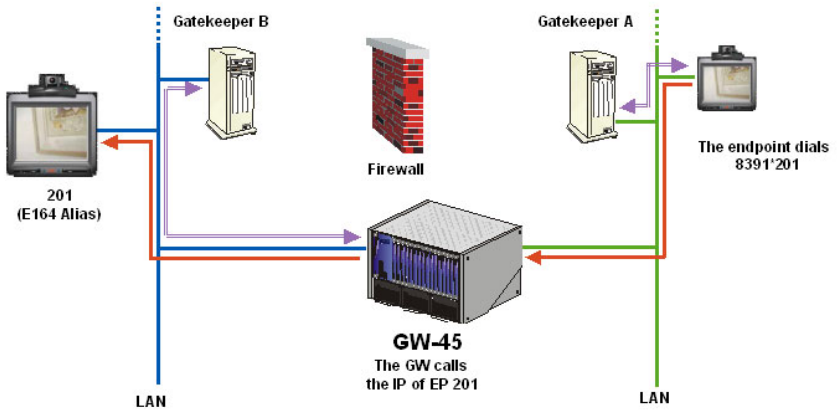


Figure 7-13: IP-to-IP System Configuration Using Session Profile

The H.323 endpoint dials the gateway prefix, profile identifier and the H.323 alias in E.164 format (step 1 in Figure 7-14, “IP-to-IP Call Flow Using Session Profile”), for example, 8391*201.

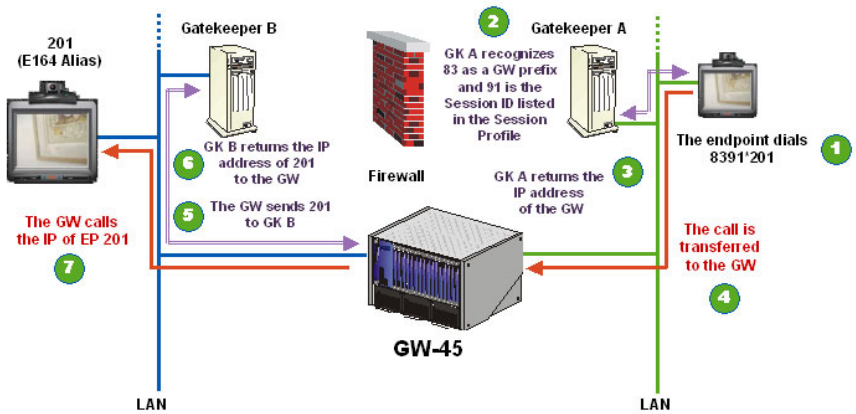


Figure 7-14: IP-to-IP Call Flow Using Session Profile

The Prefix 83 needs to be configured in the Gatekeeper and in the H.323 Network Service and the gateway prefix, which is also the entry number for the Forwarding Service. 91 is the Forwarding Service ID listed in the Session Profiles. The indicated asterisk (*) is the delimiter and the digits 201 represent the alias of the H.323 destination endpoint in E.164 format. The

number is sent to the gatekeeper A where the digits 83 identify the gateway (step 2 in Figure 10-14). Gatekeeper A returns the IP address of the gateway to the endpoint (step 3 in Figure 7-14). The call is then routed to the gateway (step 4 in Figure 7-14) including the alias of the destination endpoint (201). The gateway sends the alias 201 to gatekeeper B for address translation (step 5 in Figure 7-14). Gatekeeper B returns the IP address of the endpoint to the gateway (step 6 in Figure 7-14). The gateway connects the H.323 endpoint to the session (step 7 in Figure 7-14) using the call parameters defined in the Session Profile 91.

In this method, all H.323 endpoints on the network can call any H.323 endpoint when two gatekeepers (one in each zone) are present. The H.323 endpoints must register with the gatekeepers using their numeric aliases (E.164 format). This enables the gateway sessions over firewalls without changing the organization network configuration or compromising its security.

Table 7-3: IP-to-IP/ISDN Methods Summary

	Address Book	**Profile**
Method	The H.323 endpoint dials the gateway prefix and the ID (E.164 format) of the entry in the Address Book. The entry is translated to the ISDN number or IP address/Alias of the endpoint.	The H.323 endpoint dials the profile (same as gateway prefix) and the ISDN number or IP address/Alias of the endpoint. Each network service and configuration requires its own Profile.
Configuration	The conversion table must be defined in the gateway. Enables speed dialing to the ISDN endpoints.	No need to configure any of the numbers prior to calling. Endpoint details are transferred to the gateway in the dialed number.
Notes	Only pre-configured numbers can be used.	Any ISDN number or Alias can be dialed without special configuration of the endpoint.

TCS4 for Two Single Gateways

TCS4 Protocol can be implemented when calling from an H.323 endpoint to H.323 endpoint using two single gateways.

An H.323 endpoint (A) dials the gateway using the profile: [prefix ID] [profile ID]*[remote gateway # (DID)] # E.164 (alias type) of the remote endpoint.

The TCS4 for Two Single Gateways format: [prefix ID] [profile ID] * [remote gateway # (DID)] # E.164 (alias type) of the remote endpoint, has been changed in version 5.0.

The H.323 participant A dials 8390*8254050#1234 where 83 is the prefix ID (local gateway), 90 is the profile ID (local gateway), 8254050 is the remote gateway number (DID for the remote gateway for the Forwarding Service) and 1234 is the E.164 alias of participant B.

The local Gateway queries the remote gateway where the routing service has a pre-configured dial-in number (DID). The remote gateway sends a TCS4 request to local gateway. The local gateway translates the E.164 string into TCS4 and sends it to the remote gateway. The remote gateway translates the TCS4 message into the E.164 alias and connects the call to the remote H.323 endpoint (B).

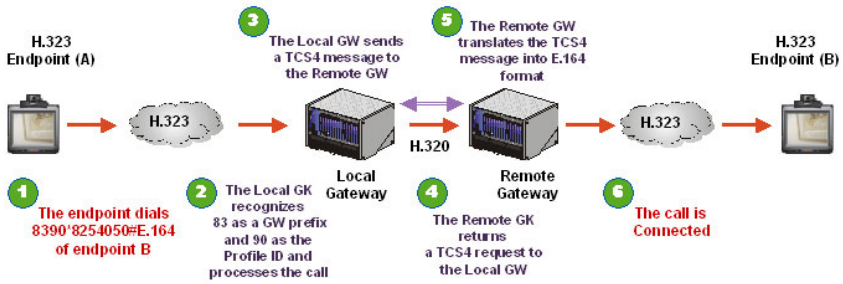


Figure 7-15: TCS4 for Two Single Gateways

Calling Methods Using the Double Gateway

The Double Gateway can perform six basic call directions:

- H.320 Endpoint over H.323 Backbone to H.323 Endpoint
- H.323 Endpoint over H.323 Backbone to H.320 Endpoint
- H.320 Endpoint over H.323 Backbone to H.320 Endpoint
- H.323 Endpoint over H.323 Backbone to H.323 Endpoint
- H.323 Endpoint over H.320 Backbone to H.323 Endpoint

With an H.320 backbone you cannot initiate a double gateway call from an ISDN endpoint, since a single gateway does not support an H.320 to H.323 call.

When an endpoint calls another endpoint, the dial-in number depends on the network used by the call initiator and on the method used to route the call. The Routing Method depends on the way the gateways are configured. In a Double Gateway communications setup, the Remote Gateway Definition and Gateway Link require configuration according to the Routing Method that is to be implemented.

Gateway Configuration - General Settings

When using the double gateway you are required to use the same settings for both the local and remote gateway.

It is strongly recommended that default settings are used for the Speed dial indicator (Address Book indicator) and the Multiple-number Delimiter (Profile indicator).

H.323 to H.323 to H.320/H.323 Calls

When a H.323 endpoint calls an endpoint (H.323 or 320), two different methods may be used to reach the same endpoint: Profile or Address Book.

H.323 Endpoint Over an H.323 Backbone to H.320 Endpoint, Using Profiles

In this method, the endpoint number and the gateway session configuration details are transferred to the gateway in the dialed number.

The H.323 endpoint connects using the following string: [**local GW prefix**, **first GW Link ID**]*****[**ISDN No.**], for example, 7011*1234.

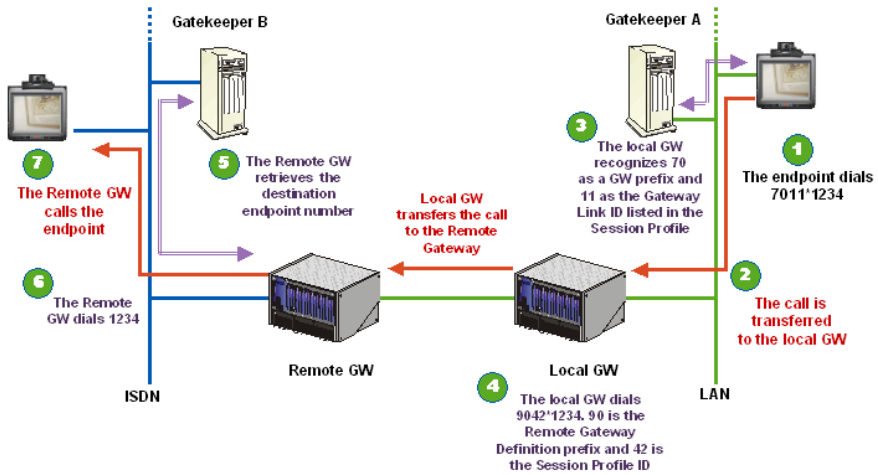


Figure 7-16: IP-to-ISDN Over H.323 Backbone Call Flow Using Profile

Step 1. The H.323 endpoint dials 7011*1234 representing the gateway prefix, the Gateways Link ID, the Delimiter and ISDN number as shown in the above example.

The digits 70 represent the local gateway prefix defined in the Network Service Properties and 11 is the local Gateway Link ID retrieved from the Gateway Link.

Step 2. The local gateway automatically dials the remote gateway using the string 9042*1234.
The digits 90 represent the remote gateway (H.323) ID prefix taken from the local Gateway Link. The Remote Gateway H.323 profile ID, 42, represents the configured Session Profile (ID E.164) parameter defined in the *To H.320 Session Profile Definition* dialog box. The * is the Delimiter defined in the *Gateway Configuration - General Settings* dialog box. 1234 is the dialed ISDN number and represents the destination endpoint number.

Step 3. The remote gateway dials 1234 and connects the call.

H.323 Endpoint Over an H.323 Backbone to H.323 Endpoint, Using Profiles

In this method, endpoint details are transferred to the gateway using pre-configured numbers. It is used when an local H.323 endpoint calls the remote H.323 endpoint.

The H.323 endpoint connects using the following string: [**local GW prefix**, **first GW Link ID**]*[**Alias**], for example, 7011*1234

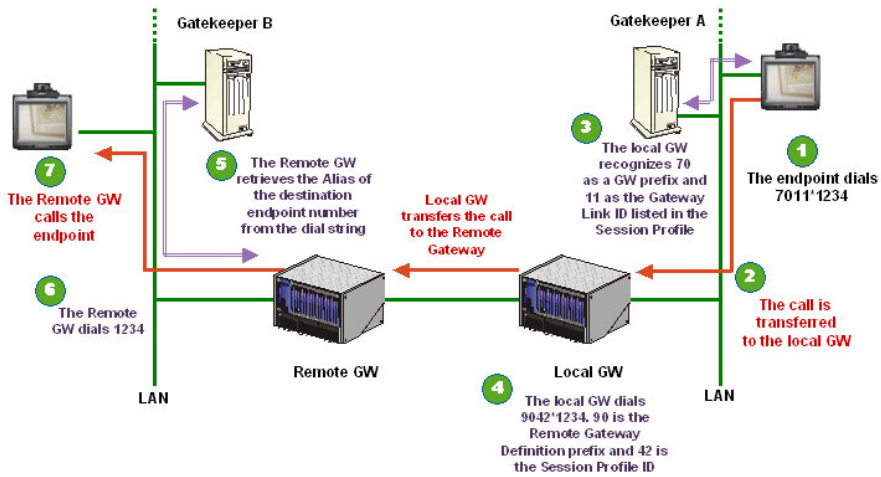


Figure 7-17: IP-to-IP Over H.323 Backbone Call Flow Using Profile

Step 1. The H.323 endpoint dials 7011*1234 representing the gateway prefix, the Gateways Link ID, the Delimiter and Alias as shown in the above example.

The digits 70 represent the local gateway prefix defined in the Network Service Properties and 11 is the local Gateway Link ID retrieved from the Gateway Link.

Step 2. The local gateway automatically dials the remote gateway using the string 9042*1234. The digits 90 represent the remote gateway (H.323) prefix taken from the local Gateway Link. The Remote Gateway H.323 profile ID, 42, represents the configured Session Profile (ID E.164) parameter defined in the *To H.323 Session Profile Definition* dialog box. The * is the Delimiter defined in the *Gateway*

Configuration - General Settings dialog box. 1234 is the Alias retrieved from the dial string and represents the destination endpoint.

Step 3. The remote gateway dials 1234 and connects the call.

H.323 Endpoint Over an H.323 Backbone to H.320 Endpoint, Using the Address Book

In the Address Book method, the gateway includes a conversion table in which each E.164 ID number is assigned a destination H.320 (ISDN/PSTN) number. In this method, the destination endpoint details are taken from the Address Book table. It is used when an internal IP endpoint calls an external ISDN number.

The H.323 endpoint connects using the following string: [**local GW prefix**, **first GW Link ID**]*[**ISDN No.**], for example, 7011*1234.

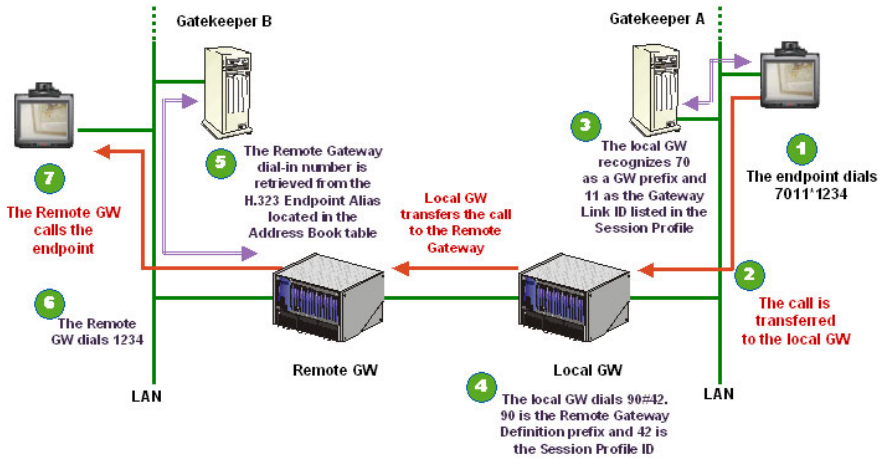


Figure 7-18: IP-to-ISDN Over H.323 Backbone Call Flow Using Address Book

Step 1. The H.323 endpoint dials 7011*1234 representing the gateway prefix, the Gateways Link ID, the Delimiter and ISDN number. The local gateway dials the remote gateway using the string 7011*1234.

The digits 70 represent the local gateway prefix defined in the Network Service Properties and 11 is the local Gateway Link ID retrieved from the Gateway Link.

With the Address Book method, the gateway includes a conversion table in which each E.164 ID number is assigned a destination phone

number. In this method, the destination endpoint details are taken from the Address Book table.

Step 2. The local gateway automatically dials the remote gateway using the string 90#42. The digits 90 represent the remote gateway (H.323) prefix taken from the local Gateway Link. The Remote Gateway H.323 profile ID, 42, represents the configured Session Profile (ID E.164) parameter defined in the *To H.320 Session Profile Definition* dialog box. The # is the Speed Dial indicator (Address Book field) defined in the *Gateway Configuration - General Setting*s dialog box.

Step 3. The remote gateway retrieves the endpoint ISDN number from the Address Book table and connects the call.

H.323 Endpoint Over an H.323 Backbone to H.323 Endpoint, Using the Address Book

In the Address Book method, the gateway includes a conversion table in which each E.164 ID number is assigned a destination alias or IP address. In this method, the destination endpoint details are taken from the Address Book table. It is used when an internal IP endpoint calls an external IP address.

The H.323 endpoint connects using the following string: [**local GW prefix**, **first GW Link ID**]*****[**Alias**], for example, 7011*1234.

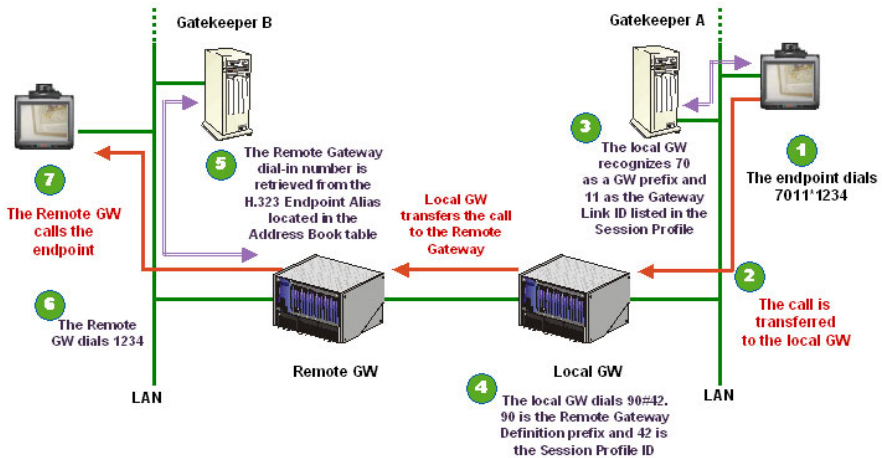


Figure 7-19: IP-to-IP Over H.323 Backbone Call Flow Using Address Book

Step 1. The H.323 endpoint dials the gateway prefix, the Gateway Link ID, the Delimiter and Alias.

The digits 70 represent the local gateway prefix defined in the Network Service Properties and 11 is the local Gateway Link ID retrieved from the Gateway Link.

With the Address Book method, the gateway includes a conversion table in which each E.164 ID number is assigned a destination alias. In this method, the destination endpoint details are taken from the Address Book table.

Step 2. The local gateway automatically dials the remote gateway using the string 90#42. The digits 90 represent the remote gateway (H.323) prefix taken from the local Gateway Link. The Remote Gateway H.323 profile ID, 42, represents the configured Session Profile (ID E.164) parameter defined in the *To H.323 Session Profile Definition* dialog box. The # is the Speed Dial indicator (Address Book field) defined in the *Gateway Configuration - General Settings* dialog box.

Step 3. The remote gateway retrieves the endpoint Alias from the Address Book table and connects the call.

H.323 to H.320 to H.323 Calls

When an H.323 endpoint calls an H.323 endpoint two different methods may be used to reach the same endpoint: Forwarding Service or Address Book/ Destinations.

H.323 Endpoint Over an H.320 Backbone to H.323 Endpoint, Using the Address Book

In this method, the destination endpoint number and the gateway session configuration details are transferred to the gateway in the dialed number.

The H.323 endpoint connects using the following string: [**local GW prefix**, **first GW Link ID**]*, for example, 7011*.

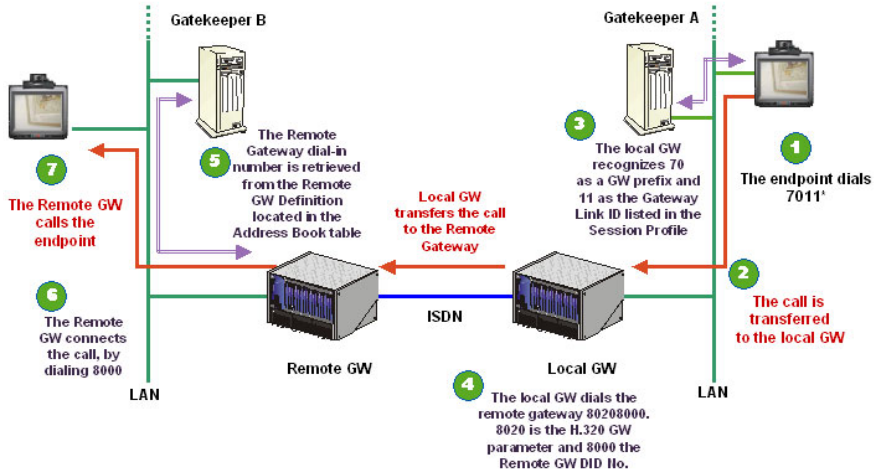


Figure 7-20: IP-to-IP Over H.320 Backbone Call Flow Using Address Book

Step 1. The H.323 endpoint dials 7011* representing the gateway prefix, the Gateway Link ID and the Delimiter.

The digits 70 represent the local gateway prefix defined in the Network Service Properties and 11 is the local Gateway Link ID retrieved from the Gateway Link.

With the Address Book method, the gateway includes a conversion table in which each E.164 ID number is assigned a destination alias. In this method, the destination endpoint details are taken from the Address Book table.

Step 2. The local gateway automatically dials the remote gateway using the string 80208000. 8020 is the H.320 Gateway Parameter (access PRI number) taken from the Remote Gateway Definition and 8000 the Remote Gateway DID number taken from the Gateway Link. The digits 8000 represent the destination endpoint alias in H.323 format.

The Address Book - Endpoint Definition dialog box contains the Destination Identifier whose configuration is set to H.323 endpoint and is defined in the H.323 Endpoint Parameters settings. The H.323 Endpoint Parameters settings define the Alias Type, Alias Name and IP Address.

Step 3. The remote gateway uses the Address Book to find the H.323 phone number 8000 as defined in the Remote Gateway Definition. Using the Dial string the remote gateway finds the entry and dials 8000 the destination endpoint.

H.323 Endpoint Over an H.320 Backbone to H.323 Endpoint, Using Destinations

In this method, the destination endpoint number and the gateway session configuration details are transferred to the gateway in the dialed number.

The H.323 endpoint connects using the following string: [**local GW prefix**, **first GW Link ID**]*, for example, 7011*.

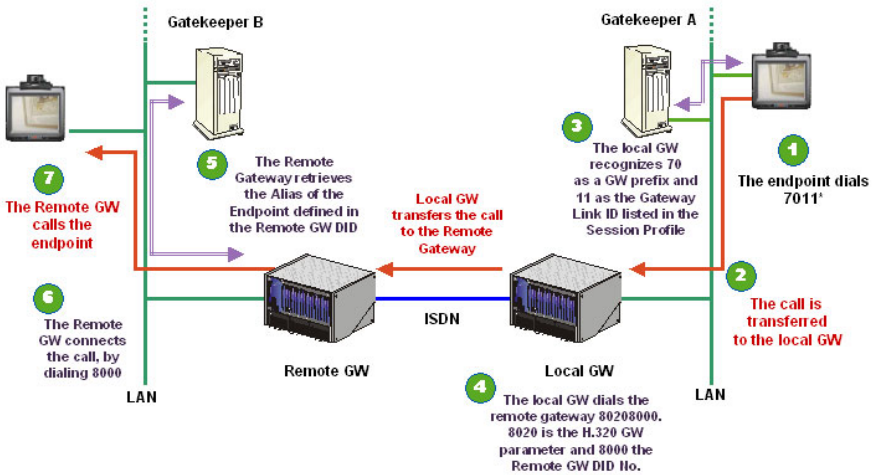


Figure 7-21: IP-to-IP Over H.320 Backbone Call Flow Using Destinations

Step 1. The H.323 endpoint dials 7011* representing the gateway prefix, the Gateways Link ID and the Delimiter.

The digits 70 represent the local gateway prefix defined in the Network Service Properties and 11 is the local Gateway Link ID retrieved from the Gateway Link.

In this method, endpoint details are transferred to the gateway which includes a conversion table in which each E.164 ID number is assigned a destination alias. Endpoint details are transferred to the

gateway using pre-configured numbers. It is used when an local H.323 endpoint calls the remote H.323 endpoint.

Step 2. The local gateway automatically dials the remote gateway using the string 80208000. 8020 is the H.320 Gateway Parameter (access PRI number) taken from the Remote Gateway Definition and 8000 the Remote Gateway DID number taken from the Gateway Link. The digits 8000 represent the destination endpoint alias in H.323 format.

Step 3. The Remote Gateway Definition contains the Alias H.323 of the remote endpoint and locates the phone number 8000 as defined in the Remote Gateway DID. Using the Dial string the remote gateway finds the entry and dials the endpoint.

H.323 Endpoint Over an H.320 Backbone to H.323 Endpoint, Using Forwarding Services

The H.323 endpoint connects using the following string: [**local GW prefix**, **first GW Link ID**]***** [**Alias**], for example, 7011*1234.

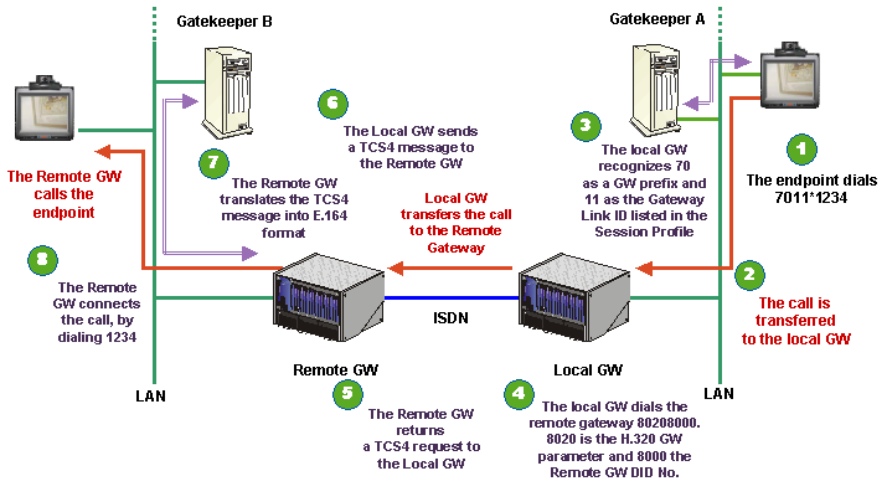


Figure 7-22: IP-to-IP Over H.320 Backbone Call Flow Using Forwarding Service

Step 1. The H.323 endpoint dials 7011*1234 representing the gateway prefix, the Gateways Link ID, the Delimiter and Alias.

The digits 70 represent the local gateway prefix defined in the Network Service Properties and 11 is the local Gateway Link ID

retrieved from the Gateway Link. The indicated asterisk (*) is the Delimiter and the digits 1234 represent the destination Alias.

Step 2. The local gateway automatically dials the remote gateway using the string 80208000. 8020 is the H.320 Gateway Parameter (access PRI number) taken from the Remote Gateway Definition and 8000 the Remote Gateway DID number taken from the Gateway Link. The digits 8000 represent the destination endpoint alias in H.323 format. The local Gateway queries the remote gateway where the routing service has a pre-configured dial-in number (DID). The remote gateway has no information but the Forwarding Service knows that it has to request the string from the local gateway using the TCS4 channel. The local gateway translates the E.164 string into TCS4 and sends it to the remote gateway.

Step 3. The remote gateway translates the TCS4 message into E.164 format and connects the call to the remote H.323 endpoint. The remote gateway forwards the Alias by retrieving the H.323 dialup sting that has been stored at the local gateway. The local gateway sends the string to the remote gateway and connects the call to the endpoint dialing 1234.

H.320 to H.323 to H.320/H.323 Calls

When an H.320 endpoint calls an endpoint (H.323 or H.320), two different methods may be used to reach the same endpoint: Address Book or Profile.

With the Address Book method, the carrier allocates the dial-in numbers to the MCU/Gateway. Usually the carrier only transfers part of the number (the last digits from the end of the number) to the gateway, for example, 1001 to 1600. Each dial-in number is assigned to a specific destination H.323 or H.320 endpoint. The destination H.323 or H.320 endpoints will have to be configured according to the dial-in numbers allocated to the gateway using aliases in E.164 format. For example, if the dial-in number 1001 is allocated to an H.323 endpoint, the endpoint alias will have to be configured as 1001 in E.164 format. Each of the H.323 endpoints must register with the gatekeeper using its E.164 alias. The H.323 endpoint dials the gateway prefix with the H.323 alias in E.164 format; for example, 11118291*90#42.

H.320 Endpoint Over an H.323 Backbone to H.323 Endpoint, Using Address Book

The H.320 endpoint connects using the following string: [**Dial-in No.**][**Link DID**], for example, 43218071.

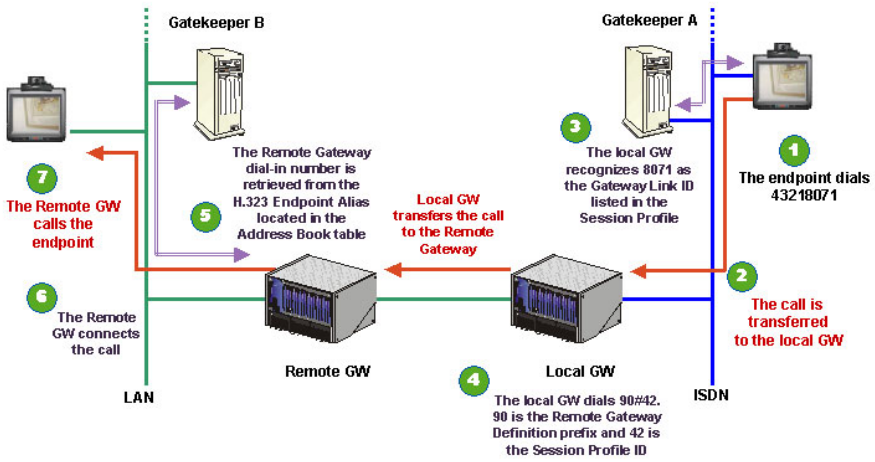


Figure 7-23: ISDN-to-IP Over H.323 Backbone Call Flow Using Address Book

Step 1. The H.323 endpoint dials the MCU/gateway prefix and the Link DID. The digits 4321 represent the Dial-in number defined in the Network Service Properties, 8071 is the Gateway Link DID taken from the Gateway Link. The Gateway Link DID contains the Dial-in number entered in the Network Service (ISDN).

Step 2. The local gateway automatically dials the remote gateway using the string 90#42. The digits 90 represent the remote gateway (H.323) prefix taken from the local Gateway Link. The Remote Gateway H.323 profile ID, 42, represents the configured Session Profile (ID E.164) parameter defined in the *To H.323 Session Profile Definition* dialog box. The # is the Speed Dial indicator (Address Book field) defined in the *Gateway Configuration - General Settings*. dialog box *The Address Book - Endpoint Definition* dialog box contains the Destination Identifier whose configuration is set to H.323 endpoint and is defined in the H.323 Endpoint Parameters settings. The H.323 Endpoint Parameters settings define the Alias Type, Alias Name and IP Address.

Step 3. The remote gateway retrieves the endpoint Alias from the Address Book table and connects the call.

H.320 Endpoint Over an H.323 Backbone to H.320 Endpoint, Using Address Book

The H.320 endpoint connects using the following string: [**Dial-in No.**][**Link DID**], for example, 43218071.

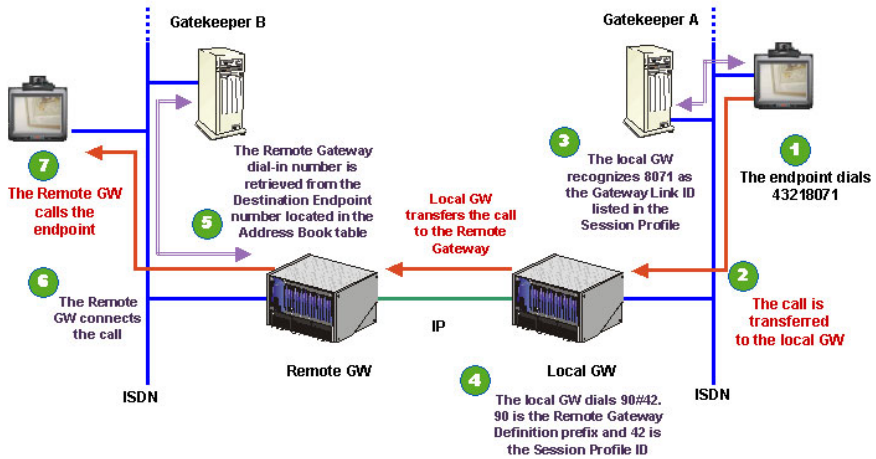


Figure 7-24: ISDN-to-ISDN Over H.323 Backbone Call Flow Using Address Book

Step 1. The H.320 endpoint dials the MCU/gateway prefix and the local Link DID. The digits 4321 represent the Dial-in number defined in the Network Service Properties, 8071 is the Gateway Link DID taken from the Gateway Link. The Gateway Link DID contains the Dial-in number entered in the Network Service (ISDN).

Step 2. The local gateway automatically dials the remote gateway using the string 90#42. The digits 90 represent the remote gateway (H.323) prefix taken from the local Gateway Link. The Remote Gateway H.323 profile ID, 42, represents the configured Session Profile (ID E.164) parameter defined in the *To H.320 Session Profile Definition* dialog box. The # is the Speed Dial indicator (Address Book field) defined in the *Gateway Configuration - General Settings* dialog box. *The Address Book - Endpoint Definition* dialog box contains the Destination Identifier whose configuration is set to H.323 endpoint

and is defined in the H.323 Endpoint Parameters settings. *The Address Book - Endpoint Definition* dialog box contains the Destination Identifier whose configuration is set to *H.320 endpoint* and is defined in the H.320 Endpoint Parameters settings. The H.320 Endpoint Parameters settings define the Phone Number and Bonding Phone number.

Step 3. The remote gateway retrieves the endpoint ISDN number from the Address Book table and connects the call.

H.320 Endpoint Over an H.323 Backbone to H.323 Endpoint, Using Profile (with TCS4)

The H.320 endpoint connects using the following string: [**Dial-in No.**, **Link DID**]^[**Alias**], for example, 43218071^222.

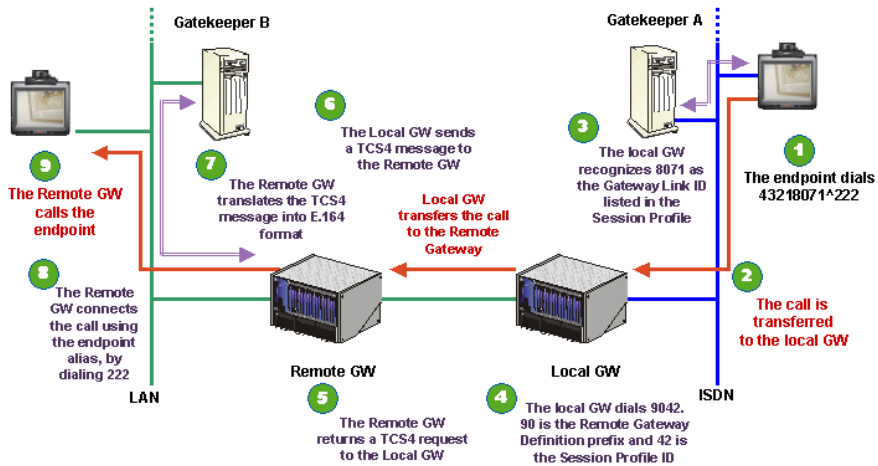


Figure 7-25: ISDN-to-IP Over H.323 Backbone Call Flow Using Profile (With TCS4)

Step 1. The H.320 endpoint dials the MCU/gateway prefix, Link DID and Alias.

The digits 4321 represent the Dial-in number defined in the Network Service Properties, 8071 is the Gateway Link DID taken from the Gateway Link. The Gateway Link DID contains the Dial-in number entered in the Network Service (ISDN), ^ is the TCS4 indicator and 222 the alias (in E.164 format) of the H.323 endpoint.

Step 2. The local gateway automatically dials the remote gateway using the string 9042. The digits 90 represent the remote gateway (H.323) prefix taken from the local Gateway Link. The Remote Gateway H.323 profile ID, 42, represents the configured Session Profile (ID E.164) parameter defined in the *To H.323 Session Profile Definition* dialog box. The remote gateway sends a TCS4 request to local gateway. The local gateway translates the E.164 string into TCS4 and sends it to the remote gateway. The remote gateway translates the TCS4 message into the E.164 alias and connects the call to the remote endpoint. 222 is the Alias retrieved from the dial string and represents the destination endpoint.

Step 3. The remote gateway dials 222 and connects the call.

H.320 Endpoint Over an H.323 Backbone to H.320 Endpoint, Using Profile

The H.320 endpoint connects using the following string: [**Dial-in No.**, **Link DID**]^[**ISDN No.**], for example, 43218071^222.

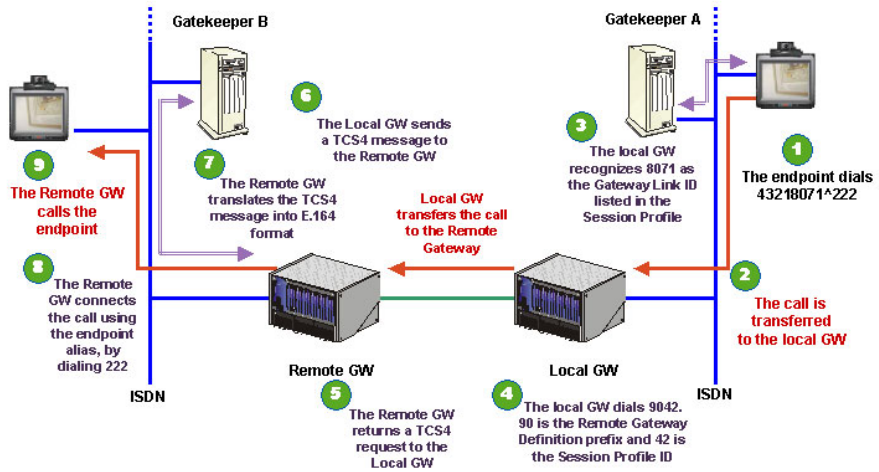


Figure 7-26: ISDN-to-ISDN Over H.323 Backbone Call Flow Using Profile

Step 1. The H.320 endpoint dials the MCU/gateway prefix, Link DID and ISDN number.

The digits 4321 represent the Dial-in number defined in the Network Service Properties, 8071 is the Gateway Link DID taken from the

Gateway Link. The Gateway Link DID contains the Dial-in number entered in the Network Service (ISDN) and 222 in the ISDN number (in E.164 format) of the H.320 endpoint.

Step 2. The local gateway automatically dials the remote gateway using the string 9042. The digits 90 represent the remote gateway (H.323) prefix taken from the local Gateway Link. The Remote Gateway H.323 profile ID, 42, represents the configured Session Profile (ID E.164) parameter defined in the *To H.323 Session Profile Definition* dialog box. The remote gateway sends a TCS4 request to local gateway. The local gateway translates the E.164 string into TCS4 and sends it to the remote gateway. The remote gateway translates the TCS4 message into the E.164 alias and connects the call to the remote endpoint. 222 is the Alias retrieved from the dial string and represents the destination endpoint.

Step 3. The remote gateway dials 222 and connects the call.

Gateway Session Profiles

A Session Profile defines how the call leaves the gateway (which network is used to handle the call), and how to establish the connection with the destination endpoint, mainly which line rate to use, and the Transcoding mode. All these parameters are defined in the Session Profile.
The following section describes the various session parameters that are defined in the Session Profile.

Network Services

The MGC unit is designed to work with different telephone carriers. In particular, the MGC unit can be connected to any public or private network that supplies ISDN lines, leased lines, ATM connections or IP connections. These include long distance carrier services and local area services. In addition, the MGC unit may be connected to a serial network using the MPI serial network interface card.

Line Rate

The transfer rate of multimedia (audio and video) between the two endpoints. The maximum line rate currently supported for H.323 participants is E1 (1920 Kbps).

Transcoding

Transcoding enables participants using different line rates and video formats to communicate, thus maintaining the highest video capabilities each participant can achieve with his/her endpoint. There are three Transcoding modes: *None*, *When Required* and *Always*.

None - No Transcoding.

When Required - Automatic Switching to Transcoding when the system identifies the need.

Always - Transcoding is always used.

Audio Only

When one of the endpoints cannot use video or is a telephone, the session is defined as *Audio Only.*

Restricted

In restricted lines, the line rate of each channel is 56 Kbps instead of 64 Kbps. This option is primarily for the United States. If one of the endpoints is using Restricted lines, the gateway session should be set to *Restricted*.

Gateway Configuration

Planning the Gateway Configuration

Before you configure the gateway, you need to:

- Ensure that appropriate Network Cards are installed and configured. For more information see "Managing the Functional Module Cards (MGC-50/MGC-100/MGC+50/MGC+100)" on page 4-2.
- Configure the Network Services according to the type of Functional Modules installed on the system. Configure the Dial-in numbers range in the ISDN Network allocated to the gateways sessions. These numbers must be different from the dial-in numbers allocated to multipoint conferencing (in the Network Service the defined dial-in gateway ranges appear in the Routing Services). For more information see "Defining Network Services" on page 3-1.
- For H.323 services define the gateway prefix. For more information see "Defining Network Services" on page 3-1.
- Select the appropriate Routing Method(s) - depending on your system configuration and the number of dial-in numbers that can be allocated to the gateway sessions, select Destinations, Address Book or Forwarding Service.

Configuration Outline

The gateway configuration flow consists of the following stages:

1. To support H.239 in gateway calls, enable the appropriate flag in the system.cfg.
2. To support multiple ISDN video endpoints calls over the same MGC gateway to reach the same IP destination, enable the appropriate flag in the system.cfg.
3. To change the default number of digits that comprises the Session Profile ID fro 2 to 1, the appropriate flag must be added to the system.cfg.
4. If required, change the General Delimiter definitions.
5. Define the dial-in numbers range allocated to the gateway in the ISDN network Service.

6. Define the Gatekeeper and Network Service prefix (Gateway) in the H.323 Network Service.
7. Defining Session Profiles: *To H.323* Session Profiles and *To H.320* Session Profiles for both ISDN and IP endpoints.
8. If required, define the Address Book entries.
9. Define the Routing Services for H.320 to H.323 gateway sessions.

To start the configuration procedure you must be connected to the MCU unit to be configured as gateway.

System.cfg Flag Configuration

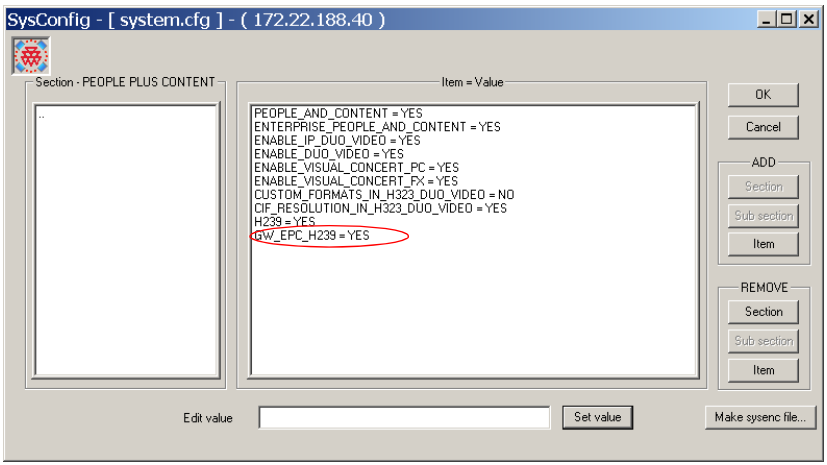
1. Right-click the *MCU* icon, click **MCU Utils** and then click **Edit "system.cfg"**.

   The *SysConfig* dialog box opens.

To enable H.239 support in gateway calls:

2. In the *SECTION* pane, double-click the **PEOPLE PLUS CONTENT** option.

   The PEOPLE PLUS CONTENT flags are displayed in the *Item = Value* pane.



3. Set the *GW_EPC_H239* flag to **YES**.

To enable multiple ISDN calls to the same IP address:

4. Return to the *SECTION* list and double-click the **H323 GK FLAGS** section.
5. Add the flag **GATEWAY_DESTINATION_SERVER** and set its value to **YES**.

To modify the default number of digits in the Session ID:

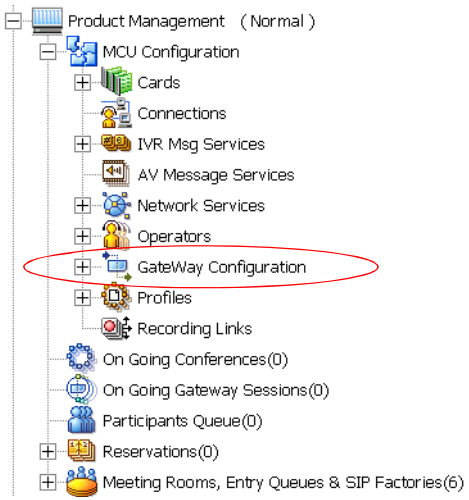
6. Return to the *SECTION* list and double-click the **GENERAL** section.
7. Add the flag **NUM_OF_DIGITS_IN_GW_PROFILE** and set its value to **1.**
8. Click **OK**.

For more details on Flag modification in the "system.cfg", *see "Edit "system.cfg"" on page 5-64*.

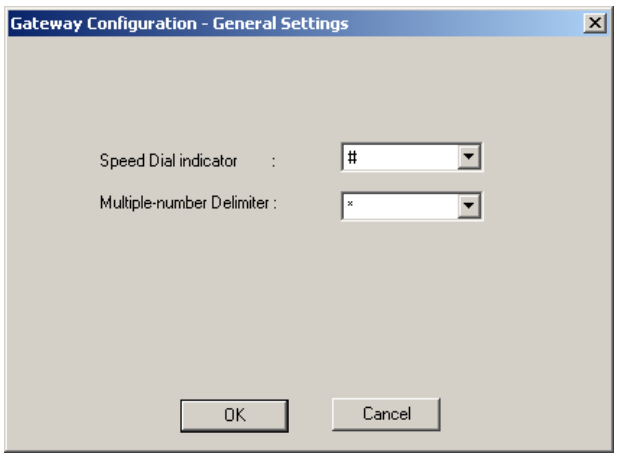
9. Reset the MCU for the flag changes to take effect.

Defining the Gateway Delimiters

1. Expand the *MCU* tree.
2. Expand the *MCU Configuration* tree to list its options.



3. Right-click the *Gateway Configuration* icon, and then click **General Parameters**.
The *Gateway Configuration - General Settings* dialog box opens.



This dialog box is used to define the indicators that will be used by H.323 endpoints when dialing into the gateway. A default value is assigned to each of these indicators. However, you may change them if required, but this is not recommended when implementing the double gateway feature.

If you are using two gateways, the indicator on both gateways must have an identical value.

4. Change the default value of the gateway indicators using the following options:

Table 7-4: Gateway Configuration - General Settings Options

Indicator	Description
Speed Dial Indicator (Address Book)	This indicator is used by the H.323 endpoint to specify an entry in the Address Book table. The digits preceding this indicator specify the gateway prefix and Session Profile to be used.

Table 7-4: Gateway Configuration - General Settings Options

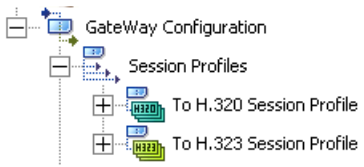
Indicator	Description
Speed Dial Indicator (Address Book) (cont.)	For example, if the H.323 endpoint enters 8391#30, the gateway searches the Address Book table for entry 30 and will take the destination endpoint properties from the table. Possible characters that can be selected are: * and #. If one is selected as the Address Book indicator, the other is automatically set as the Session Profile indicator. **Note:** Changing the *Speed Dial Indicator* setting is not recommended when implementing the *Double Gateway* feature.
Multiple-number Delimiter (Profile)	This indicator is used by H323 participants to instruct the gateway to use a Session Profile as the Routing Method. The digits preceding this indicator specify the Session Profile to be used. The digits following this indicator represent the destination endpoint phone number. For example, if the H.323 participant enters 8390*7654321, 83 specifies the gateway prefix, 90 is the Session Profile ID and 7654321 is the ISDN dial number (assuming that the selected Profile destination type is set To ISDN H.320). Possible characters that can be selected are: * and #. If one is selected as the Profile indicator, the other is automatically set as the Address Book indicator. **Note:** Changing the *Multiple-number Delimiter* setting is not recommended when implementing the *Double Gateway* feature.

Defining Gateway Session Profiles

Session Profiles define the call parameters. Session Profiles from H.323 to H.320/H.323 calls are also used to indicate the calling mode. The call parameters definition is the same for both *H.323 and H.320*: Line rate, Restricted/Non-Restricted, Audio Only/Video and Transcoding Mode. The difference between H.323 and H.320 is the Network Service to handle the call.

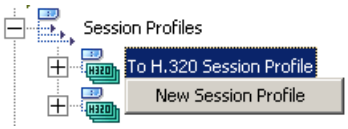
There are two main types of Session Profiles:

- To H.320 Session Profile
- To H.323 Session Profile

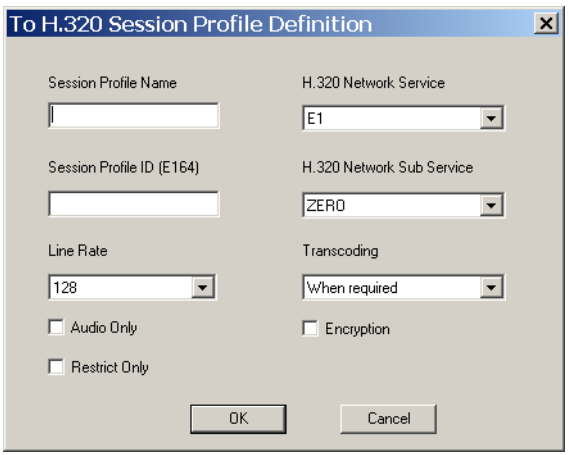


To define a To H.320 Session Profile:

1. Double-click the **Gateway Configuration** icon or click the **Plus** [+] icon next to the *Gateway Configuration* icon to list its options.
2. Double-click the **Session Profiles** icon or click the **Plus** [+] icon next to the *Session Profiles* icon to list its options.
3. Right-click the ***To H.320 Session Profile*** and then click **New Session Profile** to define a new Session Profile for H.320 destination endpoints.



The *To H.320 Session Profile Definition* dialog box opens.



4. Define the following parameters:

Table 7-5: To H.320 Session Profile Definition Options

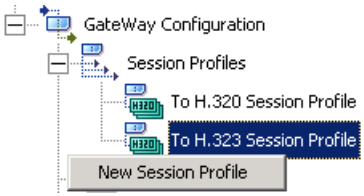
Field	Description
Session Profile Name	A name assigned to the Session Profile to identify it in the To H.320 Session Profiles list. The name is not used to handle calls.
Session Profile ID (E.164)	Enter the Session Profile ID in E.164 format (digits only). Currently, the ID is defined using up to two digits. If the call originates from H.323, using this profile ID, the endpoint enters this ID to indicate how the call is handled by the gateway. In such a case, the parameters defined for this profile will be used to handle the call gateway session.
H.320 Network Service	Select from the drop-down list the Network Service to handle the call to the destination endpoint. The default H. 320 Network Service is automatically listed.
H.320 Sub-Service	Select from the drop-down list the name of the *H.320 Sub-Service*. This field lists the default Sub-Service defined for the selected Network Service. Leave blank if no Sub-Service is to be used.

Table 7-5: To H.320 Session Profile Definition Options (Continued)

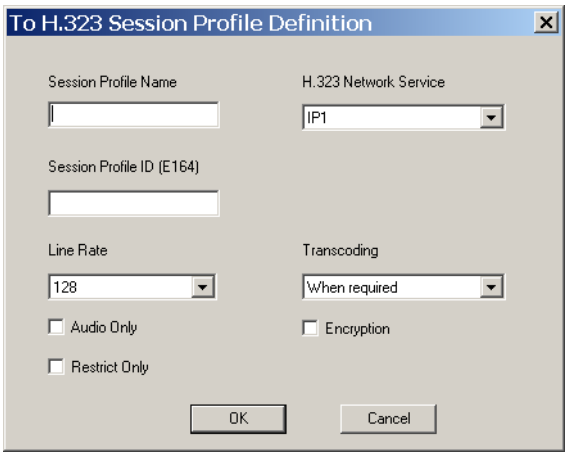
Field	Description
Line Rate	Select the multimedia (audio, video or data) transfer rate in Kbps for the gateway session. Maximum line rate currently supported is E1 (1920 Kbps).
Transcoding	Select from the drop-down list one of the following options: **Always** - The system forces transcoding in all the gateway sessions. A video card is required to support this mode. **When Required** - "Smart Video Switching" mode - the gateway tries to connect the two endpoints in video switching mode (that is both endpoints use the same line rate, video protocol and frame rate). On failure, the gateway will use transcoding to connect each participant using the participant's highest video and audio capabilities that can be achieved. A video card is required for transcoding. **None** - Transcoding is unavailable in this mode. In such a case, when the two endpoints use different line rate or protocols they will not be able to connect or they will connect in Audio Only mode (without video). **Note:** None is the default setting and it should be used when you do not want to use video resources for gateway sessions.
Audio Only	Select this check box if the gateway session should be run using audio only (without video). When cleared, video can be used during the conference.
Restrict Only	Select this check box if one of the endpoints is using restricted lines. The line rate for each channel of restricted lines is 56 Kbps instead of 64 Kbps.
Encryption	Select this check box if encryption is to be used.

To define a To H.323 Session Profile:

1. Double-click the *Gateway Configuration* icon, or click the plus [+] icon next to the *Gateway Configuration* icon to list its options.
2. Double-click the *Session Profiles* icon or click the plus [+] icon next to the *Session Profiles* icon to list its options.
3. Right-click the *To H.323 Session Profile* icon and then click **New Session Profile** to define a new To H.323 Session Profile.



The *To H.323 Session Profile Definition* dialog box opens.



4. Define the following parameters:

Table 7-6: To H.323 Session Profile Definition options

Field	Description
Session Profile Name	A name assigned to the Session Profile to identify it in the To H.323 Session Profiles list. The name is not used to handle calls.

Table 7-6: To H.323 Session Profile Definition options (Continued)

Field	Description
H.323 Network Service	Select from the drop-down list the name of the H.323 Network Service to handle the call to the destination endpoint. The default H.323 Network Service is automatically listed.
Session Profile ID (E.164)	Enter the Session Profile ID in E.164 format (digits only). Currently, the ID is defined using up to two digits. If the call originates from H.323, using this profile ID, the endpoint enters this ID to indicate how the call is handled by the gateway. In such a case, the parameters defined for this profile will be used to handle the call gateway session.
Line Rate	Select the multimedia (audio, video or data) transfer rate in Kbps for the gateway session. Maximum line rate currently supported is E1 (1920 Kbps).
Transcoding	Select from the drop-down list one of the following options: **Always** - The system forces the video transcoding mode in all the gateway sessions. A video card is required to support this mode. **When Required** - "Smart Video Switching" mode - the gateway tries to connect the two endpoints in video switching mode (that is both endpoints use the same line rate, video protocol and frame rate). On failure, the gateway will use transcoding to connect each participant using the participant's highest video and audio capabilities that can be achieved. A video card is required for Transcoding. **None** - Transcoding is unavailable in this mode. In such a case, when the two endpoints use different line rate or protocols they will not be able to connect or they will connect in Audio Only mode (without video). **Note:** None is the default setting and it should be used when you do not want to use video resources for gateway sessions.

Table 7-6: To H.323 Session Profile Definition options (Continued)

<table>
<tr><th>Field</th><th>Description</th></tr>
<tr><td>Audio Only</td><td>Select this check box if the gateway session should be run using audio only (without video). When cleared, video can be used during the conference.</td></tr>
<tr><td>Restrict Only</td><td>Select this check box if one of the endpoints is using restricted lines. The line rate for each channel of restricted lines is 56 Kbps instead of 64 Kbps.</td></tr>
<tr><td>Encryption</td><td>Select this check box if encryption is to be used.
When selected, the system automatically sets the LSD/FECC rate in encrypted and non-encrypted gateway calls as follows:
<table>
<tr><th>Gateway Connection Type</th><th>Line Rate</th></tr>
<tr><td>Non-encrypted gateway call</td><td>6.4 Kbps</td></tr>
<tr><td>H.320 to H.323
and
H.323 to H.320 encrypted call</td><td>4.8 Kbps</td></tr>
<tr><td>H.323 to H.323 encrypted call</td><td>6.4 Kbps</td></tr>
<tr><td colspan="2">Double Gateway Sessions</td></tr>
<tr><td>H.323 to H.320 to H.323 encrypted call</td><td>4.8 Kbps</td></tr>
<tr><td>H.323 to H.320 to H.323 non-encrypted call</td><td>6.4 Kbps</td></tr>
<tr><td>H.320 to H.323 to H.320 encrypted call</td><td>4.8 Kbps</td></tr>
<tr><td>H.320 to H.323 to H.320 non-encrypted call</td><td>6.4 Kbps</td></tr>
</table>
</td></tr>
</table>

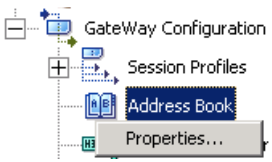
Defining and Viewing the Endpoint Address Book

The Address Book contains a list of endpoint. The list displays the information defined in the Endpoint Definition dialog box. The Address Book may be used for speed dialing when dialing from H.323 to H.320 or H.323.

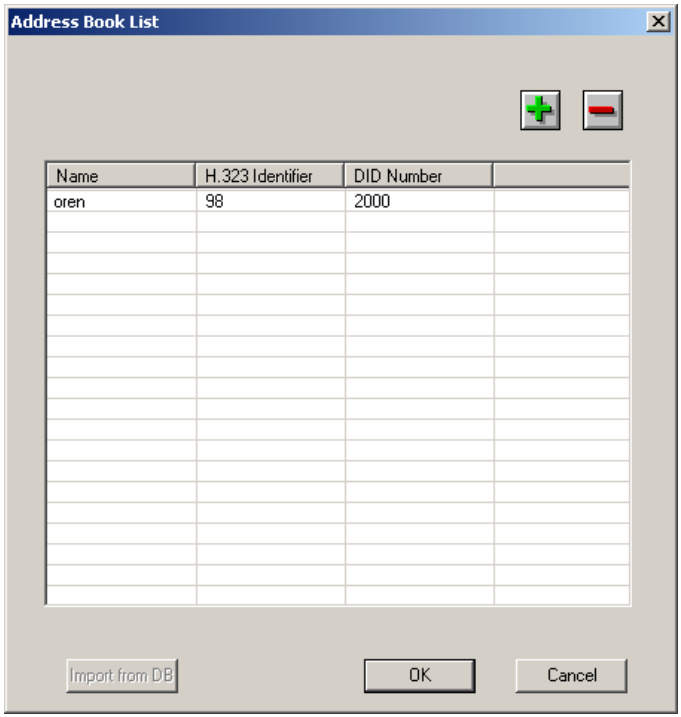
The Address Book is used to define the characteristics of an endpoint, and then associate it with either an H.323 ID or an H.320 DID, or both, depending on how you wish to reach a party. When dialing from H.320 to H.323, a DID number will be assigned to the endpoint. The DID Number will be taken from the DID number (if any) assigned to this endpoint defined in the Routing Service Definition dialog box.

To view or add an endpoint address:

1. Double-click the *Gateway Configuration* icon or click the plus [+] icon next to the *Gateway Configuration* icon to list its options.
2. Double-click the *Address Book* icon or right-click the *Address Book* icon and then click **Properties**.



The *Address Book List* dialog box opens.

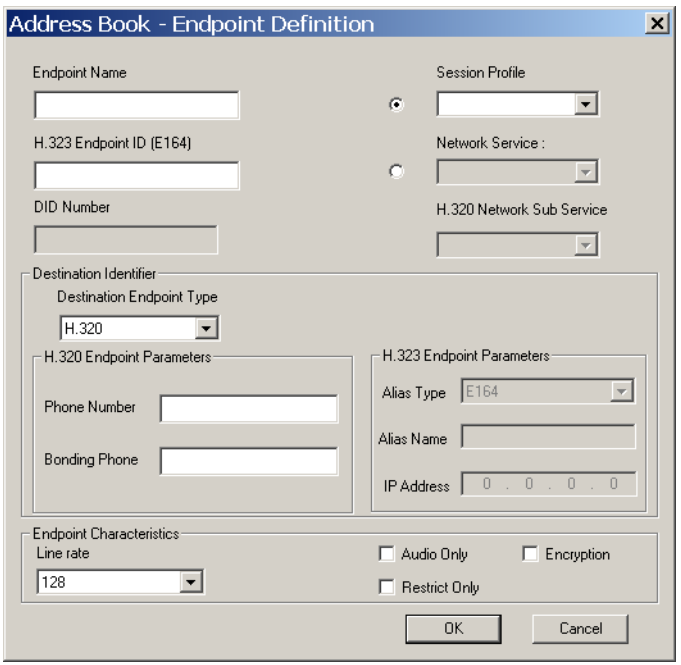


This dialog box displays a list of existing endpoints and can be sorted according to any of the table columns. The first time you access this dialog box the list is empty. The DID number (if any) is assigned to this endpoint during the H.320 Routing Service Definition.

Double click a table entry to display its properties and modify if required.

3. Click the plus [+] icon to define to add a new endpoint to the Address Book.

The *Address Book - Endpoint Definition* dialog box opens.



4. Define the following parameters:

Table 7-7: Address Book - Endpoint Definition Options

Field	Description
Endpoint Name	Enter a name that will identify the endpoint in the address book. The name is not used for call handling.

Table 7-7: Address Book - Endpoint Definition Options (Continued)

Field	Description
H.323 Endpoint ID (E164)	A number in E.164 format that identifies this endpoint. When dialing from an H.323 endpoint this number is used for speed dialing, and indicates an entry in the Address Book. When this number is dialed by the H.323 endpoint, the gateway looks for the destination endpoint parameters in the Address Book table, and routes the call to the destination endpoint according to the properties defined there. For example if you enter 88 as the *H.323 Endpoint ID,* when entering the string **# 88,** the gateway will take the endpoint parameters from the Address Book entry identified by the digits 88.
Session Profile/ Network Service	Select (from the two option buttons) whether the session parameters are taken from the Session Profile, or are defined in this dialog box. • Select the *Session Profile* option to take the Network Service definition and the session parameters from the Session Profile. Then select the session profile to be used for handling the call to this endpoint. **Note:** The Session Profile list displays the default Session Profile according to the destination endpoint type. • Select the *Network Service* option to define the session parameters and select the Network Service to handle the call in this dialog box. Then select from the dropdown list the Network Service. **Note:** The Network Service list displays the default Network Service, according to the selected endpoint type (H.320 or H.323).
H.320 Network Sub Service	Select the *H.320 Sub Network Service*. This field displays the default Sub Network Service. **Note:** This field is optional.

Table 7-7: Address Book - Endpoint Definition Options (Continued)

Field	Description
DID Number	Displays the Direct Inward Dialing (DID) number assigned to this endpoint during the *H.320 Routing Service* definition. When using H.320 services, the DID number is used to identify the destination endpoint in the Address Book table. This number cannot be changed in this dialog box and is for display purposes only.
Destination Endpoint Type	Select whether the destination Endpoint is an H.320 or H.323 endpoint. According to the selected type, the appropriate H.320 or H.323 endpoint parameters are enabled and the default Network Service Session Profile is displayed.
H.320 Endpoint Parameters	Enter the ISDN number to reach the endpoint. The number must be exactly as the MCU needs to dial it. These fields are only applicable if you chose an H.320 Endpoint **Phone number** - The H.320 endpoint phone number. **Bonding phone** - The bonding number used for aggregated channels.
H.323 Endpoint Parameters	Enter the information required to reach the endpoint. These fields are only applicable if you chose an H.323 Endpoint. **Alias Type** - The format of the endpoint *Alias Name* (H.323 ID and E.164). **Alias Name** - The Endpoint Alias according to the *Alias Type*. **Note:** Enter the *Alias Name* using the naming conventions appropriate to the selected *Alias Type*. **IP Address** - IP address of the H.323 endpoint.

Table 7-7: Address Book - Endpoint Definition Options (Continued)

Field	Description
Endpoint Characteristics	Describes the endpoint capabilities. This is especially important when importing the endpoint information from the database. These four fields appear in the Gateway Profile, the system will conduct the session according to the highest possible common denominator between the endpoint and the profile. **Line Rate** - Select the multimedia (audio, video or data) transfer rate in Kbps for the gateway session. Maximum line rate currently supported is E1 (1920 Kbps). For example, if the endpoint maximum *Line rate* is set to 384, while the Gateway Profile is set to 128 Kbps, the session will use 128 Kbps as the session Line rate. **Audio Only -** Select this check box if the gateway session should be run using audio only (without Video). When cleared, video can be used during the conference. **Restrict Only** - Select this check box if one of the participants is using restricted endpoint. The line rate for each channel of restricted lines is 56 Kbps instead of 64 Kbps. **Encryption** - Select this check box if encryption is to be used.

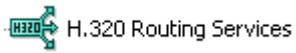
Defining H.320 Routing Services

The H.320 Routing Services define how the call originating from an H.320 endpoint will be transferred to an H.323 endpoint. There are different methods on how to transfer the call depending on the system configuration. Calls can be routed using *H.323 Destinations*, *Address Book*, *Forwarding Services* or using a *Double Gateway Link*.

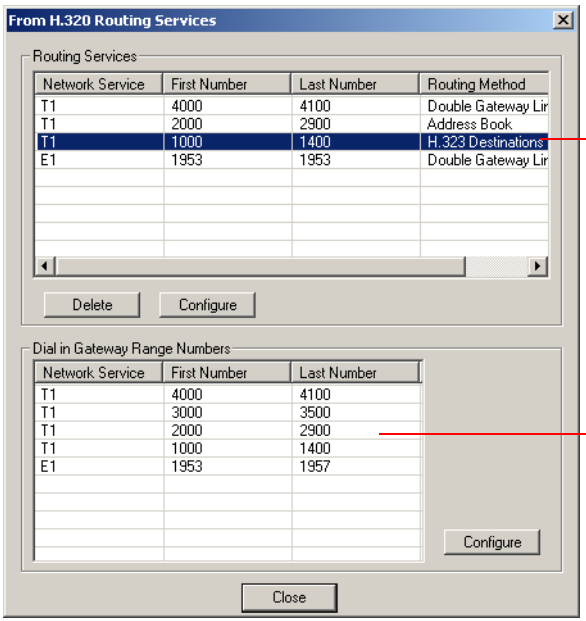
To define a new Routing Service, you start by selecting the dial in number range that will be allocated that Routing Service. Refer to “Spans and Phones Dialog Box” on page 3-14 for configuration of Dial-in number ranges. When you have completed configuration of Dial-in ranges then you define the properties of that Routing Service.

To define an H.320 Routing Service:

1. In the *Gateway Configuration* tree, double-click the **H.320 Routing Services** icon.



The *From H.320 Routing Services* dialog box opens.



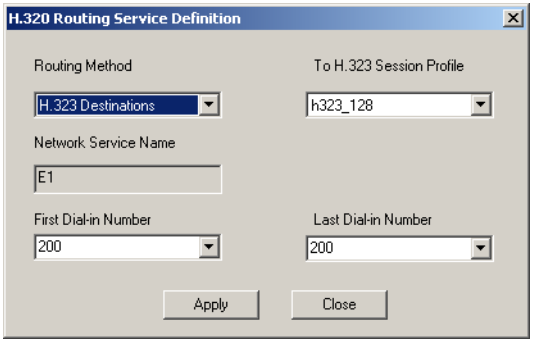
The list of dial-in numbers configured for the different Routing Methods

The list of dial-in numbers allocated to the gateway sessions in all the ISDN Network Services defined in the system

The *Dial in Gateway Range Numbers* are based on entries in the Network Services.

2. To define a new Routing Service, in the *Dial in Gateway Range Numbers*, double-click the dial-in range from which to allocate numbers to a Routing Service.
   Alternatively, in the *Dial in Gateway Range Numbers*, click the *Dial-in range* from which to allocate the number to the Routing Service and then click the **Configure** button.

   The H.320 *Routing Services Definition* dialog box opens.



3. In the *Routing Method* drop-down list, select the appropriate Routing Method. The following Routing options are available:

   — **H.323 Destinations** - The defined dial-in ranges represent also the endpoint numbers in E164 format. Use this method when H.323 endpoints register with the Gatekeeper using an Alias that is identical to the ISDN DID number. If H.323 endpoints register with the Gatekeeper using other aliases, create a conversion table in which each DID number is converted into the appropriate alias (as registered in the Gatekeeper).

   — **Address Book** - Used to assign a DID number to an Address Book entry. Using this method, the Address Book must be defined prior to the DID assignment process.

   — **Forwarding Service** - Using this method, you may use a limited number of dial-in numbers (as little as one number), and the calls will be routed to the appropriate extension according to the TCS4 information entered by the dial-in endpoint.

— **Double Gateway Link** - Used to assign a DID number to the Remote Gateway Link. In such a case, according to the DID number, the system will identify the call as being routed to a remote gateway where it will be routed to the endpoint or another gateway according to the information included in the remote gateway link. For further information, see “Defining the Remote Gateway” on page 7-66.

4. In the *To H.323 Session Profile* drop down list, select the Session Profile to be used with this Routing Service. The Session Profile defines the call parameters, such as the line rate, Restricted yes/no, Transcoding, yes/no or when required, and whether the call is an Audio Only call. In addition, it defines the Network Service that will be used to route the call from the MCU to the destination endpoint.
5. In the *First Dial-in Number* drop down list, select the first dial-in number in the range of dial-in numbers that will be allocated to the Routing Service being defined.
6. In the *Last Dial-in Number* drop down list select the last dial-in number in the range of dial-in numbers that will be allocated to the Routing Service being defined.
7. Click the **Apply** button.
8. Repeat steps 3 to 7 to define additional Routing Services with their appropriate dial-in number ranges.
   The appropriate Routing Services are added to the *From H.320 Routing Services* dialog box, in the *Routing Services* table.

Defining Routing Services Properties

Once you have assigned a Routing Service to a dial-in numbers range, you need to define the details of the Routing Service.

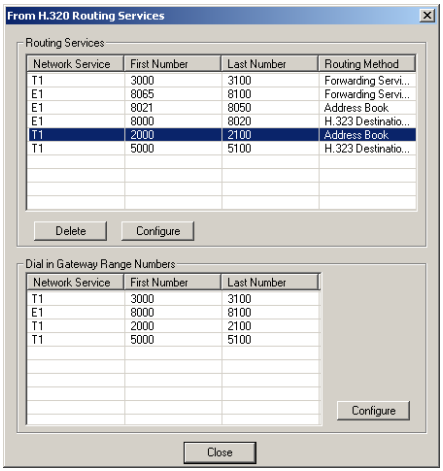
The selection of *H.323 Destinations* as the Routing Service requires no additional setting. However, you can define a conversion table in which the DID numbers are assigned the aliases with which the endpoints register. Create a conversion table when the endpoints are assigned aliases different from DID numbers. The conversion may be defined for specific or all endpoints. The table displays the list of entries already defined for the selected Routing Method. The table can be sorted according to any of the columns. The columns will display the parameters defined in the *Address Book* or *Forwarding Service* dialog box.

Defining the Properties of Existing Routing Services

1. In the *Gateway Configuration* tree, double-click the **H.320 Routing Services** icon.

   The *From H.320 Routing Services* dialog box opens.



2. In the Routing Services list, click the entry to modify and then click the **Configure** button, or double click the entry to modify.

   The H.320 *Routing Services Definition* dialog box opens.

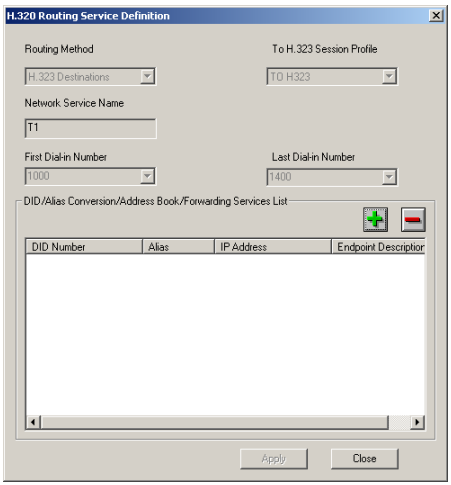


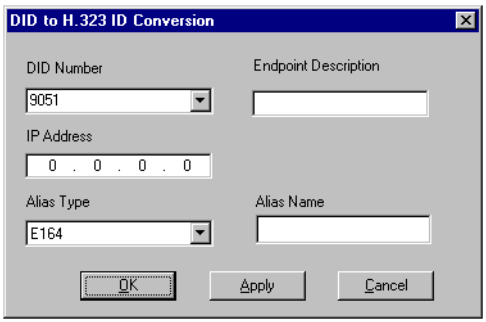
Table 7-8: Routing Services Options

Field	Description
Routing Method	Displays the selected *Routing Method*: • H.323 Destination • Address Book • Forwarding Service • Double Gateway Link **Note:** The Routing Method determines which fields will be disabled.
To H.323 Gateway Profile	Displays the name of the selected Gateway H.323 Session Profile for this Routing Service. **Note:** This field is disabled if the Routing Method used is the *Address Book*.
Network Service Name	Displays the name of the *Network Service* for reference, but the field cannot be modified.
First Dial-in Number	Displays the first number of a selected dial-in range.
Last Dial-in Number	Displays the last number of a selected dial-in range.
DID/Alias Conversion/Address Book/Forwarding Services List	Displays different parameters depending on the Routing Method.

To define the DID to H.323 Conversion table:

3. Click the plus [+] icon to add a new entry to the conversion table.

The *DID to H.323 ID Conversion* dialog box opens.



4. Define the following parameters:

Table 7-9: DID to H.323 ID Conversion Options

Field	Description
DID Number	Select the DID numbers to which to assign the H.323 endpoint IP address or Alias. The DID number may be selected from the DID number range allocated to this Routing Service.
Endpoint Description	Enter a description of the endpoint to identify it. For example, enter the name of the user to whom the endpoint is assigned.
IP Address	Enter the destination endpoint IP address. **Note**: Usually you will enter either the *IP Address* or an *Alias Name* of the endpoint. When an incoming call arrives at the Gateway with a DID number, the system will route the call to the endpoint according to the IP Address or Alias defined in the conversion table for that DID. If no entry is defined in the conversion table the DID number will be considered as the Alias in E.164 format.
Alias Type	Select the format of the alias name from the drop down list. Select either **E164** or **H323ID** (the other formats are not supported by the gateway).

Table 7-9: DID to H.323 ID Conversion Options (Continued)

Field	Description
Alias Name	Any given name that is assigned to the H.323 Endpoint. Enter the Alias name using the naming conventions appropriate to the Alias Type.

5. Click the **Apply** button to add the new entry to the conversion table and define an additional entry, repeating steps 3 to 4.
   Alternatively,
   click **OK** to add the new entry to the conversion table and return to the *H.320 Routing Services Definition* dialog box.
6. In the *H.320 Routing Services Definition* dialog box, click **Close** to return to the *From H.320 Routing Services Definition* dialog box.
7. Define the properties of additional Routing Services by double-clicking the appropriate Routing Service.
8. Complete the definition and exit this dialog box by clicking the **Close** button.

   For additional explanations on the Address Book Properties definition, see page 7-60.

   For additional explanations on the Forwarding Services, see “Defining the Properties of Forwarding Services” on page 7-63.

   For additional explanations on the Double Gateway Links, see “Double Gateway” on page 7-65.

Routing Method - Address Book

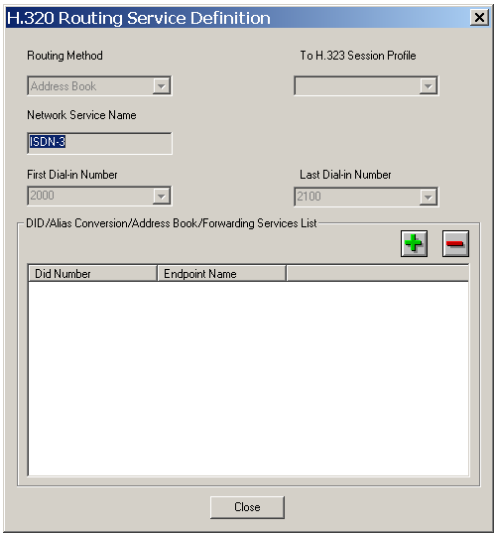
When a call using the DID number reaches the gateway, the call will be routed to the appropriate endpoint according to the endpoint IP address or Alias defined in the Address Book. The session parameters are taken from the Address Book and from the Session Profiles assigned to this Address Book entity.

If one of the Routing Services methods is set to the Address Book, you need to assign DID numbers to the entries to be called from an H.320 endpoint.

To define the properties of Address Book entries:

1. In the *From H.320 Routing Services Definition* dialog box, double-click a *Routing Service* that uses the Address Book method.

The *H.320 Routing Service Definition* dialog box opens.



2. Click the plus [+] icon to assign a DID number to an Address Book entry.

   The *Routing Method - Address Book* window opens.

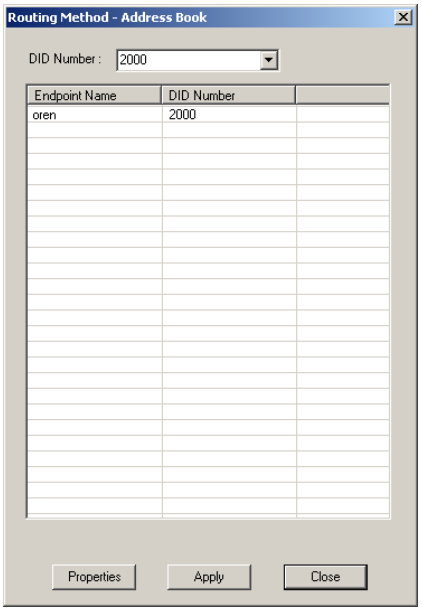


Table 7-10: Address Book List Options

Field	Description
DID Number	The system displays the first number in the range of dial-in numbers assigned to the *Address Book*. You may select another DID number from the drop-down list.
Endpoint Name column	Lists endpoints including their DID number as defined in the Address Book. **Note:** Highlighting an endpoint and clicking on the *Properties* button will enable the user to modify the properties of the endpoint. In such a case, the changes will apply to all the endpoint occurrences.
DID Number column	Lists the DID number assigned to the endpoint.

3. **Optional**
   To view the endpoint parameters as defined in the *Address Book* table, click the **Properties** button.
4. From the *DID Number* list, select the DID you wish to assign to an endpoint.
5. In the *Endpoint Name* column, select the name of the endpoint to which to assign the DID number you have selected in step 4.
6. Click the **Apply** button. The new entry is added to the Address Book list in the H.320 Routing Services Definition dialog box.
7. Repeat steps 4 to 6 to assign DID numbers to additional endpoints in the Address Book.
8. Click the **Close** button to terminate the assignment of DID numbers and return to the *H.320 Routing Services Definition* dialog box.
9. Click the **Close** button to return to the *H.320 Routing Services* dialog box.

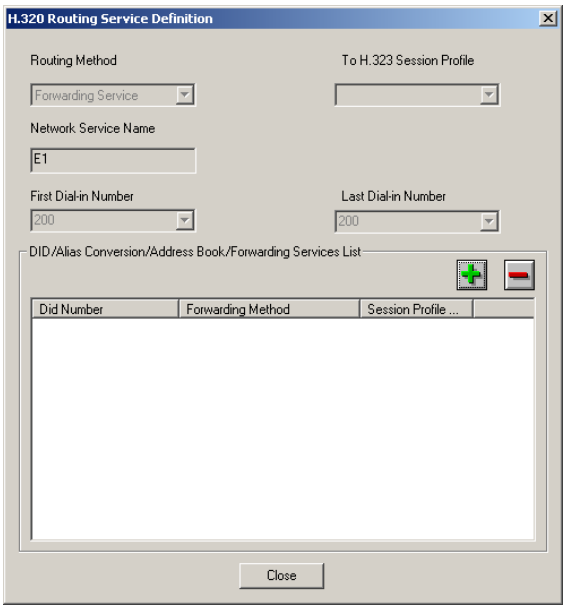
Defining the Properties of Forwarding Services

If one of the Routing Methods is set to *Forwarding Services*, define the Forwarding Services properties. This method enables you to use a limited number of dial-in numbers to route a call to destination H.323 endpoints. When the system identifies the DID number as a Forwarding Service it will expect a TCS4 input of the extension number.

To define a Forwarding Service:

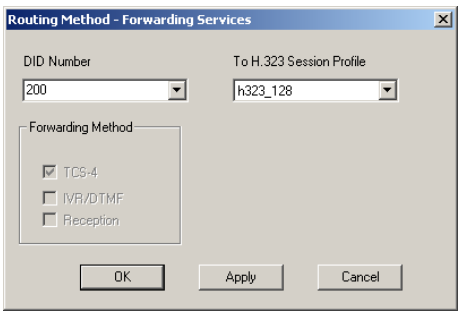
1. In the *From H.320 Routing Services Definition* dialog box, double-click a *Routing Service* that uses the Forwarding Service method.

   The *H.320 Routing Service Definition* dialog box opens.



2. Click the plus [+] icon to define a new DID to H.323 ID Conversion or select and double-click an entry to modify the properties of the Forwarding Service.

The *Routing Method - Forwarding Services* dialog box opens.



3. Define the following parameters:

Table 7-11: Routing Method - Forwarding Services Options

Field	Description
DID Number	The system displays the first number in the dial-in number range of numbers assigned to the *Forwarding Services*. You may select another DID number from the drop-down list.
To H.323 Session Profile	Select the Session Profile to be used with this DID number. The default *To H.323 Gateway Session Profile* is displayed. You may select another Session Profile from the drop-down list.

Currently, only the TCS4 Forwarding method is available.

4. Click the **Apply** button to add this Forwarding Service to the list of Forwarding Services in the H.320 Routing Services.
5. Repeat steps 3 to 4 to define additional Forwarding Services (useful when you want to define Forwarding Services with different session parameters (profile).
6. Click **OK** to complete the Forwarding Services Definition and return to the *H.320 Routing Services Definition* dialog box.
7. Click the **Close** button to return to the *H.320 Routing Services* dialog box.

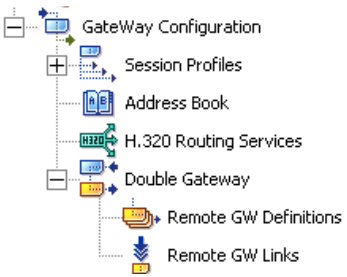
Double Gateway

The Double Gateway feature enables a call session to be routed through multiple Gateways, avoiding the cost of long distance charges, optimizing gateway usage and by-passing firewalls. The Double Gateway provides each endpoint with a connection to a local gateway and routes the long distance connection of a call between two "local" gateways on different networks.

It is strongly recommended to configure two Single Gateways prior to configuring the Double Gateway.
The Double Gateway functionality is in essence a Local Gateway, whose Party-out reaches a Remote Gateway Party-In, and then invokes the Address Book, H.323 Destinations, or Forwarding Services on the Remote Gateway. It is based on the Single Gateway methodology that uses the similar principles.

The Gateway Configuration tree includes the following entries, ranked in the order in which the user should define them:

- Remote Gateway Definitions
- Remote Gateway Links

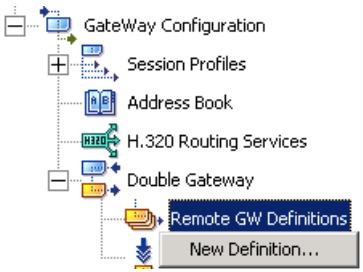


Defining the Remote Gateway

Gateways enable traffic from one network to another. In gateway to gateway communications two gateways have to be configured, the local and remote gateway.

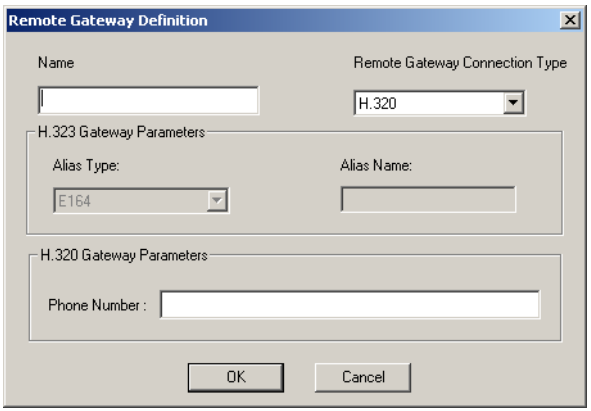
To define the Remote Gateway:

1. Double-click the *Gateway Configuration* icon or click the plus [+] icon next to the *Gateway Configuration* icon to list its options.
2. Double-click the *Double Gateway* icon or click the plus [+] icon next to the *Double Gateway* icon to list its options.
3. Right-click the *Remote GW Definitions* icon.



4. Click **New Definition**.

   The *Remote Gateway Definition* dialog box opens.



   If the selected Remote Gateway Connection Type is H.323, the *H.320* field is disabled.

If the selected Remote Gateway Connection Type is H.320, the *H.323* fields are disabled.

5. Define the following parameters:

Table 7-12: Remote Gateway Definition Options

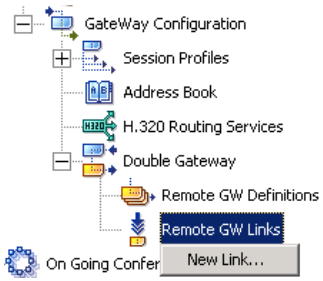
Field	Description
Name	Enter the participant Name for the remote gateway. The name is used to identify the definition in the Remote GW Definitions list and does not affect the call setup.
Remote Gateway Connection Type	Choose the type of span by which you will reach the Remote Gateway. **H.320** - Selects H.320 as the network connection protocol for linking to the remote gateway. **H.323** - selects H.323 as the network connection protocol for linking to the remote gateway.
H.323 Gateway Parameters	**If H.320 is selected as the remote gateway connection type, this field is disabled.** **Alias Type** - The format of the *Alias Name*. H.323 ID and E.164 are supported. **Alias Name** - The alias name of the remote gateway/ endpoint.
H.320 Gateway Parameters	**If H.323 is selected as the remote gateway connection type, this field is disabled.** **Phone Number** - The PRI number on the MCU and the Prefix of the remote gateway. Enter the first part of the ISDN # assigned to the Remote Gateway. The Local Gateway will take this string value with string value from the *Gateway Link - Remote GW DID* field to form a complete phone number.

Defining a Gateway Link

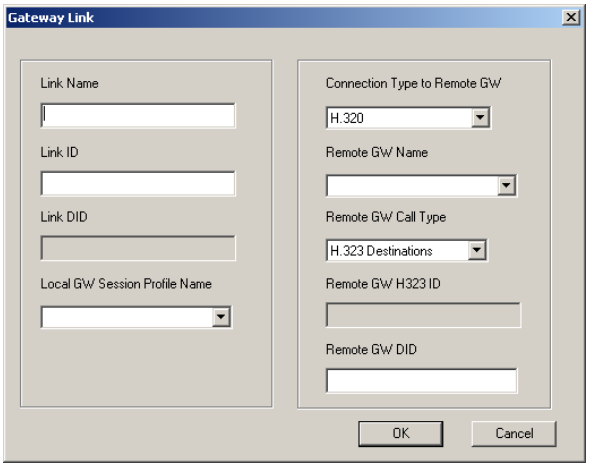
Gateway to gateway communications requires the definition of how communication is to take place between the gateways. For each Gateway link, parameters must be configured based on network requirements.

To define a Remote Gateway:

1. Double-click the *Gateway Configuration* icon or click the plus [+] icon next to the *Gateway Configuration* icon to list its options.
2. Double-click the *Double Gateway* icon or click the plus [+] icon next to the *Double Gateway* icon to list its options.
3. Right-click the *Remote GW Links* icon.



4. Click **New Link**.
   The *Gateway Link* dialog box opens.



Parameters on the left side define the activity of the local gateway. The parameters on the right side define the activity of the remote gateway.

5. Define the following parameters:

Table 7-13: Gateway Link Options

Field	Description
Link Name	Enter the gateway link name; it is advised to associate the name with the call type.
Link ID	Enter the H.323 *Link ID* number. The endpoint will call the link and connect to the Double/Multiple gateway during call setup.
Link DID	This field is disabled if no dial-in numbers were defined in the H.320 Routing Services table. Enter the H.320 *Link DID* number. The endpoint will call the link in order to connect to the Double/Multiple gateway (This number is retrieved from the H.320 Routing Services table where it is defined as the Dial-in number).
Local GW Session Profile Name	Select from the drop-down list the Session Profile to use. The available Session Profiles depend on the *Connection Type to Remote GW* selection.
Connection Type to Remote GW	Define the connection type (backbone) of the remote gateway, either H.320 or H.323. **H.320** - Selects H.320 as the network connection protocol for linking to the remote gateway. Possible connection methods include: • H.323 Destinations • Address Book • Forwarding Service **H.323** - Selects H.323 as the network connection protocol for linking to the remote gateway. Possible connection methods include: • Address Book • Profile
Remote GW Name	Select from the *Remote GW Name* list the name of the Remote Gateway.

Table 7-13: Gateway Link Options (Continued)

Field	Description
Remote GW Call Type	Define the type of dialing method that will be used to call the remote gateway: • H.323 Destinations • Profile Address (Address Book H.323 ID) • Forwarding Service • Profile (ID)
Remote GW H323 ID	This field is disabled if no H.323 ID number was defined in the Address Book. Define the H.323 ID to dial to the remote gateway. Enter the *Remote Gateway H323 ID* number. The call arrives at the Remote Gateway using the H.323 backbone and retrieves from the Address Book the H.323ID.
Remote GW DID	Define the H.320 Direct Inward Dialing (DID) number to dial to the remote gateway. Enter the *Remote Gateway DID* number.

8

Audio and Video Conversion Tools

This chapter describes the tools used to prepare audio messages and video slides used in IVR enabled conferences and during the Greet and Guide conference. It also provides step-by-step instructions for the following procedures:

- Converting the voice message files into MGC internal format
- Preparing the Video slide for video IVR Services and AV Message Services used in Greet and Guide conferences
- Downloading the files to the MCU

IVR Settings Workflow

IVR enabled conferences can be defined only if the following procedures are completed:

- For IVR enabled conferences, the Audio+ card and the Music IO card (optional) are installed in the MCU. For more details, see the MGC Hardware & Installation Manual, Chapter 2.
- The audio messages are recorded. The MGC Manager is shipped with default message files already converted to the MGC internal format. If you used these files, you may skip this step.
- The welcome video slide is created (applicable to video IVR Services).
- The Audio message and the Video slide are converted into the MGC format. If you are using the default voice messages provided with the MGC Manager, this step may be skipped.

Greet and Guide Settings Workflow

Greet and Guide conferences can be defined only if the following procedures are completed:

- For Greet and Guide conferences, during installation, the Message extension and the Music IO card (optional) are installed in the MCU and the Standard Audio card is configured accordingly. For more details, see the MGC Hardware & Installation Manual, Chapter 2.

- The welcome audio message is recorded.
- The welcome video slide is created.
- The Audio message and the Video slide are converted into the MGC format.
- A new AV Message Service is defined.

The audio message, video slide and Message Services may be prepared in advance for different types of conferences and used repeatedly over time, or they may be created when needed.

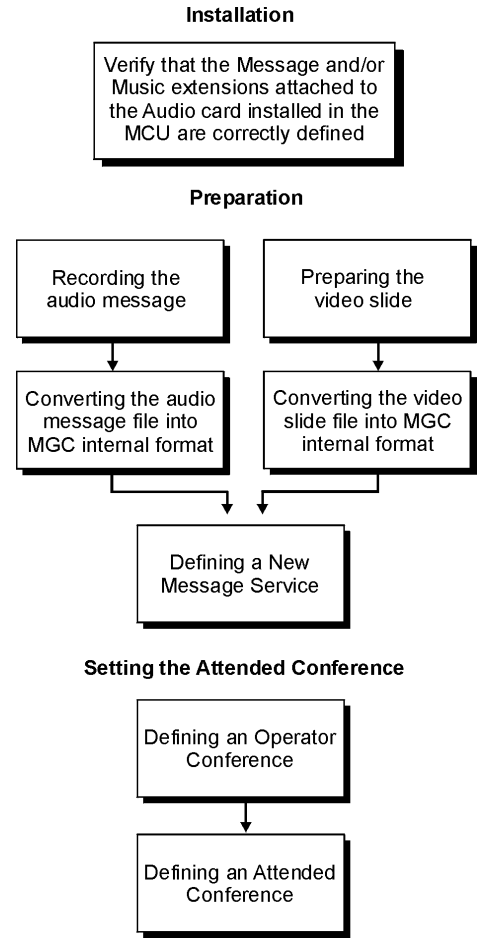


Figure 8-1: Greet and Guide Conference definition workflow

Recording an Audio Message

To record an audio message, use any sound recording utility available in your computer. Make sure that this utility can save the recorded message as a Wave file (*.wav format).

This section describes the use of the Sound Recorder utility delivered with Windows 95/98/2000/XP. This utility is found in the Multimedia menu under Programs /Accessories (from the Start menu). If you do not have it installed, install it using the Add/Remove Program utility from the Control Panel. For more details, refer to the Microsoft Windows 95/98/2000/XP documentation.

Make sure that a microphone or a sound input device is connected to your PC.

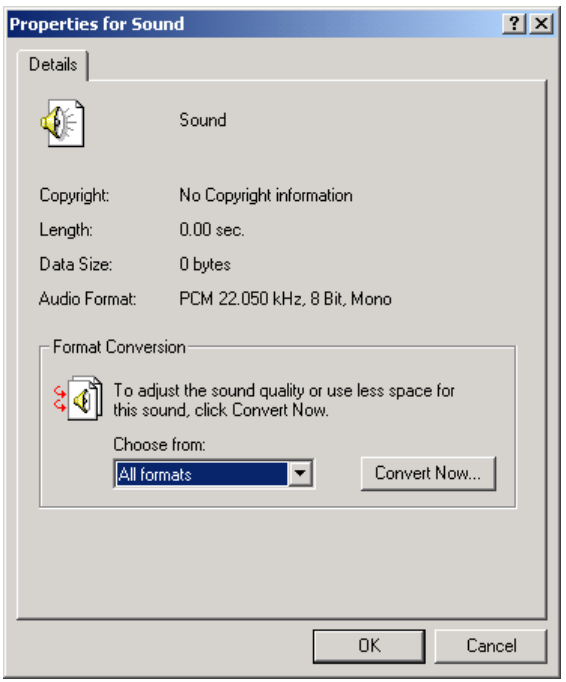
To record a new audio message:

1. Select **Programs** from the *Start* menu.
2. Open the *Accessories* group, click the **Entertainment** group and select **Sound Recorder**.

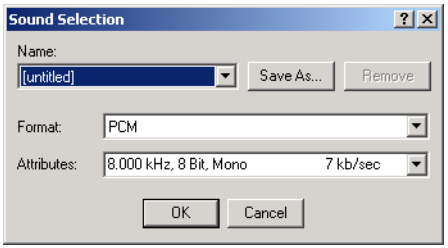
   The *Sound–Sound Recorder* dialog box opens.

3. To define the recording format, from the *File* menu, select **Properties**.

The *Properties for Sound* dialog box opens.

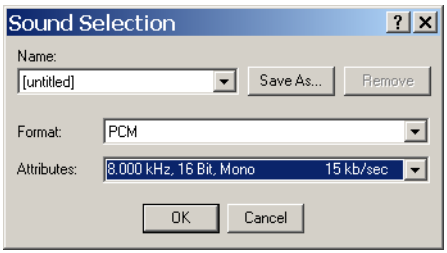


4. Click the **Convert Now** button.
   The *Sound Selection* dialog box opens.

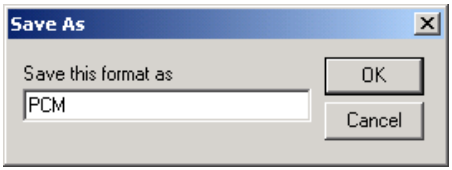


5. In the *Format* field, select **PCM**.
6. For **AV Message Service** (Greet and Guide conferences), in the *Attributes* drop-down list, select **8000Hz, 8Bit, Mono**.

For **IVR Message Service** (IVR enabled conferences), in the *Attributes* drop-down list, select **8000Hz, 16Bit, Mono.**



7. To save this format, click the **Save As** button.
   The *Save As* dialog box opens. Select the location where the format will reside and type a name for the format, for example, PCM, and then click **OK**.



   The format name appears in the *Name* field.
8. Click **OK**.
   The system returns to the *Properties for Sound* dialog box.
9. Click **OK**.
   The system returns to the *Sound–Sound Recorder* dialog box.
10. To create a new recording, from the *File* menu, select **New**.
11. Click the **Record** button.
    The system starts recording.
12. Start narrating the desired message.
13. **For IVR Services**, stop the recording anytime between 1 and 32 seconds (which is the maximum duration allowed for an IVR voice message).

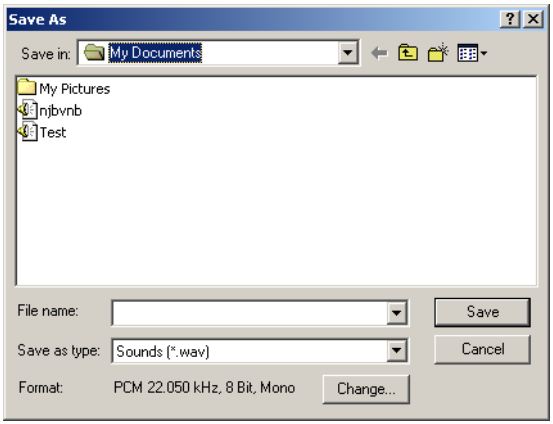
    If the message exceeds 32 seconds, it will be automatically clipped to exactly 32 seconds when converted into the MGC internal format file.

    The audio message can be recorded in one of the following durations: 2, 4, 8, 16 and 32 seconds.

For AV Message Services, stop the recording anytime between 1 and 20 seconds. The recorded message should not exceed 20 seconds. If the message exceeds 20 seconds, it will be automatically clipped to exactly 20 seconds when converted into MGC internal file.

14. To save the recorded message as a wave file, from the *File* menu, select **Save As**.

    The *Save As* dialog box opens.



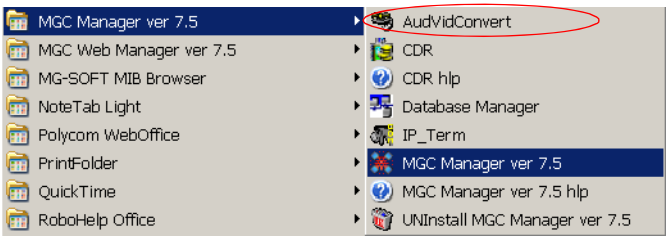
15. In the *Save in* box, select the directory where the file will be stored.
16. In the *Save as Type* box, select the ***.wav** file format, as this is the only format that the MGC converter recognizes.
17. In the *File name* box, type a name for the message file, and then click the **Save** button.
18. To record additional messages, repeat steps 9 to 16.

Converting the Audio Message Files into MGC Format Files

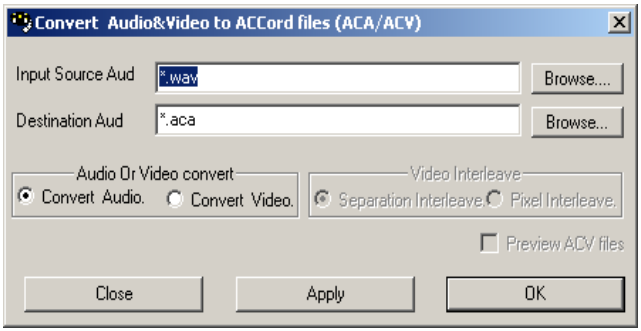
The MGC Manager includes tools that allow you to convert the audio files into a format recognized by the MCU, and send the converted files to the MCU for storage in the memory of the appropriate card.

To convert an audio message file into MGC internal format:

1. Open the **AudVidConvert** Application from the MGC Manager group.



   The *Convert Audio&Video to ACC format files (ACA/ACV)* dialog box opens.



2. Make sure that the **Convert Audio** option in the *Audio Or Video Convert* box is selected (it is the default option).
3. In the *Input Source Audio* field, enter the name of the *.wav file recorded previously or click the **Browse** button to select the appropriate file from the *Open* dialog box.
4. In the *Destination Aud* field, select the directory where the converted file (in the *.aca format) is to be stored.

5. To convert the files you can either click the **Apply** button or **OK**. Clicking **Apply** converts the file while leaving the dialog box open, allowing you to listen to the converted audio file.
   A message indicating that the conversion process was successful is displayed.
6. If the **Apply** button was selected, repeat steps 3 to 5 to convert additional audio files into MGC format.

Creating the Welcome Video Slide

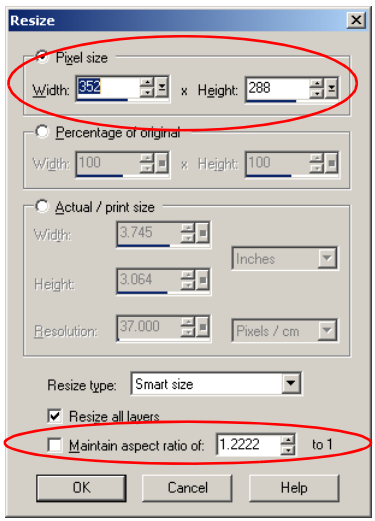
The video slide is a still picture that can be created in any graphic application such as Photoshop, CorelDraw, Paint Shop Pro etc., or any video frame captured using the appropriate application. This picture is then converted into a RAW format file, which is the only format identified by the MGC converter. The picture conversion is done in the Jasc Paint Shop Pro or Adobe Photoshop applications.

The video converter tool is based on a clip from a single slide that uses the H.261 standard. The video clip can be viewed by both low-level endpoints, and high-level endpoints with line rates higher than 768Kbps.

The *raw file size should not exceed 352 pixels in the width and 288 pixels in the height, or a file size of 297K.

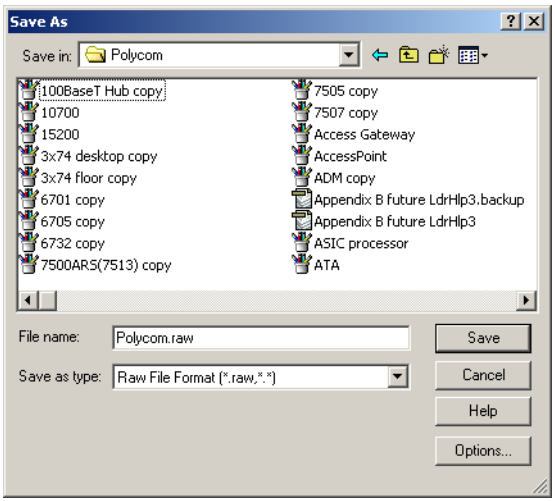
Converting the Image into a *raw Image File

1. Open the image in the Jasc Paint Shop Pro application or Adobe Photoshop. This procedure describes the creation of a *raw file in Jasc Paint Shop Pro application.
2. On the *Image* menu, click **Resize**.
   The *Resize* dialog box opens.



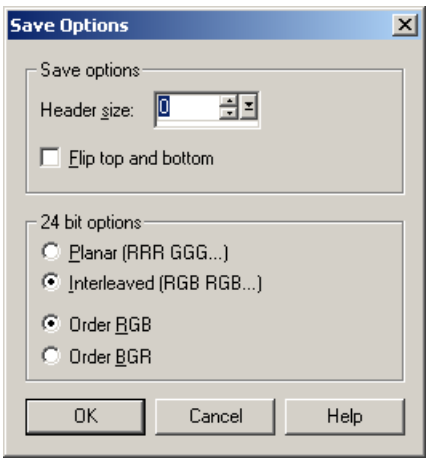
3. Clear the **Maintain Aspect Ratio** check box.
4. In the *Pixel Size* box, change the size of the image; in the *Width* box, enter a maximum of **352** pixels and in the *Height* box enter a maximum of **288** pixels.
5. Click **OK**.
6. From the *File* menu, select **Save As**.

   The *Save As* dialog box opens.



7. In the *Save As Type* box, select **Raw (*.raw)** from the drop-down list.
8. In the *File Name* box, enter the file name.
9. In the *Save in* box, select the directory where the saved file will be stored.
10. Click the **Options** button to define the Raw format options.

The *Save Options* dialog box opens.



11. In the *Save Options* box, do not change the default values.

    In the *24 bit Options* select either **Interleaved (RGB, RGB...)** and **Order RGB** or **Planar (RRR, GGG...)** and **Order RGB**.

    In an **Interleaved Order** format (known in MGC Manager terms as Pixel Interleave), the three channels (RGB colors) information is saved together for each of the picture pixels.

    In a **Planar Order** format (known in MGC Manager terms as Separation Interleave), each channel information is saved separately, for the entire separation.

    The format used to save the color channels must be as indicated when converting the file to MGC internal format.

12. Click **OK.**
    You are returned to the *Save As* dialog box.
13. Click **Save** to save the file in the raw format.

Converting the Video Slide into MGC File Format

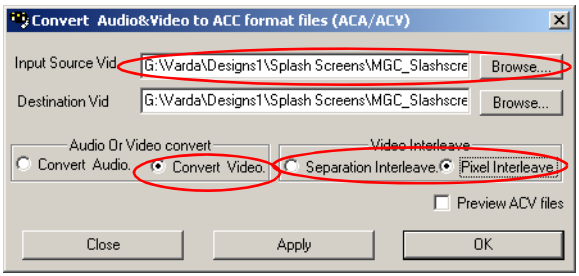
1. From the *Start* menu, select **Programs – MGC Manager Ver 7.5**, and then click **AudVidConvert**.

   The *Convert Audio&Video to ACC format files (ACA/ACV)* dialog box opens.

2. Select the **Convert Video** option in the *Audio Or Video Convert* box. The *Video Interleave* options are enabled.

3. In the *Input Source Vid* field, click the name of the *.raw file, or click the **Browse** button to select the appropriate file from the *Open* dialog box.

4. In the *Destination Vid* field, select the directory where the converted file (in the *.acv format) will reside, or click the **Browse** button to select the appropriate directory.



5. Select the order in which the RGB color channels were saved in the RAW file.

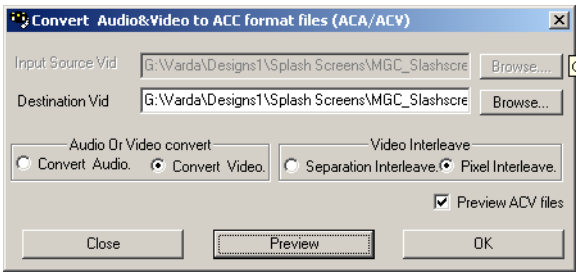
   — Select **Pixel Interleave** if the file was saved in *Interleave Order* mode.

   — Select **Separation Interleave** if the file was saved in *Planner Order* mode. In an Interleaved Order format (known in MGC Manager terms as Pixel Interleave), the three channels (RGB colors) information is saved together for each of the picture pixels.

6. To convert the file, either click the **Apply** button or click **OK**. **Apply** converts the file while leaving the dialog box open, allowing you to view the converted video slide and convert additional files. **OK** converts the file and closes this dialog box.

   The system informs you that the conversion process may take some time.

When the conversion process is completed, you may display the video slide by selecting the **Preview ACV Files** check box. The **Apply** button changes to the **Preview** button, and the *Input Source Vid field* is disabled.



7. Select the file that you wish to preview from the *Destination Vid* field, and then select the **Preview** button.
   The *VideoViewer* window opens, displaying the video slide.

8. Close the preview of the video clip.
   You are returned to the *Convert Audio&Video to ACC format files* dialog box.

9. Click **Close**.
   The *Convert Audio&video to ACC format files* dialog box closes.

If the **Apply** button is selected, repeat steps 2 to 8 to convert additional video files into MGC format.

A

Appendix A: Faults

The *Faults* function, found in the MCU's right-click menu, records faults related to the MCU that are encountered during its operation. The following is a list of fault codes sorted by fault category.

Fault Category - File

Table A-1: File Fault Descriptions

Code	Level	Description
BAD_FILE	major	One of the following errors occurred: • Invalid external application server configuration in the system.cfg file • Error reading the LCD XML file
FILE_NOT_EXIST	major	The file does not exist. This problem may be caused by an intentional file deletion or if the MCU was interrupted while writing the file, or by disk failure.
INCONSISTENT_INFORMATION_IN_FILE	major	The information in the file is inconsistent. This problem may be caused if the MCU was interrupted while writing the file or by disk failure.

The following files may be the source of the problem:

Table A-2: Fault Source Files

File Category	Description	File Name/Type
CARDS_ CONFIGURATION	Information about the location, type and layout of the cards.	In a form similar to: card.003
LOGGING	Logging information.	In a form similar to: msg001.idx msg001.cfg
NETWORK_ CONFIGURATION	Information regarding network configuration.	In a form similar to: net005.idx net005.cfg
OPERATORS_ CONFIGURATION	Information about operator accounts, users, and passwords.	In a form similar to: oper001.idx oper001.cfg
RESERVATION_ DATABASE	Holds information about conferences that were still in reservation when the MCU was last shut down.	In a form similar to: rsrv001.idx rsrv001.cfg
SYSTEM_ CONFIGURATION	General system configuration.	system.cfg
VERSION_ CONFIGURATION	Information about software and hardware versions of the cards and version related configuration information.	version.txt

To overcome such problems it is recommended to back up the configuration files.

To back up the configuration files:

1. Right-click the *MCU* icon, and then click the **MCU Utils** option.
   A cascading menu opens.
2. Click **Backup Configuration**.

When such a problem occurs, delete the configuration files and reset the MCU. The next time the MCU is started, some of these files will be created automatically, except for the two files:

- version.txt
- system.cfg

These files cannot be created automatically. To create these two files, use the **Restore Configuration** option from the *MCU Utils* menu (from the MCU right click menu).

If you did not backup the configuration files, you may install these files from the installation disk. You may need to reconfigure some of the settings after this operation.

If the problem persists, consult your service engineer.

For more information on backing up and restoring files, see Chapter 5, MCU Utilities.

Fault Category - Reservation

Reservation Faults are errors that occur if the system reboots while there are still reserved conferences that have not begun when the system was last shut down.

Table A-3: Reservation Fault Descriptions

Code	Level	Description
CONFERENCE_HAS_NO_ SUFFICIENT_RESOURCES	minor	If during an On Going Conference the MCU is reset, and then there are insufficient resources for the conference to continue. This situation can occur when a card is removed.
END_TIME_OF_ON_GOING_ CONF_IS_OVER	minor	The end time of the On Going Conference has passed. In this case, the conference is deleted from the On Going Conferences list.
END_TIME_OF_RESERVED_ CONFER_IS_OVER	minor	The end time of the reserved conference has passed. In this case, the conference is deleted from the reservations list.

Table A-3: Reservation Fault Descriptions (Continued)

Code	Level	Description
RESERVED_CONFERENCE_HAS_NO_SUFFICIENT_RESOURCES	minor	The conference cannot be reserved as there are insufficient resources. This may be caused when the reserved conference requires MUX, T1, audio, video or data resources that are not currently available on the system. Such a problem can occur if something in the configuration has changed since the reservation was made, such as, removal of a card, changes to the MUX configuration, or changes to the network service configuration.

Fault Category - Card

Card Faults are errors that occur in the hardware cards, either in the entire card or in one of its components.

Table A-4: Card Fault Descriptions

Code	Level	Description
AUDIO_ALGORITHM_NOT_SUPPORTED_BY_CARD	major	An attempt was made to enable a specific audio algorithm not supported by the card.
BLUE_ALARM	major	Similar to red alarm, but resulting in transmission failure between the local span and the PBX. Check the connection between the net spans, the transmission equipment and the PBX.
CARD_IS_IN_SIMULATOR_MODE	minor	For development use only. May occur if the simulation check box was checked during card installation.

Table A-4: Card Fault Descriptions (Continued)

Code	Level	Description
CARD_SOFTWARE_FILE_NOT_EXIST	major	The software file of the required version does not exist. You must reinstall this file. If this does not solve the problem, consult your service engineer.
CARD_STARTUP_NOT_IN_TIME	major	This fault is related to the function: "OnUnexpectedStartupIndication" that is called only when receiving: • NEW_CARD_INDICATION • STARTUP_COMPLETION_INDICATION • START_POLLING_INDICATION when the card is in normal state.
CARD_TYPE_NOT_EXIST_IN_CONFIG	major	The entry is missing in version.txt on the Main Control's local disk. Consult your service engineer.
CCOM_FATAL_ERROR	major	There was a fatal error in the CCOM card. This will cause the reset of the CCOM card. When the reset is complete, the system should continue to function normally. This may interfere with On Going Conferences. It is recommended to reset the MCU when idle (when there are no On Going Conferences).
D_CHANNEL_IS_NOT_ESTABLISHED	major	The span failed to establish a D-Channel. Check the physical connection and the network configuration settings.
FAULTY_UNIT_RECOVERED	minor	Occurs after VideoPlus/H.323 card self-recovery.
H323_LAN_LINK_STATUS_DOWN	major	No LAN link to IP card.
IP_CARD_STATUS_DHCP_SERVER_TIMEOUT	major	The card could not find the DHCP Server.
IP_CARD_STATUS_NAT_AUTODISCOVERY_FAIL	minor	Autodiscovery failed.

Table A-4: Card Fault Descriptions (Continued)

Code	Level	Description
IP_CARD_STATUS_DNS_SERVER_TIMEOUT	major	The DNS Server did not respond.
IP_CARD_STATUS_DNS_SERVER_IP_NOT_PROVIDED	major	The DHCP Server did not return the DNS Server IP address.
IP_CARD_STATUS_SIP_PROXY_IP_NOT_PROVIDED	major	The DHCP Server did not return the SIP Proxy IP address.
IP_CARD_STATUS_NOT_PROVIDED	major	The DHCP Server did not return the Gatekeeper IP address.
IP_CARD_STATUS_ADDRESS_CHANGED	major	The DHCP Server sent a new address for the IP card.
LARGE_CONF_NOT_SUPPORTED_BY_CARD	major	Applicable only to a legacy Audio card where conferences with more than 16 participants are not supported by the current software version of the card.
MESSAGE_DOWNLOAD_HARDWARE_PROBLEM	major	There is a problem downloading a message to the audio card.
MESSAGE_TRANSMISSION_PROBLEM	major	There is a problem transmitting a message to the audio card.
NET_CARD_STARTUP_PROBLEM	major	Problems occurring during PRI card startup.
NETWORK_SERVICE_ERROR	major	May be caused when assigning a network service to a span and then deleting the network service.
NO_CONNECTION_WITH_CARD	major	The MCU failed to communicate with the card. The card may have been removed, or is not firmly in place. This may also be caused by a faulty card.

Table A-4: Card Fault Descriptions (Continued)

Code	Level	Description
NO_DUAL_SLOT_MASTER_VIDEO_CARD	major	Applicable to dual video cards. The video card is identified as master but there is no Slave video card identified. Removing the Slave card may be the cause. Check if the card is indeed a dual card. If it is, consult your service engineer. If there is no dual card you may reset this card.
NO_DUAL_SLOT_SLAVE_VIDEO_CARD	minor	Applicable to dual video cards. The video card is identified as slave but there is no Master video card identified. Removing the Master card may cause this. Check if this is indeed a dual card. If it is, consult your service engineer. If there is no dual card, you may reset this card.
NOT_ATTENDED_HARDWARE_VERSION	major	Card software does not support attended conferences when the MESSAGE flag in the GREET AND GUIDE/IVR section of the "system.cfg" is configured to **YES**.
RED_ALARM	major	The local span failed to identify the line. Check the connection between the net span and the PBX.
UNEXPECTED_CARD_TYPE	major	The card in this slot is of a different type than expected. For example, this may happen if a card of a one type physically replaces a card of different type. If this is the case, use the operator to remove the card and then reset the card slot.
UNEXPECTED_EMPTY_SLOT	major	An empty slot was encountered where a card was expected. This will be caused if a card is physically removed without removing it in the MGC Manager as well.
UNIT NOT RESPONDING	major	Unit is not responding to requests due to a card component fatal error

Table A-4: Card Fault Descriptions (Continued)

Code	Level	Description
VIDEO_HIGH_BIT_RATE_NOT_SUPPORTED_BY_CARD	major	When the HIGH BIT RATE flag in the system.cfg file, FLAGS section is configured to **YES**, but the card's hardware version installed in the system is too old.
VIDEO_HIGH_FRAME_RATE_NOT_SUPPORTED_BY_CARD	major	Video card version is less than 1.24 and in the GENERAL section of the "system.cfg" HIGH_VIDEO_FRAME_RATE is configured to **YES.**
YELLOW_ALARM	major	The local span identified the line but the PBX failed to identify the local span.

Fault Category - Exceptions

A severe system error, or exception, is an error that prevents the current task from being executed. When the system detects such an error, it automatically locks (or suspends) the task that caused the error. The effect of this suspension depends on the type of the task. An error in a main or critical task will cause the system to restart itself.

An error in a **conference task** will lock the conference. In this case, all conference related operations will be blocked, including terminate, add participant, remove participant etc. From the participants' point of view, the conference will go on but will stay in its current state, for example no video switching will take place. However all other On Going Conferences will not be affected. The operator can wait for these conferences to end, and then restart the system manually. Similar behavior will take place when the error is caused by a **participant task**.

The system indicates the detection of a **severe error** by logging a fault message. The message is displayed as follows:

Table A-5: Fault Log Message

Time	Category	Level	Code
06:23 pm june 15	exception	major	EXCEPTION_HANDLER_MESSAGE

Description	
EXCEPTION: error=0x0 error_address=0x1c0e74 TaskID=0x370000 tskname=**CONF** interpt_num=0	

This message can be viewed in the *Fault Messages* window. If such a fault occurs, it is very important that you write down the fault message description as well as the sequence of operations that led to it, and transfer it to the system service engineer so that the problem can be fixed.

Fault Category - General

Table A-6: General Fault Descriptions

Code	Level	Description
APPLICATION_SERVER_INTERNAL_ERROR	major	An internal error in the external application server where the Ad-Hoc database resides.
BAD_SPONTANEOUS_INDICATION	minor	When there is a fault in the Audio card.
CAN_NOT_ESTABLISH_CONNECTION_WITH_APPLICATION_SERVER	major	Cannot establish a connection with the external application server where the Ad-Hoc database resides.
CAN_NOT_ESTABLISH_CONNECTION_WITH_SIP_REGISTRAR	minor	The SIP registrar did not respond. Check the configuration of the SIP server in the IP Network Service. If the configuration is OK, try pinging the IP address.
CONNECTION_ERROR	major	LAN driver error.
DONGLE_ERROR	major	May be due to one of the following unit errors: • Failure in reading the dongle file • Failure in reading the dongle serial number • Failure in reading the dongle data
DONGLE_NOT_ATTACHED	major	May be due to one of the following unit errors: • Failed to find the dongle driver • No dongle button found
EMPTY_PERFORMANCE_MONITORING_TRASH_HOLD	minor	Not all the fields in the PERFORMANCE MONITORING section of the system.cfg file are valid.
FAILED_TO_LOAD_XML_SCHEMAS	major	The XML schemas were not loaded.

Table A-6: General Fault Descriptions (Continued)

Code	Level	Description
FAN_1_FAILURE	major	Applicable to MGC-25 only. Fan one failed.
FAN_2_FAILURE	major	Applicable to MGC-25 only. Fan two failed.
GATE_KEEPER_ERROR	minor	Occurs when an attempt to register with the Gatekeeper has failed.
GATEKEEPER_MESSAGE	system message	Returns the code: REGISTRATION_SUCCEEDED, the card succeeded in registering to the Gatekeeper.
INSUFFICIENT_TDM_ALERT	major	Failure occurs during TDM time slot (TSS) allocation when the requested number of TSS are not available, and the corresponding resources cannot be used. For each port in the MCU TSS interaction between cards is conducted using a TDM (Time Division Multiplex) method, where two types of TSS allocation are used: • Static • Dynamic
LINE_PM_ERROR	minor	Occurs when there is a problem with performance monitoring. All network issues are notified via the Net card.
LOW_MEMORY_ALERT	major	There is a high fragmentation problem, which has caused a memory overload.
MCU_VERSION_IS_NOT_PERMITTED	major	Dongle error status—no permission granted for MCU version.
MORE_THAN_ONE_CLOCK_SOURCE_TYPES	minor	Occurs when more than one flag in the MCU CLOCKING section of the system.cfg file is configured to **YES**.

Table A-6: General Fault Descriptions (Continued)

Code	Level	Description
NO_AUDIO_MESSAGE_IN_ CONFIGURATION	major	Occurs when the MESSAGE flag in the system.cfg file, ATTENDED section is configured to **YES**, but there is no suitable hardware in the system.
NO_CLOCK_SOURCE	major	This error usually follows a red, blue or yellow alarm. If the MCU fails to identify the PRI line it is unable to synchronize itself by the PBX.
NO_MUSIC_IN_ CONFIGURATION	major	Occurs when the MUSIC flag in the system.cfg file, ATTENDED section is configured to **YES**, but there is no suitable hardware in the system.
PASSWORDS_CONFLICT__ PLEASE_SEE_ pscnflct_log_ FILE_FOR_DETAILS	startup	The password assigned to a conference or reservation loaded from a previous version is not valid in the current version. For details see the pscnflct.log file in the MCU root directory.
POWER_SUPPLY_ FAILURE		Applicable to MGC-25 only. The power supply failed.
RESET_MCU_BY_ OPERATOR	minor	The MCU was reset by the MGC Manager from the *Reset MCU* sub-menu.
SINGLE_CLOCK_SOURCE	minor	Only one span was able to synchronize itself with the PBX. The system will continue to function normally but there will be no backup clock source. If there are more than one net (T1 or E1) cards connected to the PBX, this may indicate a problem with the connection to the PBX.

Table A-6: General Fault Descriptions (Continued)

Code	Level	Description
UNEXPECTED_HARDWARE_ VERSION	major	Card version does not match "card.cfg". This situation can occur if a card of the same type but of a different hardware version is replaced while the MCU is off.
UNKNOWN!!!	major	An inconsistent MGC Manager version is being used.
VERSION_DOSNT_MATCH	major	Version number in the arrow configuration is less than 5.
WRONG_DONGLE_ ATTACHED	major	When an inconsistent dongle is attached to the MGC.

Fault Category - Assert

Table A-7: Assert Fault Descriptions

Code	Level	Description
SOFTWARE_ASSERT_FAILURE	major	A program assertion has failed. This indicates an error in the program execution. If this problem persists, consult your service engineer.

Fault Category - Startup

Table A-8: Startup Fault Descriptions

Code	Level	Description
SYSTEM STARTUP	startup	This message is generated each time the system is booted.

Table A-8: Startup Fault Descriptions (Continued)

Code	Level	Description
UNSUITABLE_AUDIO_PLUS_CONF_FREQUENCY_SETTING_TO_SUPPORT_SIREN_14	startup	System configuration (system.cfg) conflict occurring when: • The AUDIO PLUS FLAGS section AUDIO_PLUS_FREQUENCY is configured to **14** and the H320 AUDIO section SIREN14_320 is configured to **YES** • The AUDIO PLUS FLAGS section AUDIO_PLUS_FREQUENCY is configured to **14** and the H323 AUDIO section SIREN14_323 is configured to **YES**
UNSUITABLE_MUSIC_SETTING_TO_SUPPORT_SINGLE_PARTY_HEARS_MUSIC	startup	System configuration (system.cfg) conflict occurring when: • The AUDIO PLUS FLAGS section SINGLE_PARTY_HEARS_MUSIC is configured to **YES** and the GREET AND GUIDE/IVR section MUSIC is configured to **YES**

B

Appendix B: PPP Setup

The PPP (Point to Point Protocol) support enables the operator to establish TCP/IP communication with the MCU via a telephone line with a modem, or directly via a serial connection.

In order to use the PPP support, both the remote PC that runs the MGC Manager and the MCU must be set up.

Currently, only one PPP session is supported by the MCU. This PPP session can be either via Modem connection or via direct serial connection.

The Modem connection involves attaching a modem to one of the MCU's serial connectors. The remote station can then connect to the MCU via the modem.

The Direct Line connection involves connecting the remote station to the MCU using a Null Modem cable.

Software Setup

The MCU software includes PPP support that is usually disabled. In order to activate the PPP support, the file **PPP.CFG** must be placed in the directory **c:\MCU\CFG.**

The file PPP.CFG contains the PPP configuration parameters. It specifies the COMM port number to be used by the PPP connection, the type of connection (Modem or Direct) and several other parameters such as baud rate and modem initialization parameters.

Except CON_TYPE, all the parameters have default values, and should only be included in the ppp.cfg file if they have been altered.

The file format is similar to the windows INI files format - text file with sections.

The modification of the setup file is done manually using the appropriate text editing application, such as Notepad.

Following are two examples of ppp.cfg files setup:

1. Open the Notepad application.

```
[COMM2]
CON_TYPE=MODEM
```

2. Type in the text as described in the following table depending on the type of PPP connection you are using.

```
[COMM3]
CON_TYPE=DIRECT
```

In the example shown above, the ppp.cfg file contains the setup for COMM 2 to Modem connection.

In the second example, the ppp.cfg file contains setting for COMM 3 to Direct connection.

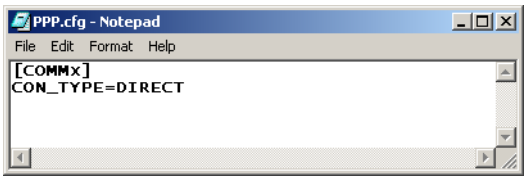
Before configuring the PPP to a COMM port, you have to check that no other device is configured to use the same port.

Following is the list of sections in the configuration file and their parameters.

COMMx

In Modem connection, the COMM port x can be 1,2,3,4,5 or 6.

In Null Modem connection, x is either 1 or 2, depending on the serial port used.



CON_TYPE - Connection type. May be either **MODEM** or **DIRECT**.

MODEM stands for a modem connection. Modem configuration requires MODEM_SETUP_STRING and MODEM_HANGUP_STRING (and if they are not specified, the default values are taken).

- **MODEM_SETUP_STRING** - This is a combination of configuration parameters of the specific modem type and the PPP driver's CHAT Script.
  Since the modem is only expected to answer calls, the initialization string is the default value that can be used with most of the standard modems. However, if a non-standard modem is used, or if a special feature of the modem is to be used, the parameters can be (carefully!) changed.
  This parameter is ignored if CON_TYPE=DIRECT.
- **MODEM_HANGUP_STRING** - This is a combination of the hang-up parameters of the specific modem type and the PPP driver's CHAT Script.
  Since the hang-up string is simple, the default value can be used with most of the standard modems. However, if a non-standard modem is used or if a special feature of the modem is to be used, the parameters can be (carefully!) changed.
  This parameter is ignored if CON_TYPE=DIRECT.
- **BAUD** - Serial Port's baud rate. May be 300, 1200, 2400, 4800, 9600, 19200, 38400, 57600 or 115200.
  Default value: 19200.

To set up PPP:

1. Save the file as ppp.cfg in any directory.
2. Send the file to the MCU by using the *Send* option in the MGC Manager *MCU Utilities*.
3. Copy the file to the CFG directory using the Telnet option in the MGC Manager MCU's right-click menu.
4. Now type in the following information as shown:

   pSH+> cd 7.256/mcu

   pSH+> cd cfg

   pSH+> cd.

   pSH+> cd Bin

   pSH+> mv ppp.cfg /mcu/cfg
5. Reset the MCU.

Hardware Setup

The MCU can have either 2 COMM ports, or, if a MOXA serial board is plugged into the system, it will be able to support 6 COMM ports. Before installing a MOXA serial board, shut down the MCU. When turning on the system, the MCU will automatically identify the MOXA board (if it exists). There is no need for software setup.

Modem Setup

An external modem may be connected to each of the serial ports.

To connect the modem:

1. Configure the modem in ppp.cfg.
2. Shut down the MCU.
3. Connect the modem to the COMM port (as defined in ppp.cfg), connect its power supply and turn it on.
4. Turn on the MCU.

During the MCU power-up, the modem will be initialized and ready to receive calls from remote operators.

Direct Line Setup

The direct line cable (null modem cable) can be connected at any time. However the port it is connected to must be defined in ppp.cfg.

The following tables describe the null modem wire-up for different connector combinations.

Table B-1: Null Modem 25/9 Pin Connector Wire-up

25 Pin Connector	9 Pin Connector
2	2
3	3
4	8
5	7
6,8	4
7	5
20	6,1

Table B-2: Null Modem 9/9 Pin Connector Wire-up

9 Pin Connector	9 Pin Connector
3	2
2	3
7	8
8	7
6,1	4
5	5
4	6,1

Table B-3: Null Modem 25/25 Pin Connector Wire-up

25 Pin Connector	25 Pin Connector
2	2
3	3
4	4
5	5
6,8	20
7	7
20	6,8

PC Setup for PPP Support

The setup described in this section applies only to Windows 95.

Modem Connection Setup

Use the built-in *Dial-Up Networking* feature to define the dial-up connection.

Use the following dial-up connection parameters (Properties):

- In the *Main* window, enter the telephone number of the MCU's Modem, and the Operator's modem type.
- In the *Server Type* window, select the **PPP: Windows 95, Windows NT** and check only the **Enter the Network** and the **TCP/IP** options.
- In the *TCP/IP definitions* window, enter only the Operator's IP address. Select the *Server Assigned Name* server address (you don't need to specify the MCU IP address). Check the two options at the bottom (**IP compression** and **Use default gateway**).

In order to activate the connection, double-click the **Dial-Up-Networking** icon created previously, enter the User name, Password and the Phone number, and then select **Connect**. As soon as the connection is established, the MGC Manager software can run and communicate with the MCU.

Direct Connection Setup

Use the built-in *Dial-Up Networking* feature to define the dial-up connection (as in modem connection setup).

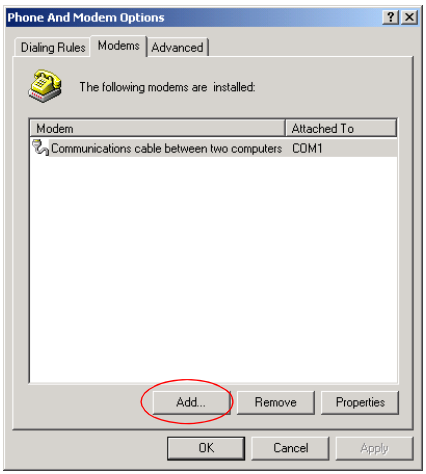
To set a direct connection, you need to install a **Null Modem** driver.

To install the Null Modem driver, follow the instructions described in the following Web site: http://www.kevin-wells.com/net/

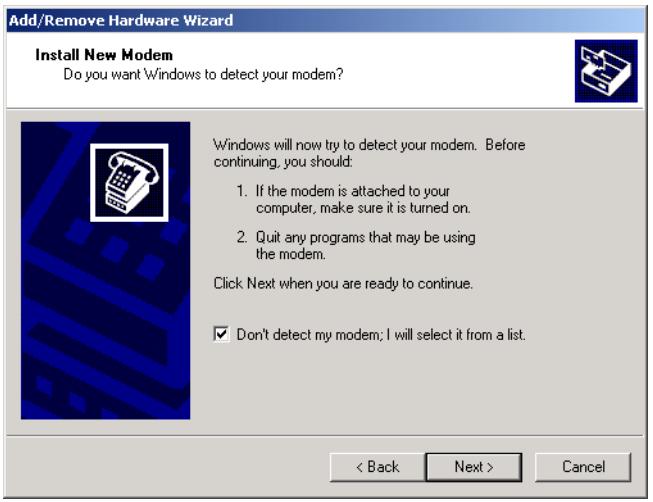
This site contains the following information (with some modifications) from May 14, 1997. It is recommended to check the page again for updates and changes.

1. Download the file **mdmcbx.inf,** which is needed for all direct connections. There are different versions listed on the Web page. If Windows 95 will not install the above file, try an earlier version. This problem may occur especially with non-US versions of Windows 95.

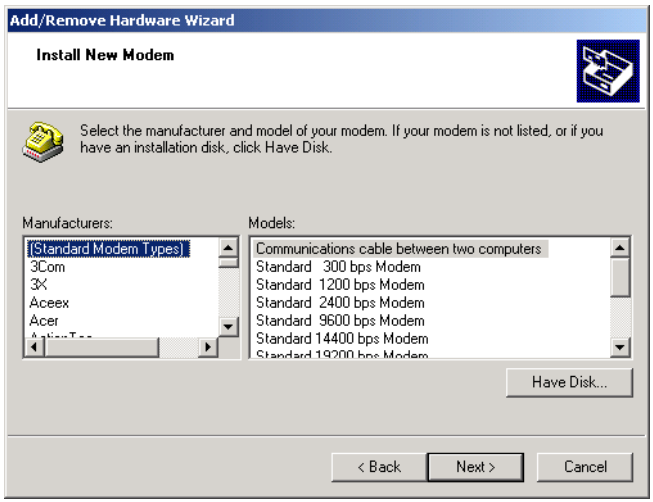
2. Select *Start – Settings – Control Panel*, and then click the *Phones and Modems* icon  .
   The *Phone And Modem Options* dialog box opens.



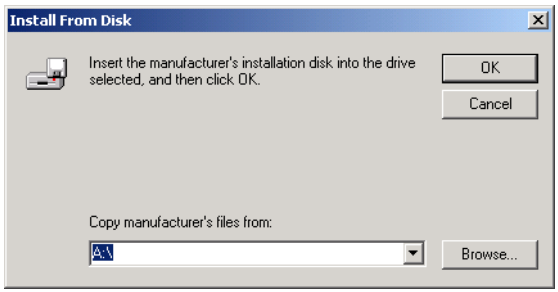
3. Select the **Modems** tab and then click **Add**.
   The *Add/Remove Hardware Wizard* dialog box appears.



4. Click the **Don't detect my modem I'll select it from a list** check-box and then click **Next**. The list of modems is displayed.

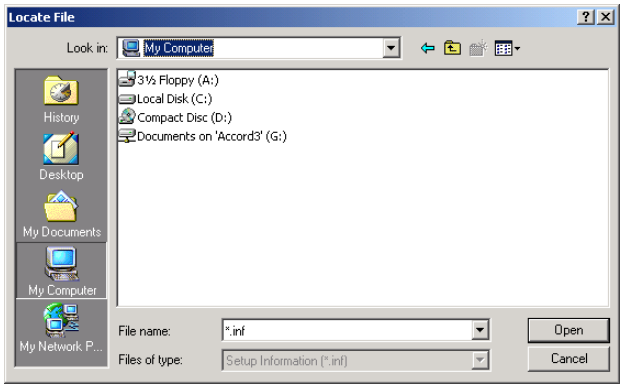


5. Click the **Have disk** button.
The *Install From Disk* dialog box opens.



6. Type the file name and path (that you downloaded in step 1) in the *Copy manufacturer's files from* drop-down list, or click **Browse**.

   The *Locate File* dialog box opens.



   Select the file, and then click **Open**.

7. In the dialog box that opens, a modem named *Direct Connection* should be listed. Highlight this modem and click on the **Next** button.

8. Choose the communications port to which the null modem cable is connected. You may have to look in the back of your computer. Click the desired COMM port and then click **Next**.

9. Click the **Finished** button to complete the setup. A modem called *Direct connection* is displayed in the *Modems* box.

10. Double-click the *Direct Connection* icon to activate the connection. When prompted for a phone number, enter any number, as the driver does not need this parameter to activate the connection. The user name and password should be taken from the MCU. (The default user name and password are POLYCOM.)

Setting up your PC - Detailed Description

Your PC may have any one of the following Operating Systems (OS):

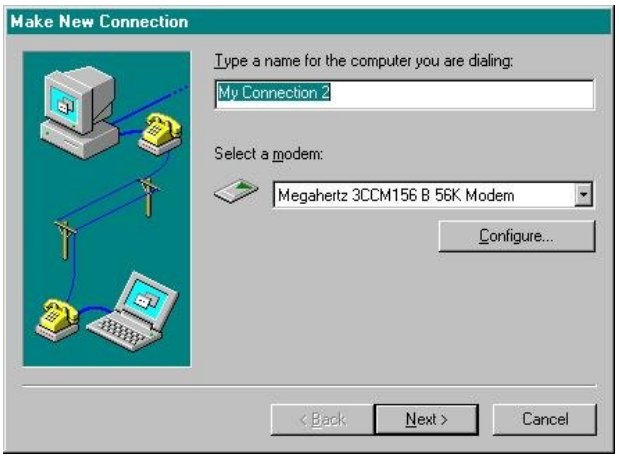
- Windows 95
- Windows 98
- Windows NT

For a Windows 2000 connection, see "Windows 2000 - Network Connection Settings" on page B-16.

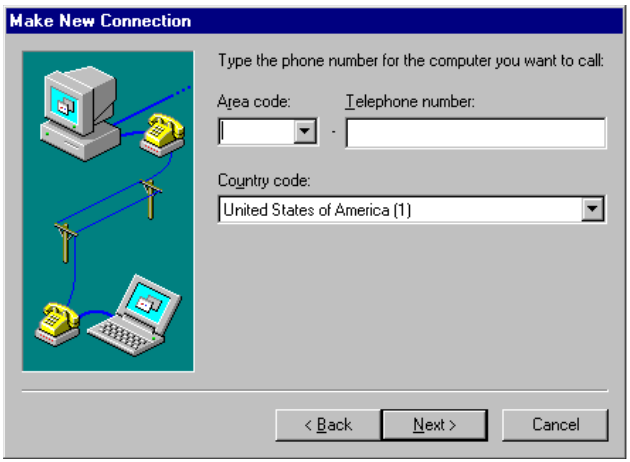
To make a new dial-up connection for Windows 95/98/NT:

1. On your PC access *My Computer*/*Control Panel* and select the *Dial-Up Networking* folder.
2. From the Windows Network and Dial-up Connections, establish a new connection by selecting the *Make New Connection* icon.

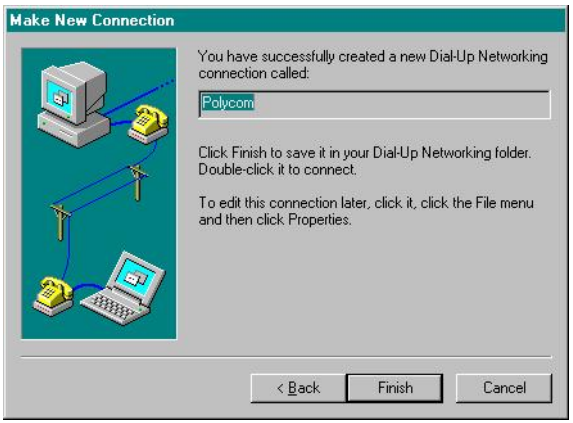
   The *Make New Connection* dialog box opens.



3. Assign a name to that connection (If you have more than one modem defined, you are also required to select the relevant one).
4. Click **Next**.

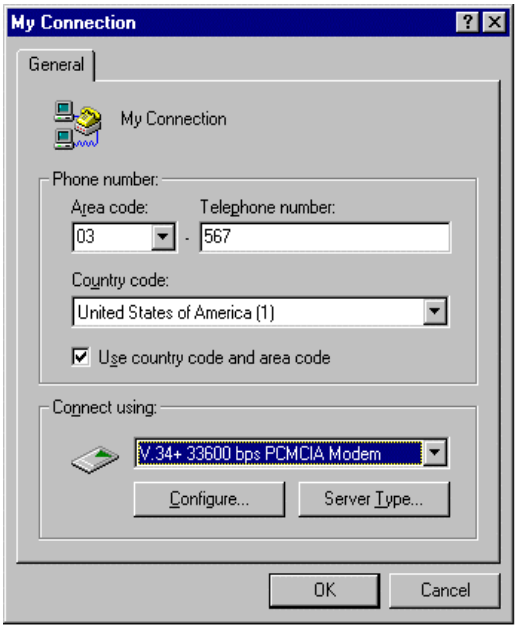


5. Type the phone number of the line connected to the MCU.
6. Click **Next**.



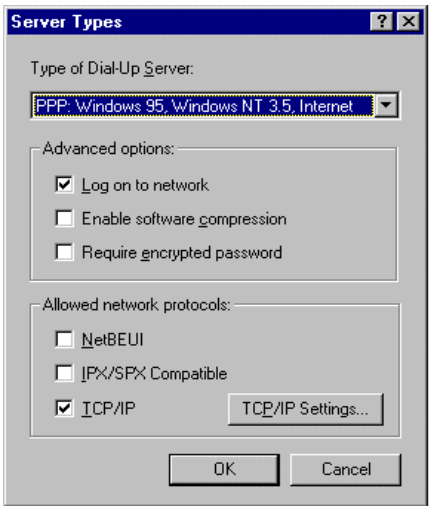
7. Click **Finish** to enter the connection in your dial-up connections window. At this stage, you should see a dial-up icon.
    a. To configure this connection, right-click on its icon, and choose **Properties**.

b. The *My Connection* dialog box opens:



c. Click the **Server Type** button.

d. The *Server Types* dialog box opens.



e. Configure it as follows (exactly as it appears in this screen):

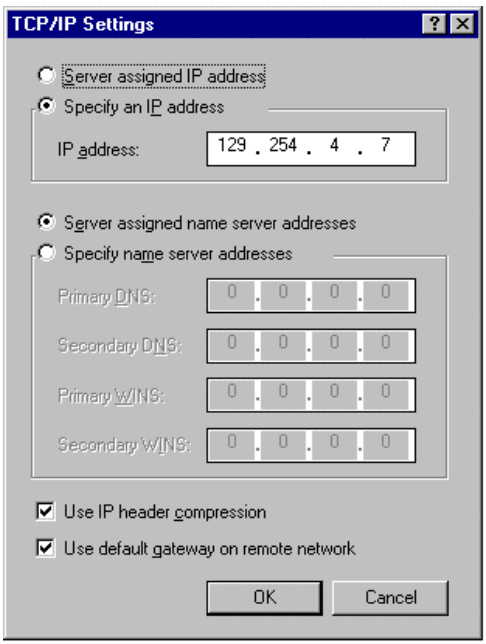
— *Type of Dial up Server* - **PPP: Windows 95, Windows NT 3.5, Internet**

— *Advanced options* - choose only **Log on to network**.

— *Allowed network protocols* - choose only **TCP/IP**.

f. Click the **TCP/IP Settings** button.

The *TCP/IP* dialog box opens.



g. Choose **Specify an IP address** and enter the IP address of your PC.

h. Choose **Server assigned name server addresses**.

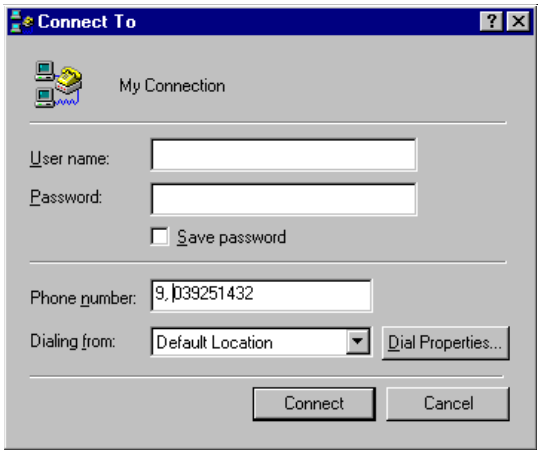
i. Choose both **Use IP header compression** and **Use default gateway on remote network**.

j. Choose **OK** on all dial-up networking windows that are still open.

8. Make a connection to the newly established configuration:

Double-click the *New Connection* icon.

The *Connect To* dialog box opens.



9. In the *User name* and *Password* fields use the following defaults:

   User name: POLYCOM

   Password: POLYCOM

   Or any other login profile configured within the MCU.

10. Click **Connect** to establish a connection.

11. Once the connection is established with the modem that is connected to the MCU, use the operator workstation application to connect to the MCU.

Windows 2000 - Network Connection Settings

To make a new dial-up connection for Windows 2000:

1. From the Start menu select the following path: **Programs**/**Accessories**/**Communications**/

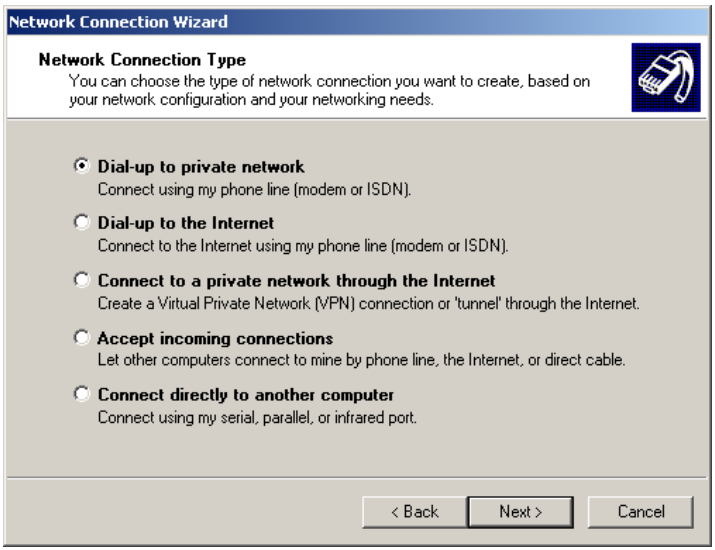
   Or

   On your PC access the Windows *Control Panel*.
2. Select **Network and Dial-up Connection.**
3. Double click the *Make New Connection* icon.

   The *Welcome to the Network Connection Wizard* dialog box opens.

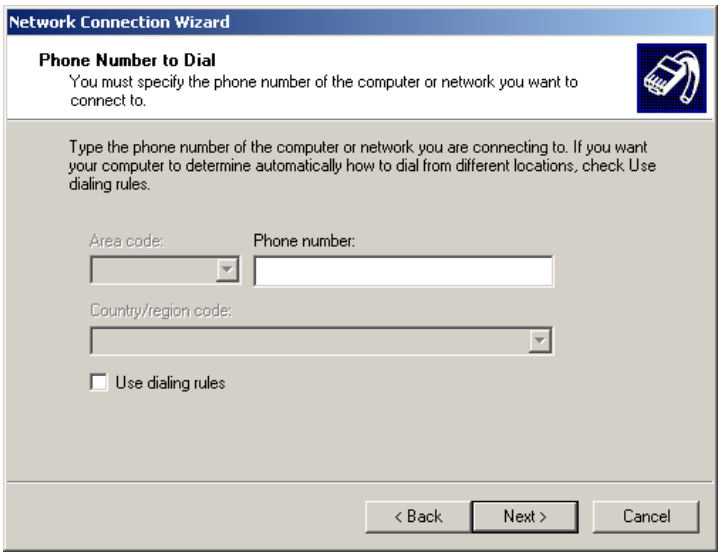
4. Click **Next**.

   The *Network Connection Type* dialog box opens.



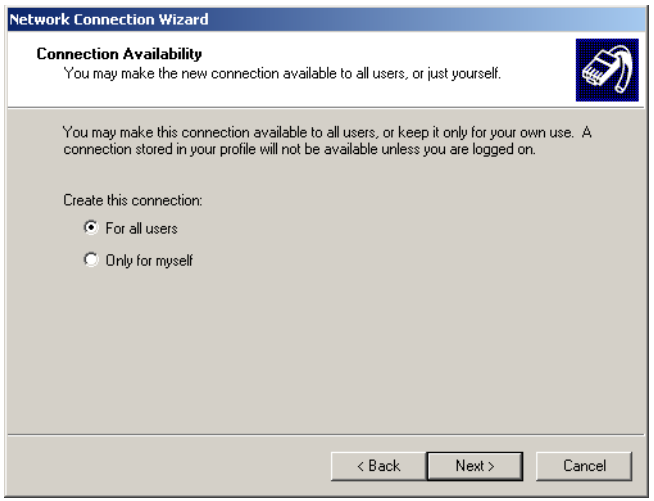
5. Select the default settings and click **Next**.

   The *Phone Number to Dial* dialog box opens.



6. Type the phone number of the line connected to the MCU.
7. Click **Next**.

   The *Connection Availability* dialog box opens.



8. Select the relevant connection and click **Next**.

   The *Completing the Network Connection Wizard* dialog box opens.

9. Enter the name of the network connection and click **Finish**.

Select any given name for your network.
In the previous dialog box, *Completing the Network Connection Wizard* the network has been given an arbitrary name: **MCU Connection.** This name designation is used in the Windows 2000 - Advanced Network Settings.

A new icon appears with the named MCU Connection.

Windows 2000 - Advanced Network Settings

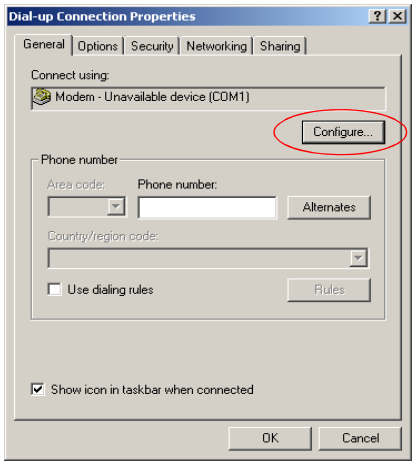
Establish a new dialup connection by using the following dial-up connection parameters (Properties):

- In the *Server Type* window, select the **PPP Windows 95/98/NT4/ Windows 2000, Internet** and check only the **Enter the Network** and the **TCP/IP** options.
- In the *TCP/IP definitions* window, enter only the Operator's IP address. Select the *Server Assigned Name* server address (you don't need to specify the MCU IP address). Check the options (**IP compression** and **Use default gateway**).

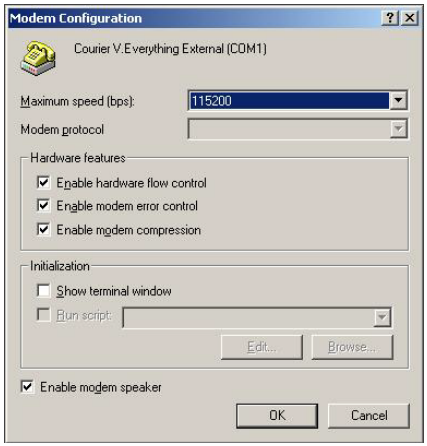
In order to activate the connection, double-click the **Dial-Up-Networking** icon created previously, enter the User name, Password and the Phone number, and then select **Dial**. As soon as the connection is established, the MGC Manager software can run and communicate with the MCU.

To define a new dial-up connection:

1. Double-click the *MCU Connection* icon.
   The *Dial-up Connection Properties* dialog box appears.

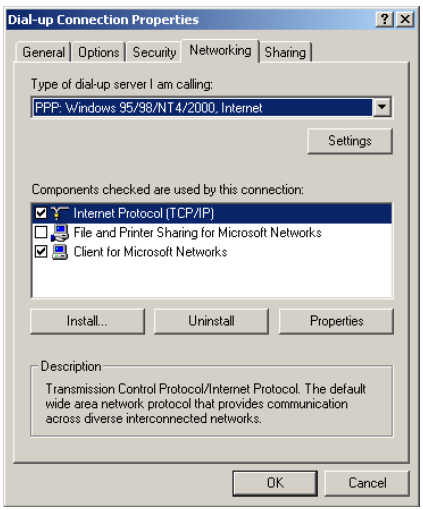


2. Click the **Configure** Button.
   The *Modem Configuration* dialog box appears:



3. Select **Maximum speed** (bps) and **Modem protocol** (if required).
4. Click **OK**, and you return to *Dial-up Connections Properties–General* dialog box.
5. Click the **Networking** tab.

The *Dial-up Connections Properties–Networking* dialog box appears.



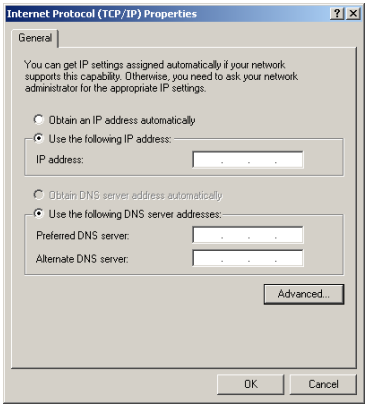
Configure this dialog box as follows (exactly as it appears in this screen):

— *Type of Dial up Server* - **PPP: Windows 95/98/NT4/ Windows 2000, Internet**.

— *Components checked are used by this connection* - choose **Internet Protocol TCP/IP**, **Client for Microsoft Networks**.

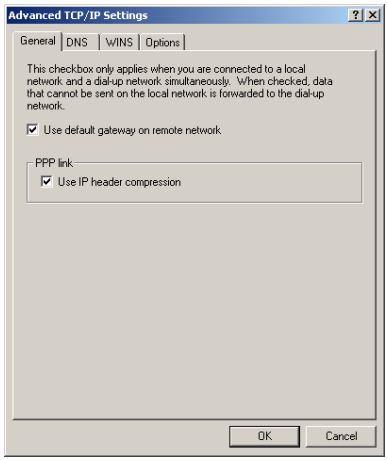
6. Highlight **Internet Protocol TCP/IP**.
7. Click the **Properties** button.

   The *Internet Protocol (TCP/IP) Properties* dialog box appears.



8. In the *General options* - select **Use the following IP address**.
9. Enter the MCU **IP address** and click the **Advanced** button.

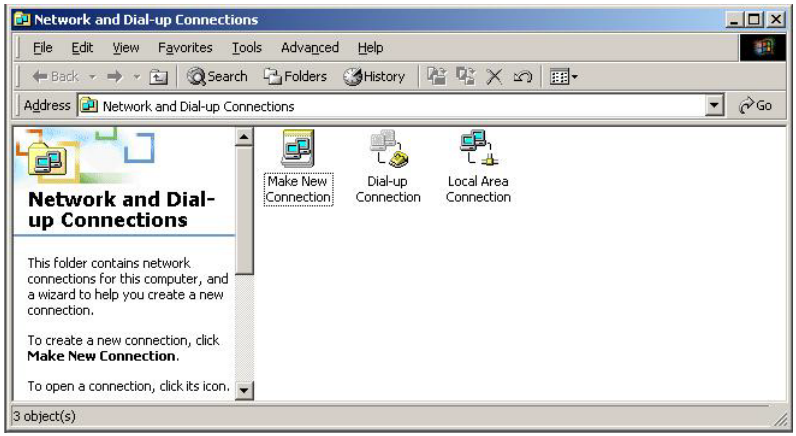
   The *Advanced TCP/IP Settings* dialog box appears.



10. Select both **Use default gateway on remote network** and **Use IP header compression**.
11. Click **OK** on all dial-up networking windows that are still open.

Connecting to the MCU using the new dial-up connection:

1. Select **Network and Dial-up Connection**.
   The *Network and Dial-up Connections* window opens.



2. In the Network and Dial-up Connections window double-click the *New Connection* icon.
   The *Connect Dial-up Connection* dialog box opens.

3. In the **User name** and **Password** use the following defaults:

   User name: POLYCOM

   Password: POLYCOM

   Or any other operator login profile configured within the MCU.

4. Click **Dial** to establish a connection.

5. Once the connection is established with the modem that is connected to the MCU, use the MGC Manager application to connect to the MCU.

Appendix C: Performance Monitoring NET-T1/Net-E1

The MGC Manager application enables you to produce statistical information on the performance of the ISDN lines connected to the Net-T1/ Net-E1 Network Interface module installed in the MCU. According to the statistical data presented by the system, you can ascertain the reasons for the connection problems during conference startup. If the problems affecting the quality of the line and service persist, they can be forwarded to the service provider. The Performance Monitoring option relates to the connection between the Net Access Network Interface module installed in the MCU and the first switch.

The Performance Monitoring option is available only for Net-T1/Net-E1 Network Interface modules and not for NET-2/4/8 modules.

The ISDN performance can be monitored in two modes: automatic and manual.

In the automatic mode, the status of the ISDN line is constantly monitored for common error conditions. When the number of occurrences of any of the monitored conditions exceeds a predefined threshold, the system issues a warning message (which appears in the Faults list) and the MCU status changes to Minor.

In the manual mode, the statistics of a specific ISDN line are retrieved for the last monitored time interval, depending on the selected interval. The E1 or T1 lines are monitored in 15-minute and 24-hour intervals. In a 15-minutes interval, the network card collects the number of occurrences for the various error conditions and accumulates them. At the end of the 15 minutes, these counters are initialized. In a 24-hour interval, the system accumulates the number of occurrences of each of the error conditions in the

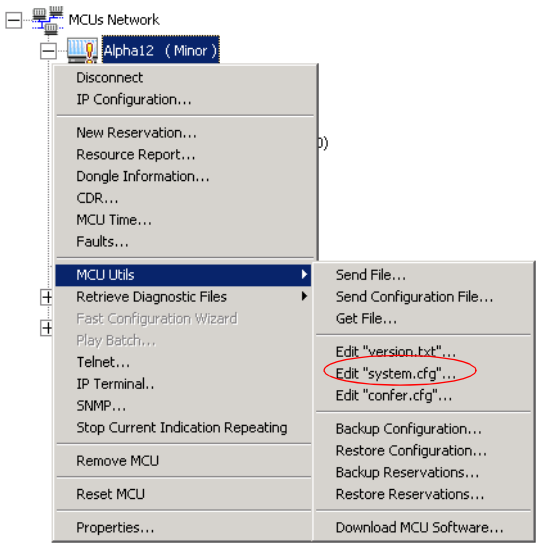
96 intervals of 15 minutes. You can view the statistics for the last 15 minutes or for the last 24 hours.

Automatic Performance Monitoring

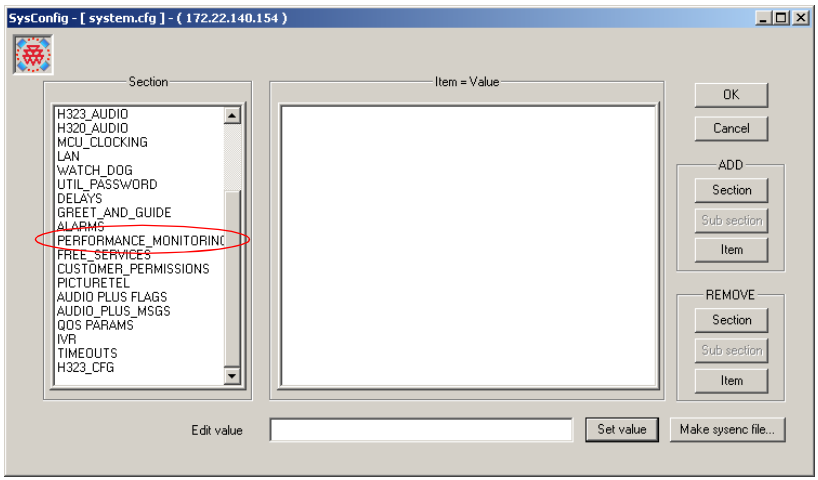
To enable the Automatic Performance Monitoring and to define the time-out period, you must access and edit the parameters in the “system.cfg” file.

To modify the “system.cfg” file:

1. In the *Browser* pane, right-click the *MCU* icon, click **MCU Utils**, and then click **Edit “system.cfg”**.

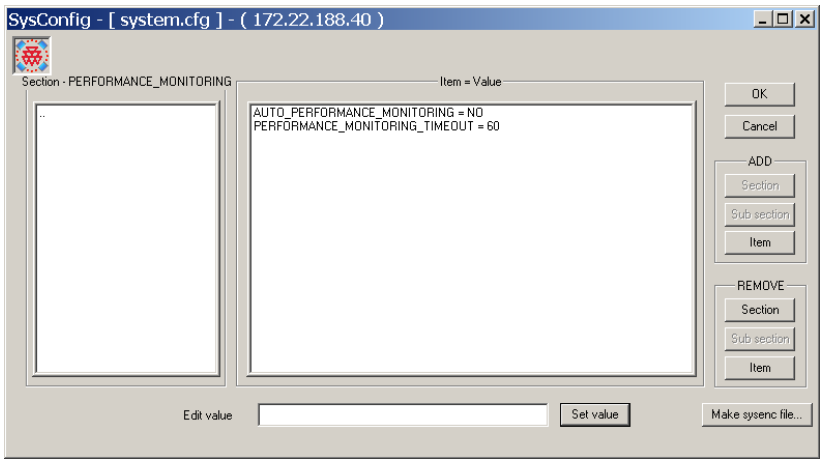


The *SysConfig* dialog box opens.



2. In the *Section* box, double-click **PERFORMANCE_MONITORING**

   The various Performance Monitoring flags are listed in the *Item = Value* box.



3. Set the AUTO_PERFORMANCE_MONITORING flag to **YES**

   a. In the *Item = Value* box, click **AUTO_PERFORMANCE_MONITORING**

   b. In the *Edit Value* box, type **YES**.

c. Click the **Set Value** button.

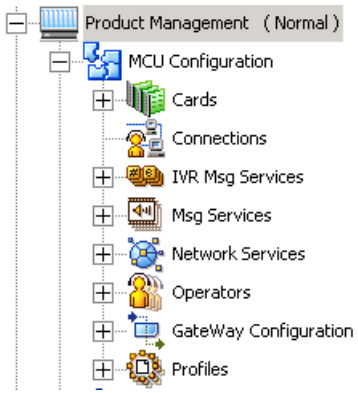
4. Set the PERFORMANCE_MONITORING_TIMEOUT flag to the required value.
5. Click **OK**.

Manual Performance Monitoring

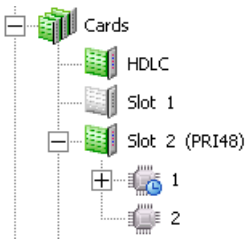
Use this option to monitor the state of a specific ISDN line in the last 15 minutes or 24 hours and ascertain whether there are quality problems, which should be forwarded to the service provider of the ISDN line.

To retrieve the statistical information regarding an ISDN span:

1. Connect to the MCU whose modules you want to list.
2. In the *Browser* pane, expand the tree to list its options.
3. Double-click **MCU Configuration** icon, or click the plus [+] icon next to the *MCU Configuration* icon.
   A list of options appears below the *MCU Configuration* icon.
4. Double-click the *Cards* icon or click the plus [+] icon next to the *Cards* icon, to list the cards installed in the MCU.



A list of slots appears.

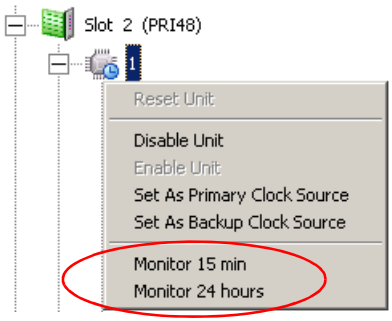


5. Click the slot containing the Net-T1/Net-E1 Network Interface module (PRI48) to configure, or click the plus [+] icon next to the card icon, to list its spans.

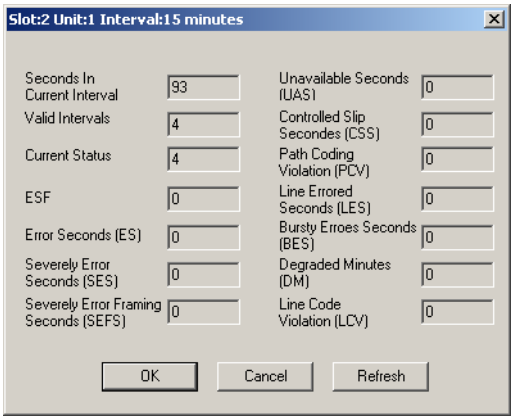
6. Right-click the unit whose ISDN line quality you want to check, and then select:

   Monitor 15 min to retrieve statistical data on the line quality in the last 15 minutes.

   Monitor 24 hours to retrieve statistical data on the line quality in the last 24 hours (in 15 minute intervals).



The *Performance Monitoring* dialog box opens.



The dialog box heading indicates the span being monitored and the monitoring time interval.

Table C-1, "Performance Monitoring Options." describes the monitored parameters.

Table C-1: Performance Monitoring Options

Error Condition	Description
Seconds In Current Interval	Indicates the number of actual seconds within the 15 minute interval. Possible values are from 0 to 900 seconds.
Valid Intervals	Indicates the number of valid 15 minute intervals in the last 24 hour period. Possible values are from 0 to 96 minutes. This field only applies when you are monitoring the performance over a 24 hour period.
Current Status	Indicates the current status.
ESF	Refers to errors on a T1 line, specifically when the frame structure cannot be found.

Table C-1: Performance Monitoring Options (Continued)

Error Condition	Description
Error Seconds (ES)	ES is a second with one or more Path Code Violations (PCV), or one or more Out Of Frame (OOF) defects, or one or more Controlled Slip (CS) events, or where AIS defects have occurred.
Severely Error Seconds (SES)	SES is a second with 320 or more Path Code Violation (PCV) error events, or one or more Out Of Frame (OOF) defects, or where AIS defects have occurred.
Severely Errored Framing Seconds (SEFS)	SEFS is a second with one or more Out Of Frame (OOF) defects, or where AIS defects have occurred.
Unavailable Seconds (UAS)	Unavailable Seconds are calculated by counting the number of one-second intervals during which the ISDN line is unavailable as a result of 10 contiguous SES errors, or when there are yellow and red alarms, CRC errors or synchronization problems.
Controlled Slip Seconds (CSS)	Controlled Slip Seconds are calculated by counting the number of one-second intervals during which one or more Controlled Slip events occurred.
Path Code Violation (PCV)	A frame synchronization bit error. See detailed explanation above.
Line Errored Seconds (LES)	A second in which one or more Line Code Violation error events were detected.
Bursty Errored Seconds (BES)	A second in which fewer than 320 and more than one Path Code Violation error events were detected.
Degraded Minutes (DM)	A condition when one or more of the established performance parameters fall outside predetermined limits and results in a lower quality of service.

Table C-1: Performance Monitoring Options (Continued)

Error Condition	Description
Line Code Violation (LCV)	See detailed explanation above.

Handling the Performance Monitoring Errors

If *Line Code Violation* errors are indicated, make sure that the Line Coding option selected in the Network Service properties is identical to the actual Line Coding used by the service provider. If necessary, contact the service provider for further information.

If *Path Code Violation* errors occur, make sure that the network line is properly connected to the MCU and that the network cable is firmly inserted into the 8-pin RJ45 connector. Ask the service provider to check the connectivity of the line to the switch at the far end.

If there are many *CSS* errors this may indicate a synchronization problem as a result of no clock signal. Check the clock configuration of the network cards.

D

Appendix D: The Falcon Diagnostic Tool

The Falcon diagnostic tool is an add-on to the MGC application that enables you to run diagnostic tests on the hardware and software of the MGC-25, MGC-50 and the MGC-100 units. The Falcon diagnostic tool is used by the integration team to test all new units or applicable cards that are installed on the system. This ensures that all new elements run properly. This tool is also used by Polycom support personnel or the customer's System Administrator to provide data for checking the hardware performance. When running the Falcon Diagnostic tool, it is best to run all the available tests on each applicable card to locate any problem in the hardware. If a fault is discovered, it should be reported to Polycom support personnel. More specific diagnostic tests can then be run on the units.

The Falcon diagnostic tool runs diagnostic tests on the following cards on:

MGC-50/100:

- The Audio+ cards
- The Video+ cards
- The IP+ cards
- MUX+ cards (from version 7.01)

MGC-25:

- The Audio+ card
- The Video+ card
- The IPN card

On the MGC-25 unit, the IPN card can be configured as a virtual NET-2, IP+ and MUX+ cards. The Falcon diagnostic tool displays the NET-2 and the two processors (IP+ and MUX+) as IPN card units. The Audio+ and Video+ cards are displayed in the diagnostic tool as they are actually installed. These parameters can be viewed in the card Properties - Card Settings dialog box.

Test Description

The following table lists the diagnostic tests performed, by card and unit. The tests differ depending on the selected card and unit. For a description of the terms that appear in the table, see "Test Glossary" on page D-24.

Table D-1: Diagnostic Tests

Card	Unit	Test	Description
IP+ (MGC-50, MGC-100)	CM	Local memory	Checks buses' data and addresses. Checks memory integrity and capacity.
	Proc	Clock	Checks the frequency rate of the processor.
		Local memory	Checks buses' data and addresses. Checks memory integrity and capacity.
		Neighbor	Checks the *PCI* access between processors.
		Clock	Checks the frequency rate of the processor.
		LAN	This test requires that a LAN cable be connected to the I/O of the card. See "Connecting the LAN and ISDN Loopback cables" on page D-15. Checks the *ping* between the card and the Falcon host machine IP Address.
		TDM	Creates a loop between the DSP through the backplane and back to the DSP to check data transfer through the loop.
		Full memory	Checks all the processing memory of the card manager.

Table D-1: Diagnostic Tests (Continued)

Card	Unit	Test	Description
IPN (MGC-25 only)	NET-2	ISDN-Loopback	The Falcon diagnostic tool displays the NET-2 card as a unit in the IPN card. This test checks the ISDN hardware. To run this test, an ISDN Loopback cable must be connected to the Network I/O card. For more details, see “Connecting the LAN and ISDN Loopback cables” on page D-15.
	Proc	Clock	Checks the frequency rate of the processor
		Local memory	Checks buses’ data and addresses. Checks memory integrity and capacity.
		Neighbor	Checks the *PCI* access between processors.
		LAN	This test requires that a LAN cable be connected to the I/O of the card. See “Connecting the LAN and ISDN Loopback cables” on page D-15. Checks the *ping* between the card and the Falcon host machine IP Address.
		TDM	Creates a loop between the DSP through the backplane and back to the DSP to check data transfer through the loop.
		Full memory	Checks all the processing memory of the card manager.

Table D-1: Diagnostic Tests (Continued)

Card	Unit	Test	Description
MUX+	CM	Local memory	Checks buses' data and addresses. Checks memory integrity and capacity.
		LAN	Checks the *ping* between the card and the Falcon host machine IP Address.
	Proc	Local memory	Checks buses' data and addresses. Checks memory integrity and capacity.
		Full memory	Checks all the processing memory from the card manager.
		Neighbor	Checks the *PCI* access between processors.
		Clock	Checks the frequency rate of the processor.
		TDM	Creates a loop between the DSP through the backplane and back to the DSP to check data transfer through the loop.

Table D-1: Diagnostic Tests (Continued)

Card	Unit	Test	Description
Audio+	CM	PCI	Scans the *PCI* to ensure that its components are working properly.
		TDM	Creates a loop between the DSP through the backplane and the QIFI then back to the DSP via the time slot switch to check data transfer through the loop.
		QIFI	Checks the watchdog.
		Memory	Checks buses' data and addresses. Checks memory integrity and capacity.
	Proc	Clock	Checks the frequency rate of the processor.
		Memory	Checks buses' data and addresses. Checks memory integrity and capacity. Checks burst and data bus energy changes.

Table D-1: Diagnostic Tests (Continued)

Card	Unit	Test	Description
Video+	CM	PCI	Scans the PCI to ensure that its components are working properly.
		Memory	Checks buses' data and addresses. Checks memory integrity and capacity.
		TDM	Creates a loop between the DSP through the backplane and the BCOD then back to the DSP via the time slot switch to check data transfer through the loop.
		BCOD	Checks the watchdog and *BCOD* memory.
	Proc	Memory	Checks buses' data and addresses. Checks free memory.
		Clock	Checks the frequency rate of the processor.

MCU Level Tests

When the Falcon diagnostic tool is run at the MCU level, all available tests are run on all the recognized cards installed on that MCU and their units. Several MCUs can be tested simultaneously, and their tests run serially.

Card Level Tests

When the Falcon diagnostic tool runs tests on an installed recognized card, it performs all the available tests on all the card's component units. You can test all cards of a certain type, for example, all the Video+ cards. All tests run on the Falcon diagnostics tool are run serially rather than simultaneously.

Unit Level Tests

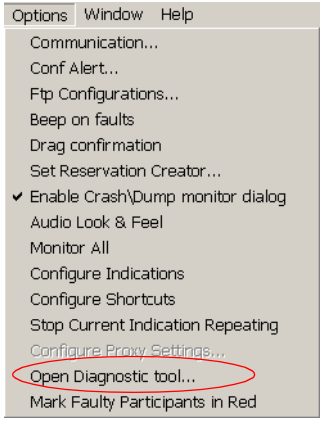
At the unit level, tests can be selected individually. A specific test, for example, the TDM test, can be run on all cards installed on the MCU as long as each test is initiated individually. The tests run serially.

Using the Falcon Diagnostic Tool

The Falcon tool is part of the MGC Manager *Options* menu.

To Start the Falcon Diagnostics Tool:

1. Terminate all On Going Conferences and cancel any soon to open Reservations on the MCUs to be tested.
2. In the *Options* menu, select **Open Diagnostics tool**.

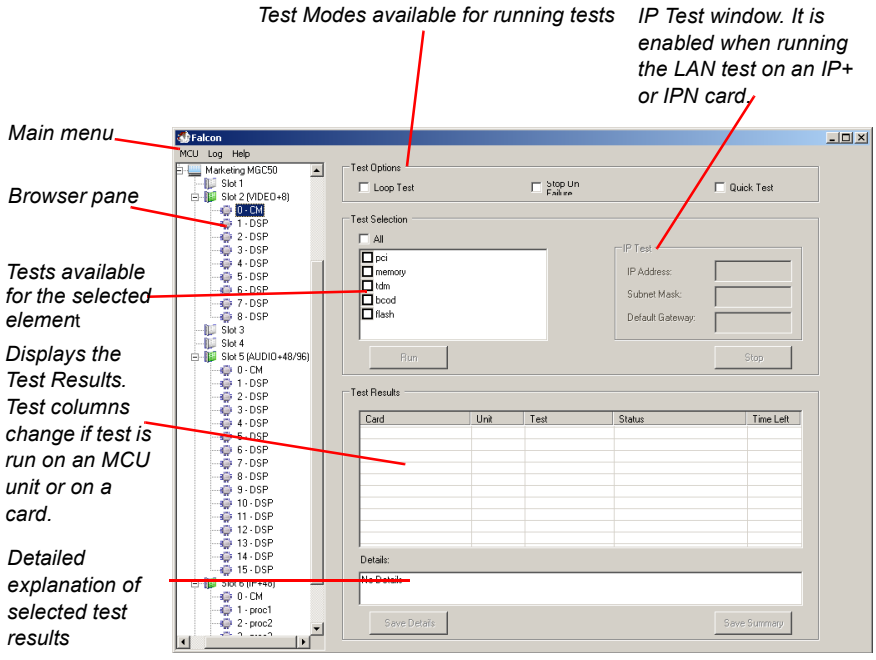


The Falcon diagnostics tool opens.

The Falcon diagnostics tool displays all the MCUs currently defined in the MGC Manager, see “Falcon Main Window” on page D-9. You can define other MCUs so they can be displayed in the MGC Manager and in the Falcon tool.

The MCU network is displayed in a *Browser* pane on the left side of the Falcon screen.

Falcon Main Window



Browser Pane

Displays the MCUs defined in the MGC Manager application. Each MCU tree can be expanded to display the cards supported for diagnostic tests.

Main Menu

The *Main Menu* includes the MCU, Log and Help menus.

Table D-2: Falcon Main Menu Description

Field	Description
MCU	Contains the following options: • ***Add MCU*** - To define a new MCU and add it to the MCU list. This option is required only for MCUs that are not currently defined in the MGC Manager application. • ***Connect*** - Connects an MCU to the application. • ***Disconnect*** - To disconnect an MCU from the Falcon diagnostic tool, while resetting the MCU. • ***Reset MCU*** - To reset the MCU without disconnecting the MCU. • ***Remove MCU*** - This option removes the MCU from the MCU list. • ***Properties*** - Lists the MCU properties: MCU Name, IP Address, Product Type (MGC-25/50/100), MCU Version, and the MCSM version.
Log	Contains the following options: • ***Set Log File Path*** - Enables you to select the folder where the log file will be saved. • ***Only Faults*** - Click this option to save only Faults in the Log file.
Help	Contains the following options: • ***About Falcon*** - Lists the Falcon diagnostic tool version. • ***Falcon Help*** - Provides On Line Help for the application.

Test Options Box

The *Test Options* box displays the modes for running tests.

Table D-3: Test Options Description

Field	Description
Loop Test	Sets tests to repeat continuously in a loop mode. This provides continuous testing for these diagnostics.
Stop on Failure	In this mode tests are run continuously until a failure is detected. The diagnostic testing then stops.
Quick Test	Enables running tests that do not run longer than 5 minutes. On the MGC-25, all tests run as they all take less than 5 minutes to run.

If no selection is made in the *Test Options* box, the tests will run one time.

Test Selection

The *Test Selection* box displays the tests that are available for the selected element.

All - Selects all the diagnostic tests to run. Tests vary depending on the selected MCU component, for details, see Table D-1 on page D-3. When the MCU icon or card icon is selected, all tests are run by default. When a card unit is selected, tests can be selected individually.

Run button - Initiates the diagnostic tests that are selected.

Stop button - Terminates on going diagnostic tests.

IP Test Box

The *IP Test* box is active during the *LAN* test. The *IP Address*, *Subnet Mask* and *Default Gateway* information must be entered. If these parameters are not entered, a pop-up box appears when the diagnostics run the LAN test, and these fields must be entered at that time. You can cancel the LAN test instead of entering the IP Test values.

IP Address - This is the address of the card and should be provided by the System Administrator.

Subnet Mask - This is provided by the System Administrator.

Default Gateway - This is necessary to test the LAN Controller.

Test Results Pane

As the tests are run, the results are displayed in the *Test Results* table. A log report is written containing these results.

The test categories depend on what tests are run. When the MCU icon is selected in the Browser pane, two categories are displayed: *Card* and *Status*. When the cards or units are selected, there are five categories displayed in this window:

Table D-4: Test Selection Categories and Descriptions

Field	Description
Card	Displays the name of the card and its serial number.
Unit	Identifies the unit on the card.
Test	Identifies the test.
Status	Describes whether or not the test was completed, if it timed out, whether the test passed or failed.
Time Left	Lists the time left to run on the test.

When you click on a test result (a row) in the summary table, the test details are displayed in the *Details* box.

The two buttons below the *Details* box determine how the test results are saved in the log report.

Save Details - Saves the details as they appear in the *Details* box.

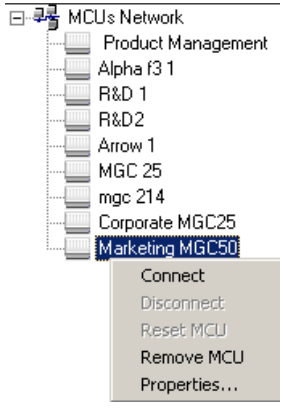
Save Summary - Saves the table in the *Tests Results* pane to the Falcon Logs folder. The log is named using the MCU name, Slot ID, Card name, Unit, Processor and Word summary.

Connecting to an MCU

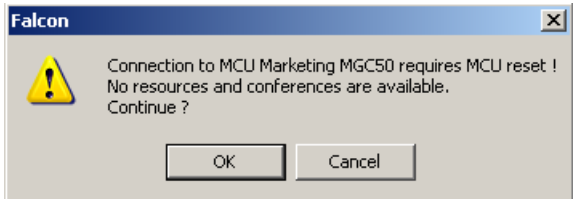
Before running the diagnostic tests on an MCU, you must connect the MCU to the Falcon diagnostic tool.

To connect the Falcon diagnostic tool to a specific MCU:

1. Double-click on the selected *MCU icon* or right-click on the *MCU icon* and click **Connect** from the right mouse menu or the Main menu options.



A message appears indicating that the MCU must be reset in the *Falcon* mode.



2. Click **OK**.

You must close all On Going Conferences before opening the Falcon diagnostic tool. If a conference is running when you try to connect to an MCU, an error message is displayed indicating that you must first close the On Going Conference.

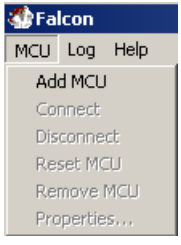
When the Falcon diagnostic tool resets the MCU, it identifies the MCU cards that can be tested. Cards that cannot be tested are displayed in the MGC Manager but not in the Falcon tool.

Adding an MCU to the Network

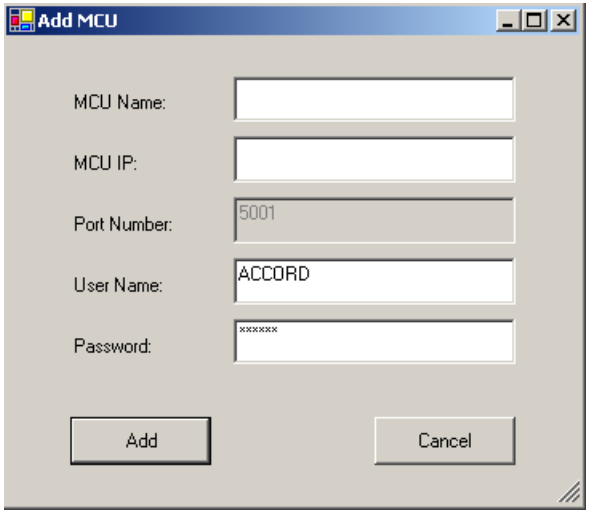
To add an MCU to the MCU Network:

1. Right-click the MCU Network icon, and then click Add MCU.

2. Alternatively, on the MCU menu, click Add MCU.



3. The *Add MCU* dialog box opens.



4. In the *Name* box, enter the name of the MCU. Specify a name that clearly identifies the MCU.
5. In the *IP Address* box, enter the IP Address of the MCU. The correct IP address should be obtained from your network administrator.

6. The correct *Port Number* appears in the dialog box.
7. Enter the user name of the MCU in the *User Name* field.
8. Enter the MCU password in the *Password* field.
9. Click the **Add** button. The *Add MCU* dialog box closes. A new icon with the specified MCU name appears in the *Browser* pane below the MCUs *Network* icon.

Running Diagnostic Tests

After you connect to an MCU, you can run the diagnostic tests. The Falcon tool reads the available cards in the MCU, and a list of tests relevant to the selected element is displayed in the Test Selection box. For a list of the specific tests run on each element, see "Diagnostic Tests" on page D-3.

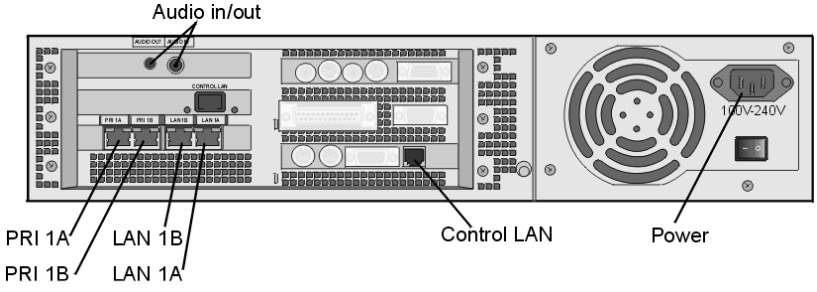
Connecting the LAN and ISDN Loopback cables

If you run a LAN test on an IP+ or IPN card, or an ISDN Loop test on an IPN card, you must connect the ISDN Loopback or LAN cables to the MCU before you run the diagnostic tests.

PPP (Point to Point Protocol) support enables the operator to establish TCP/IP communication with the MCU over a telephone line with a modem, or directly by means of a serial connection. If a modem connection is used, the modem must be connected to one of the MCU's serial connectors. If a direct line connection is used, the remote station must be connected to the MCU by means of a Null Modem cable. When the PPP is used, there is no need to run the LAN test. If you do not fill in the IP Test box, a pop-up box appears when the LAN test is about to run. You can cancel the LAN test at that time.

To connect the LAN cable and the ISDN Loopback cable to the MGC-25 unit:

1. On the MGC-25 unit, ensure that the Control LAN cable is connected to the Control LAN port.



2. Ensure that a second *LAN* cable is connected to the LAN 1A port. These two cables are necessary to run the LAN diagnostic tests on the installed IPN cards.
3. Connect the *ISDN Loopback* cable that comes with the unit to the *PRI 1A* and *PRI 1B* ports on the MGC-25 unit. This is necessary to run the ISDN Loop Test on the IPN card.

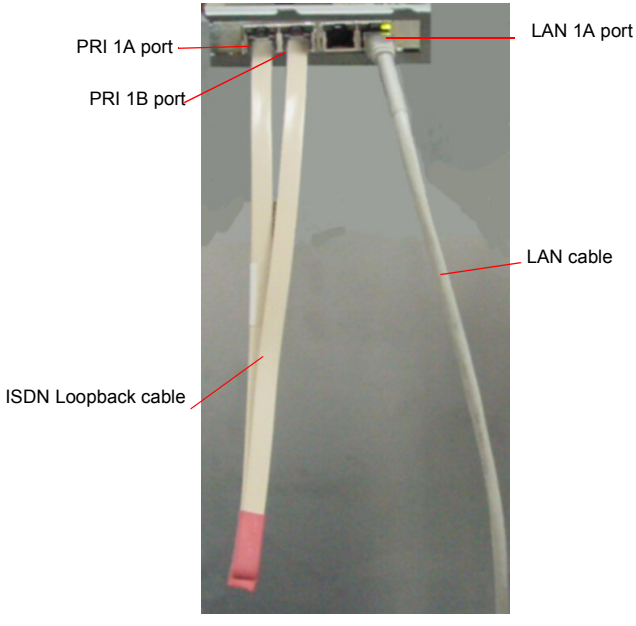
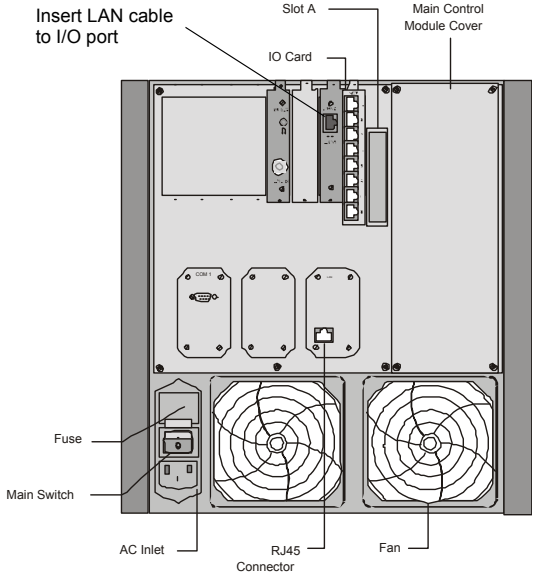


Figure D-1: ISDN Loopback Cable Connected to PRI 1A and PRI 1B Ports on the Back of the MGC-25

To connect the LAN cable to an MGC-50 unit:

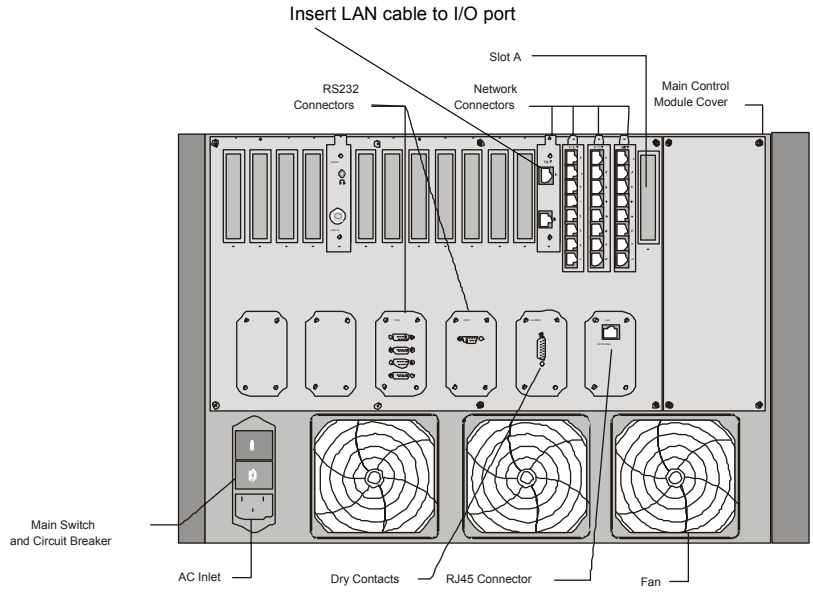
1. Ensure that the Control LAN cable is connected to the RJ 45 Connector port.
2. Connect a *LAN* cable to the *I/O* port of any installed IP+ card. This is necessary to run the diagnostic tests on the installed IP+ cards. There is no ISDN Loop test on an MGC-50 or MGC-100.



To connect the LAN cable to an MGC-100 unit:

1. Ensure that the Control LAN cable is connected to the RJ 45 Connector port.

2. Connect a *LAN* cable to the *I/O* port on the back of any IP+ card to be tested.



Running the Tests at the MCU Level

To run the diagnostic tests:

The LAN test and the ISDN Loop test are automatically run at the MCU level testing, so connect the ISDN Loopback and LAN cables to the MCU before running the tests. For more details, see “Connecting the LAN and ISDN Loopback cables” on page D-15.

1. Connect to all the MCUs that must be tested.
2. In the Test Options box, select the test mode. For a detailed description of the three modes, see “Test Options Box” on page D-11.

   For a description of how to connect the LAN or ISDN Loopback cables, see “Connecting the LAN and ISDN Loopback cables” on page D-15.

   At the MCU level, the LAN test is automatically run and therefore, the IP Test fields must be filled in. For a detailed description of the IP Test fields, see “IP Test Box” on page D-11.
3. Select a test mode in the *Test Options* box. For a description of the test selection options, see “Test Selection” on page D-11.

4. Click the **Run** button. The test results appear in the *Test Results* pane as the tests occur. For a detailed description of the *Test Results* pane, see "Test Results Pane" on page D-12.

Running Tests at the Card Level

Once you are connected to an MCU, you can expand the MCU tree to display its cards. This enables you to run the diagnostic tests on individual cards without having to run the test series on all the cards that are installed. You can set multiple tests to run at once, but they will run serially rather than simultaneously.

To run diagnostic tests on cards:

When you run the diagnostic tests on a specific card, all available tests are performed on that card.

If you run a LAN test on an IP+ or IPN card, or an ISDN Loop test on an IPN card, you must connect the ISDN Loopback or LAN cables to the MCU before you run the diagnostic tests. For a description of how to connect the LAN or ISDN Loopback cables, see "Connecting the LAN and ISDN Loopback cables" on page D-15.

1. In the *Browser* pane, expand the selected MCU tree.
2. Select the cards to test.
3. In the *Test Options* box, select the test mode. For a detailed description of the three modes, see "Test Selection" on page D-11.
4. If you have an IP or IPN card installed on your MCU, one of the tests that is run is the *LAN* test. To complete the LAN test, you must fill in the *IP Test* fields. For a description of completing the *IP Test* fields, see "IP Test Box" on page D-11.
5. Click the **Run** button

   The test results appear in the *Test Results* pane. For a detailed description of the *Test Summary* pane, see "Test Results Pane" on page D-12.

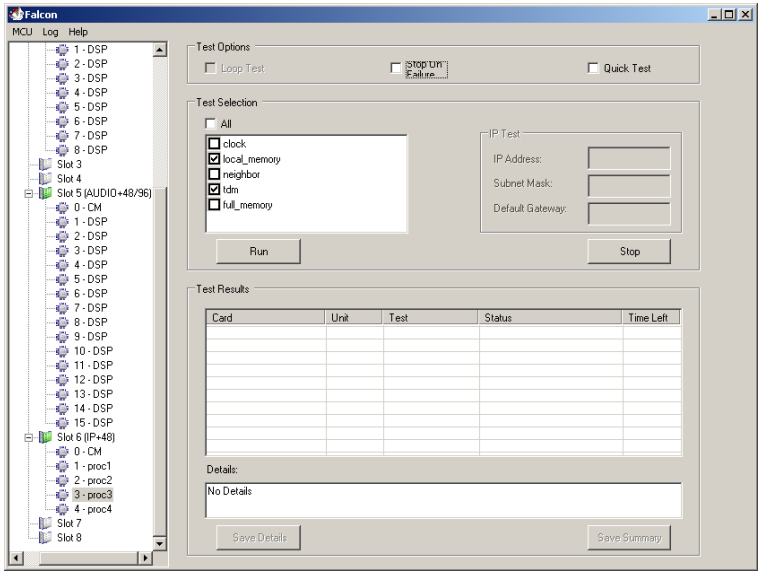
Running Tests at the Unit Level

The card unit tests are usually run by Polycom personnel.

If you run a LAN test on an IP+ or IPN card units, or an ISDN Loop test on an IPN card, you must connect the ISDN Loopback or LAN cables to the MCU before you run the diagnostic tests. For a description of how to connect the LAN or ISDN Loopback cables, see “Connecting the LAN and ISDN Loopback cables” on page D-15.

To run diagnostic tests on card units:

1. In the Browser pane, expand the selected MCU tree.
2. In the Test Options box, select the test mode. For a detailed description of the three modes, see “Test Selection” on page D-11.
3. Expand the Card tree to display its units.
4. Select the card unit on which the diagnostic tests are to be performed. The *Test Selection* window displays the available tests for that card.



5. In the *Test Selection* window select the diagnostic tests to be performed.
6. If you have an IP or IPN card installed on your MCU, one of the tests that is run is the *LAN* test. To complete the LAN test, you must fill in the

IP Test fields. For a description of completing the *IP Test* fields, see "IP Test Box" on page D-11.

7. Click **Run**.

   The test results appear in the *Test Results* pane. For a detailed description of the Test Summary pane, see "Test Results Pane" on page D-12.

Post Testing Procedure for MGC-25 Units

- After all the tests have been completed on an MGC-25 unit, remove the ISDN Loopback cable.

To save the table that is displayed in the Tests Results window to the Falcon Logs folder:

- In the *Test Results* pane, click the **Save Summary** button. The log is named using the MCU name, Slot ID, Card name, Unit, Processor and Word summary.

To save the faults details as they appear in the Details box:

- After the tests are completed, click the **Save Details** button in the *Test Results* pane.

The Test Results, Faults and Summaries are saved together with the Log files in the folder designated for that purpose when the Log file path was set. These files can be sent to support personnel to help them understand any problems with the hardware that may appear after the diagnostics are run.

Test Results

The test results appear dynamically in the *Test Results* pane as the tests run.

Whenever you connect to an MCU, a new log file is started. All Falcon functions are saved to a log file. The *Log* option in the main menu enables you to define the location of the folder where the log files are sent. You can restrict the logs to record only detected faults discovered during a diagnostic test. These log files can be sent to your System Administrator to help resolve any problems that might occur. In addition, any Test Results or Test Summaries are sent to the folder in which the log files are stored.

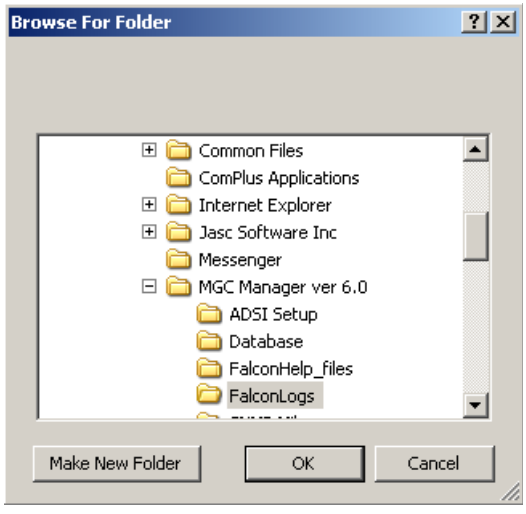
If you save *Only Faults* in the *Log* menu, files with just the faults discovered in the test results will be available in the log file folder. Otherwise, all the results are recorded.

To set the Log file path:

1. In the *Log* menu, click **Set Log File Path**.

   A browser opens to set the log file path.

2. Select the Folder to store the log files and click **OK**.



To filter the log file to list only the test faults:

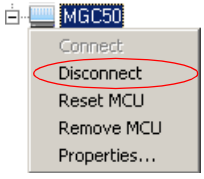
- In the *Log* menu, click **Only Faults**.

Disconnecting from the Falcon Diagnostic Tool

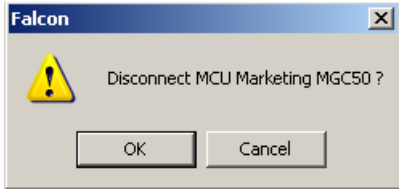
Disconnecting from the Falcon diagnostic tool resets the MCU and puts it back into *Normal* mode. If the MCU is not connecting properly in the MGC Manager Application, this option is a good way to restore the connection. This is also the recommended way to close the Falcon tool.

To disconnect from the Falcon diagnostic tool:

1. Right-click the MCU icon and then select **Disconnect**. Alternatively, on the MCU menu, click **Disconnect**.



A pop-up window appears prompting you to confirm the selection.



2. Click **OK**.

The MCU disconnects from the Falcon diagnostic tool and is reset. At the end of the reset, the MCU status is restored to *Normal* mode.

Test Glossary

The following Test Glossary describes the terms used in the diagnostic tests in the table: “Diagnostic Tests” on page D-3.

Table D-5: Diagnostic Test Terms

Test Term	Description
BCOD	An *FPGA* unit on the Video+ card.
CM	Card Manager
DSP	Digital Signal Processor, a special type of programmable co-processor, designed for performing the mathematics used for manipulating different types of information in the Audio+ card.
FPGA	Field-Programmable Gate Array, a type of programmable logic chip.
PCI	Peripheral Component Interconnect, a 64-bit bus, though it is usually implemented as a 32-bit bus.
Proc	Processor.
QIFI	An *FPGA* unit on the Audio+ card.
TDM	Time Division Multiplexing, a type of combination of multiple signals (analog or digital) for transmission over a single line or media that combines data streams by assigning each stream a different time slot in a set.

Log File Report Examples

The following is an example of the Log File Report as it might appear after you run the Falcon diagnostic tool. Note that the log file lists initiation and end of tests that were run.

Example Log Report

```
02/05/2005 15:30:00,937: *** Falcon Log File Created, version 1
02/05/2005 15:30:00,937: *** For MCU: 172.22.175.171
02/05/2005 15:30:00,937: ************************************
02/05/2005 15:30:00,937: *** Logged Messages Filter: All Messages (no filter)
02/05/2005 15:30:00,947: Test Engine started
02/05/2005 15:30:00,957: Falcon: level -g
```

Connection established with MCU

```
02/05/2005 15:30:00,967: Falcon: mgc_diag YES
```

Disconnected from MCU

```
02/05/2005 15:30:27,596: MCU Connected!
```

Connection re-established with MCU

```
02/05/2005 15:30:27,606: Falcon: level -g
02/05/2005 15:30:27,736: Falcon: am 1 0 diag.gettestlist.service
02/05/2005 15:30:27,746: Falcon: am 2 0 diag.gettestlist.service
02/05/2005 15:30:27,756: Falcon: am 3 0 diag.gettestlist.service
02/05/2005 15:30:27,776: Falcon: am 4 0 diag.gettestlist.service
02/05/2005 15:30:27,786: Falcon: am 5 0 diag.gettestlist.service
02/05/2005 15:30:27,806: Falcon: am 6 0 diag.gettestlist.service
02/05/2005 15:30:27,816: Falcon: am 7 0 diag.gettestlist.service
02/05/2005 15:30:27,826: Falcon: am 9 0 diag.gettestlist.service
02/05/2005 15:30:27,846: Falcon: am 10 0 diag.gettestlist.service
02/05/2005 15:30:27,856: Falcon: am 11 0 diag.gettestlist.service
02/05/2005 15:30:27,866: Falcon: am 12 0 diag.gettestlist.service
02/05/2005 15:31:27,743: Falcon: am 1 0 diag.gettestlist.service
02/05/2005 15:31:27,753: Falcon: am 2 0 diag.gettestlist.service
02/05/2005 15:31:27,773: Falcon: am 3 0 diag.gettestlist.service
02/05/2005 15:31:27,783: Falcon: am 4 0 diag.gettestlist.service
02/05/2005 15:31:27,793: Falcon: am 5 0 diag.gettestlist.service
02/05/2005 15:31:27,803: Falcon: am 6 0 diag.gettestlist.service
02/05/2005 15:31:27,823: Falcon: am 7 0 diag.gettestlist.service
02/05/2005 15:31:27,833: Falcon: am 9 0 diag.gettestlist.service
02/05/2005 15:31:27,843: Falcon: am 10 0 diag.gettestlist.service
02/05/2005 15:31:27,863: Falcon: am 11 0 diag.gettestlist.service
02/05/2005 15:31:27,873: Falcon: am 12 0 diag.gettestlist.service
```

Falcon requests the cards to send a list of tests to run

```
02/05/2005 15:31:31,328: MCU:
settestlist.Audio+15.7.CM.0.pci.655444.tdm.19660887.qifi.655444.memory.393224
4.END
```

The *Audio+* card responds to the request from the Falcon diagnostic tool. **Slot:** *15.7* **Unit:** *CM0* **Test Name:** *PCI* **Test Flag:** *655444* **Test Name:** *TDM* **Test Flag:** *19660887* **Test Name:** *qifi* **Test Flag:** *655444* **Test Name:** *memory* **Test Flag:** *3932244* *End* of test for this card slot.

```
02/05/2005 15:31:31,338: MCU:
settestlist.Audio+15.12.CM.0.pci.655444.tdm.19660887.qifi.655444.memory.39322
44.END
02/05/2005 15:31:31,338: MCU: startdiag.MuxPlus.4.END
02/05/2005 15:31:31,398: MCU: startdiag.MuxPlus.5.END
```

Falcon requests list of tests to run on the *MUX+* card (slots *4* and *5*).

```
02/05/2005 15:31:31,398: MCU:
settestlist.MuxPlus.4.CM.0.local_memory.23593045.lan.3932213.END
02/05/2005 15:31:31,398: MCU:
settestlist.MuxPlus.5.CM.0.local_memory.23593045.lan.3932213.END
```

Response from *MUX+* cards, slots *4* and *5* indicating the tests to run (l*ocal memory* and *lan* tests).

```
02/05/2005 15:31:31,408: MCU:
settestlist.MuxPlus.4.proc4.4.clock.3932180.local_memory.7864412.neighbor.393
2245.tdm.7864342.full_memory.23593037.END
```

The *MUX+* card responds to the Falcon diagnostic tool. **Unit:** *proc 4.4* **Test Name:** *clock* **Test Flag:** *3932180* **Test Name:** *local memory* **Test Flag:** *7864412* **Test Name:** *neighbor* **Test Flag:** *3932245* **Test Name:** *tdm* **Test Flag:** *7864342* **Test Name:** *full memory* **Test Flag:** *2359037 End* of response.

```
02/05/2005 15:31:32,39: MCU:
settestlist.Audio+15.7.DSP.1.memory.39321692.clock.655444.END
```

The *Audio+* card responds to the request from the Falcon diagnostic tool. **Slot:** *15.7* **Processor:** *DSP* **Test Name:** *memory* **Test Flag:** *39321692* **Test Name:** *clock* **Test Flag:** *19660887* **Test Name:** *qifi* **Test Flag:** *655444 End* of test for this card slot.

```
02/05/2005 15:31:32,169: MCU:
settestlist.MuxPlus.4.proc1.1.clock.3932180.local_memory.7864412.neighbor.393
2245.tdm.7864342.full_memory.39321677.END
02/05/2005 15:31:32,179: MCU:
settestlist.MuxPlus.5.proc1.1.clock.3932180.local_memory.7864412.neighbor.393
2245.tdm.7864342.full_memory.39321677.END
```

The *MUX+* card responds to the request from the Falcon diagnostic tool. **Slot:** *5* **Unit:** *proc 1.1* **Test Name:** *clock* **Test Flag:** *3932180* **Test Name:** *local memory* **Test Flag:** *7864412* **Test Name:** *neighbor* **Test Flag:** *3932245* **Test Name:** *tdm* **Test Flag:** *7864342* **Test Name:** full *memory* **Test Flag:** *39321677 End* of test for this card slot.

```
02/05/2005 15:32:21,441: MCU:
settestlist.IpPlus.2.CM.0.local_memory.19660885.END
02/05/2005 15:32:21,551: MCU:
settestlist.IpPlus.3.CM.0.local_memory.19660885.END
02/05/2005 15:32:21,561: MCU:
settestlist.IpPlus.2.proc1.1.clock.3932180.local_memory.7864412.neighbor.3932
245.lan.3932277.full_memory.39321677.END
02/05/2005 15:32:21,561: MCU:
settestlist.IpPlus.3.proc1.1.clock.3932180.local_memory.7864412.neighbor.3932
245.lan.3932277.full_memory.39321677.END
02/05/2005 15:32:21,561: MCU:
settestlist.IpPlus.9.CM.0.local_memory.19660885.END
02/05/2005 15:32:21,561: MCU:
settestlist.IpPlus.9.proc1.1.clock.3932180.local_memory.7864412.neighbor.3932
245.lan.3932277.full_memory.39321677.END
```

The *IP+* card responds to the request from the Falcon diagnostic tool. **Slot:** *9* **Unit:** *proc 1* **Test Name:** *clock* **Test Flag:** *3932180* **Test Name:** *local memory* **Test Flag:** *7864412* **Test Name:** *neighbor* **Test Flag:** *3932245* **Test Name:** *lan* **Test Flag:** *393277* **Test Name:** *full memory* **Test Flag:** *39321677 End* of test for this car slot.

```
02/05/2005 15:32:27,740: Falcon: am 1 0 diag.gettestlist.service
02/05/2005 15:32:27,810: Falcon: am 6 0 diag.gettestlist.service
02/05/2005 15:32:27,850: Falcon: am 10 0 diag.gettestlist.service
02/05/2005 15:32:27,850: MCU:
```

Additional Falcon requests from the cards to send a list of tests to run

```
settestlist.IpPlus.2.proc2.2.clock.3932180.local_memory.7864412.neighbor.3932
245.tdm.7864342.full_memory.19660877.END
02/05/2005 15:32:27,850: MCU:
```

The *IP+* card responds to the request from the Falcon diagnostic tool. **Slot:** *2* **Unit:** *proc 2* **Test Name:** *clock* **Test Flag:** *3932180* **Test Name:** *local memory* **Test Flag:** *7864412* **Test Name:** *neighbor* **Test Flag:** *3932245* **Test Name:** *tdm* **Test Flag:** *7864342* **Test Name:** *full memory* **Test Flag:** *19660877 End* of test for this card slot.

```
02/05/2005 15:32:27,900: MCU:
settestlist.Video+.1.CM.0.pci.655444.tdm.2621527.bcod.655444.memory.3932244.f
lash.39321676.END
02/05/2005 15:32:28,120: MCU:
settestlist.Video+.1.DSP.1.memory.1310804.clock.1966161.END
02/05/2005 15:32:28,130: MCU:
```

The *Video+* card responds to the request from the Falcon diagnostic tool. **Slot:** *1* **Processor:** *DSP 1* **Test Name:** *memory* **Test Flag:** *1310804* **Test Name:** *clock* **Test Flag:** *1966161 End* of test for this card slot.

```
02/05/2005 15:32:31,355: Falcon: am 4 0 diag.starttestreq.clock.1.39534.0.0
```

Falcon starting *clock* test.

```
02/05/2005 15:32:31,465: MCU: starttestind.39534.END
02/05/2005 15:33:27,807: Falcon: am 6 0 diag.gettestlist.service
02/05/2005 15:33:27,847: Falcon: am 10 0 diag.gettestlist.service
02/05/2005 15:33:27,947: MCU: finishtestind.39534.pass.END
```

Falcon finishing *clock* test.

```
02/05/2005 15:33:28,458: Falcon: am 4 0
diag.starttestreq.local_memory.1.39535.0.0
```

Falcon starting *local memory* test.

```
02/05/2005 15:33:28,648: MCU: starttestind.39535.END
02/05/2005 15:33:44,501: MCU: keepalive.39535.END
02/05/2005 15:33:44,511: MCU: keepalive.39535.END
02/05/2005 15:33:44,511: MCU: keepalive.39535.END
02/05/2005 15:33:44,511: MCU: keepalive.39535.END
02/05/2005 15:34:27,814: Falcon: am 6 0 diag.gettestlist.service
02/05/2005 15:34:27,844: Falcon: am 10 0 diag.gettestlist.service
```

Additional Falcon requests from the cards to send a list of tests to run

```
02/05/2005 15:35:21,792: Falcon: am 12 0 diag.starttestreq.pci.0.39536.1.0
```

Falcon starting *pci* test.

```
02/05/2005 15:35:22,923: MCU: keepalive.39535.END
02/05/2005 15:35:22,923: MCU: keepalive.39535.END
02/05/2005 15:35:22,923: MCU: keepalive.39535.END
02/05/2005 15:35:22,933: MCU: keepalive.39535.END
02/05/2005 15:35:22,933: MCU: keepalive.39535.END
02/05/2005 15:35:22,933: MCU: keepalive.39535.END
02/05/2005 15:35:22,943: MCU: keepalive.39535.END
02/05/2005 15:35:22,943: MCU: keepalive.39535.END
02/05/2005 15:35:22,943: MCU: keepalive.39535.END
02/05/2005 15:35:22,943: MCU: keepalive.39535.END
02/05/2005 15:35:22,953: MCU: keepalive.39535.END
```

```
02/05/2005 15:35:22,953: MCU: finishtestind.39535.pass.END
```

Falcon finishing *local memory* (*39535*) test.

```
02/05/2005 15:35:22,953: MCU: starttestind.39536.END
02/05/2005 15:35:22,963: MCU: finishtestind.39536.pass.END
02/05/2005 15:35:22,963: MCU: starttestind.39536.END
02/05/2005 15:35:22,963: MCU: finishtestind.39536.pass.END
02/05/2005 15:35:22,973: MCU: starttestind.39536.END
02/05/2005 15:35:22,973: MCU: finishtestind.39536.pass.END
```

Falcon running *pci* (*39536*) test.

```
02/05/2005 15:35:23,624: Error: Timeout expired for getting 'Start Test'
indication(MCU: 172.22.175.171 (172.22.175.171), Slot: 4-MUX+40, Unit: 1-
proc1, Test: local_memory)
```

Fault in local memory test on *MUX+* card **Unit:** *proc 1*

```
02/05/2005 15:35:23,624: Falcon: am 4 0 diag.starttestreq.neighbor.1.39537.0.0
```

Falcon starting *neighbor* test.

```
02/05/2005 15:35:27,810: VIDEO+8 Deleted (Failed to receive card test list!)
02/05/2005 15:35:27,851: VIDEO+8 Deleted (Failed to receive card test list!)

02/05/2005 15:35:29,843: MCU: starttestind.39537.END
02/05/2005 15:35:29,853: MCU: finishtestind.39537.pass.END
```

Falcon finishing *neighbor* (*39537*) test.

```
02/05/2005 15:35:29,853: MCU: starttestind.39536.END
02/05/2005 15:35:29,853: MCU: finishtestind.39536.pass.END
02/05/2005 15:35:29,853: MCU: starttestind.39536.END
02/05/2005 15:35:29,863: MCU: finishtestind.39536.pass.END
02/05/2005 15:35:29,863: MCU: starttestind.39536.END
02/05/2005 15:35:29,863: MCU: finishtestind.39536.pass.END
02/05/2005 15:35:29,873: MCU: starttestind.39536.END
02/05/2005 15:35:29,873: MCU: finishtestind.39536.pass.END
```

```
02/05/2005 15:35:29,883: MCU: starttestind.39536.END
02/05/2005 15:35:29,883: MCU: finishtestind.39536.pass.END
02/05/2005 15:35:29,883: MCU: starttestind.39536.END
02/05/2005 15:35:29,893: MCU: finishtestind.39536.pass.END
02/05/2005 15:35:29,893: MCU: starttestind.39536.END
02/05/2005 15:35:31,846: MCU: finishtestind.39536.pass.END
02/05/2005 15:35:31,846: MCU: starttestind.39536.END
02/05/2005 15:35:31,856: MCU: finishtestind.39536.pass.END
02/05/2005 15:35:31,856: MCU: starttestind.39536.END
02/05/2005 15:35:33,849: MCU: finishtestind.39536.pass.END
02/05/2005 15:35:33,859: MCU: starttestind.39536.END
```

Falcon running *pci* (*39536*) test.

```
02/05/2005 15:35:59,6: MCU: starttestind.39536.END
02/05/2005 15:35:59,6: MCU: finishtestind.39536.pass.END
02/05/2005 15:35:59,6: MCU: starttestind.39536.END
02/05/2005 15:35:59,16: MCU: finishtestind.39536.pass.END
02/05/2005 15:35:59,937: MCU: starttestind.39536.END
02/05/2005 15:35:59,947: MCU: finishtestind.39536.pass.END
02/05/2005 15:36:00,878: MCU: starttestind.39536.END
02/05/2005 15:36:01,389: Error: Timeout expired for getting 'Start Test'
indication(MCU: 172.22.175.171 (172.22.175.171), Slot: 4-MUX+40, Unit: 1-
proc1, Test: neighbor)
```

Falcon detected error in *MUX+* card **Unit:** *proc 1*
Test: *antilabor*.

```
02/05/2005 15:36:52,2: MCU: starttestind.39536.END
02/05/2005 15:36:52,12: MCU: finishtestind.39536.pass.END
02/05/2005 15:36:53,14: MCU: starttestind.39536.END
02/05/2005 15:36:53,14: MCU: finishtestind.39536.pass.END
02/05/2005 15:36:54,5: MCU: starttestind.39536.END
02/05/2005 15:36:54,15: MCU: finishtestind.39536.pass.END
02/05/2005 15:36:55,17: MCU: starttestind.39536.END
02/05/2005 15:36:55,17: MCU: finishtestind.39536.pass.END
02/05/2005 15:36:56,18: MCU: starttestind.39536.END
02/05/2005 15:36:56,18: MCU: finishtestind.39536.pass.END
02/05/2005 15:36:57,20: MCU: starttestind.39536.END
02/05/2005 15:36:57,30: MCU: finishtestind.39536.pass.END
02/05/2005 15:36:58,21: MCU: starttestind.39536.END
02/05/2005 15:36:58,31: MCU: finishtestind.39536.pass.END
02/05/2005 15:36:59,23: MCU: starttestind.39536.END
02/05/2005 15:36:59,33: MCU: finishtestind.39536.pass.END
02/05/2005 15:37:00,24: MCU: starttestind.39536.END
02/05/2005 15:37:00,44: MCU: finishtestind.39536.pass.END
02/05/2005 15:37:01,35: MCU: starttestind.39536.END
02/05/2005 15:37:01,45: MCU: finishtestind.39536.pass.END
```

```
02/05/2005 15:37:02,37: MCU: starttestind.39536.END
02/05/2005 15:37:02,37: MCU: finishtestind.39536.pass.END
```

Falcon running *pci* (*39536*) test.

```
02/05/2005 15:37:02,568: Falcon: am 12 0 diag.stoptestreq.0.39536
02/05/2005 15:37:02,738: MCU: stoptestind.39536.END
```

Falcon stopping *pci* test.

```
02/05/2005 15:48:40,648: Falcon: mcpu_reset
```

Falcon resets MCU.

E

Appendix E: IP Network Components

Conferencing with H.323 and SIP endpoints requires the presence of various components in the IP environment. Several components are common to both H.323 and SIP connections and others are unique to H.323 or SIP.

The following table lists the components required for conferencing using IP endpoints, indicating their relevancy to H.323 and SIP:

Table E-1: IP Network List of Components and Logical Entities

Name	H.323	SIP
MCU with IP card(s)	Required	Required
Subnet Mask	Required	Required
DHCP	Optional	Optional
DNS	Optional	Optional
Host Name	Required	Required
Default Router	Required	Required
Static Routes	Optional	Optional
NAT Traversal	Optional	Optional
Gateways	Optional	Optional
Gatekeepers	Optional (recommended)	N/A
H.323 endpoints	Required	N/A
SIP endpoints (User Agents)	N/A	Required

Table E-1: IP Network List of Components and Logical Entities

Name	H.323	SIP
SIP Servers—general	N/A	Optional
Registrar	N/A	Optional (recommended)

MCU with IP card(s)

H.323	SIP
Required	Required

The MCU includes IP+ cards that perform the network functions, such as signaling and capabilities exchange for conferencing. Each IP card has a LAN port that is assigned an IP address, a subnet mask, a default router and static routes. For SIP sessions, this entity is considered to be a special type of User Agent and a mixing component ('media mixer'). For conferences that include SIP participants, IP+ cards from version 4.23 and above are required. For H.323-only conferences, IP (12 or 24) cards are sufficient.

Subnet Mask

H.323	SIP
Required	Required

The IP address of a device in the LAN network is represented by bits with values between 0 - 255, grouped in four components. The Subnet Mask indicates which of the address components in the IP address of a device identify the network and which identify the host on that network. A subnet component value of 255 indicates that the corresponding IP component identifies the network, while any number between 0 to 254 indicates that the corresponding IP component identifies the host on the network. The Subnet Mask of a device allows other devices communicating with that device to identify whether the device is on the same network or on another network and whether a router is required to reach that device.

DHCP

H.323	SIP
Optional	Optional

Short for Dynamic Host Configuration Protocol, a protocol for assigning dynamic IP addresses to devices on a network. DHCP allows an IP device to download configuration information upon initialization. For general IP conferencing, the DHCP is used to answer queries from all the network entities it manages, such as subnet masks, default routers, DNS Servers, SIP servers, gatekeeper, static routes, and the MCU IP cards.

The IP devices must be registered with the DHCP using their host name to enable the DHCP to manage the assignment of IP address to the devices in the organization's network.

Usually, the DHCP server automatically recognizes the MAC address of the IP cards installed in the MCU, and will try to allocate the same IP address each time the IP card registers with the DHCP.

Once the IP card is assigned an IP address by the DHCP, it registers also with the gatekeeper using the alias and the IP address it was assigned by the DHCP. The IP address of the IP card can also be assigned manually, even if a DHCP is being used for IP address management.

In H.323 conferencing, the DHCP provides the gatekeeper IP address.

In SIP conferencing, the DHCP provides the SIP server IP address.

DNS Server

H.323	SIP
Optional	Optional

DNS—Domain Name System—is a method for assigning names to computers on the Internet. These names are pseudonyms for the computers' real IP addresses and provide easy to remember and meaningful names for IP addresses. DNS servers are used to translate domain names or host names into IP addresses. The domain names and IP addresses are distributed throughout the Internet between DNS servers. Queries are directed to a DNS server. The DNS server may be able to provide the IP address itself immediately, or else it will forward the query to a hierarchy of other servers to retrieve the IP address.

The DNS Domain name is defined manually in the DNS server. The same domain name must be entered also in the IP Network Service defined in the MGC Manager.

All the devices register with the DNS automatically or manually. The IP Network Service enables you to define the IP card host name, which allows automatic registration with the DNS server. You can also manually define the IP cards in the DNS server itself. The IP card can then be pinged using the host name.

For H.323 conferencing:

- The gatekeeper registers with the DNS using its host name enabling its auto discovery.
- The server used for detection of the external addresses for NAT Traversal, registers with the DNS using its host name.

In SIP conferencing, the DNS server is used for:

- Registering the SIP servers using their host name.
- RFC2543 Session Initiation Protocol (SIP): Locating SIP servers automatically.
- Participant definition in the MGC Manager using the participant name only, while the DNS server automatically adds the local domain name to form the user SIP address (in the format user name@domain name).

Host Name

H.323	SIP
Required	Required

Each network device is assigned an IP address and a host name. The host name is usually used for registration with the DHCP for dynamic address allocation. The device also registers with the DNS server using the host name and the IP address it was allocated by the DHCP.

Router

H.323	SIP
Required	Required

A router is a device that allows the communication between devices located on different subnetworks. Network devices transmit packets to the default router when the destination IP address is on a different subnetwork and no static route is configured.

Static Routes

H.323	SIP
Optional	Optional

A static route defines the router to be used to access another subnetwork. When a network device transmits packets to another device on a different subnetwork, it checks whether a static route is defined.

NAT Traversal

H.323	SIP
Optional	Optional

NAT Traversal (Network Address Translation) is an application used by firewalls to allow multiple devices located in a local (referred to also as private) network to share a small number of public IP addresses. The devices in the local network use IP addresses that are unique only to the local network. The NAT application maps the local IP addresses with the public IP addresses. The mapping can be either dynamic or static. Static mapping is when a device behind the firewall has a permanent public IP address mapped to its internal (local) IP address. Dynamic mapping is when a public IP address from the available public addresses is mapped to the internal address of a device that needs to communicate across the firewall for the session duration.

With multimedia protocols, including H.323 and SIP, the local IP addresses embedded in the packet payload are not routable in public networks. NAT Traversal enables un-routable private addresses to be replaced with public, routable ones in the packet payload, so that the media packets can find their way through networks (both public and private) to reach the client devices.

Gateways

H.323	SIP
Optional	Optional

A gateway is a device that converts data from the format required for one type of network to the format required for another, such as H.320 and H.323 or SIP. Gateways are optional in an IP (H.323 or SIP) network if the network does not include connections to other network types such as ISDN. A gateway enables point-to-point multimedia calls, involving only two endpoints using different signaling and media protocols, while an MCU enables multipoint conferencing (three endpoints or more). The MGC unit can be configured to include gateway functionality.

Gatekeepers

H.323	SIP
Optional (Recommended)	N/A

To comply with H.323 standard, gatekeepers must perform two main functions:

- Translation of alias addresses of endpoints, MCUs and gateways to IP addresses
- Bandwidth management

H.323 endpoints register with the gatekeeper at startup. When they register they provide the gatekeeper with their IP address and a list of aliases by which they are known to other devices. The gatekeeper maintains a database of devices in the network that are active at any time.

When one endpoint calls another endpoint using only its alias, the gatekeeper is queried for the IP address of the destination endpoint. In addition, the destination endpoint requests the permission to use the required bandwidth. When the call ends, both endpoints send a notification to the gatekeeper, which in turn releases the bandwidth to other uses.

To perform these two main functions, the gatekeeper collects and maintains information about the conferencing activity on the network. This information is also used for other gatekeeper functions, such as, routing, monitoring, billing, and more.

The gatekeeper can be incorporated in the MCU, or it can be an external, separate device. The MGC unit works with an external gatekeeper. Each zone on the LAN includes only one gatekeeper.

H.323 Endpoints

H.323	SIP
Required	N/A

H.323 endpoints must support voice communications. Video and data are optional. H.323 endpoints must also support:

- RAS (Registration Admission Status), which is a signaling protocol used to communicate between endpoints and the gatekeeper
- Q.931 for call signaling and call setup
- H.245 for session control to negotiate media capabilities and logical channel usage
- RTP/RTCP for delivery and control of audio and video streams

SIP Endpoints (User Agents)

H.323	SIP
N/A	Required

SIP enabled end-devices, are usually application programs that send SIP requests, such as a PC with headset attachment or SIP phone. User Agents (UA) must be capable of establishing and terminating a media session with another User Agent. UAs should be capable of supporting both UDP and TCP

although it is not required; support of SDP (Session Description Protocol) for media description is. A SIP User Agent contains both a client application (User Agent client, UAC) and a server application (User Agent server, UAS). UACs originate requests and UASs originate responses to requests.

SIP Server

H.323	SIP
N/A	Optional (Recommended)

A SIP server is a server that provides routing functionality; it is an intermediary that receives SIP messages and forwards them. Most SIP servers support both TCP and UDP since they provide services to User Agents that can use either type of protocol. The SIP server includes a registrar with a proxy server or a registrar with a redirect server. Currently, the MGC MCU supports only a registrar with a proxy server. These logical entities are usually located on the same server.

SIP servers fulfills three main functions:

- Proxy services—Deliver packets to their correct destinations. Each network has a proxy(ies) that is an administration entity for the incoming/outgoing traffic.
- Registration—List the aliases of SIP entities with their associated IP addresses.
- Presence—Some proxies provide presence tracking of registered aliases/ participants. Similar to 'Buddy lists' from instant messaging applications, this feature allows checking of whether the invited aliases are online and available, or not.

SIP Proxy

H.323	SIP
N/A	Optional (Recommended)

The SIP proxy server is a logical entity that is part of the SIP server. The SIP proxy facilitates endpoints locating and contacting each other, but it can drop out of the signaling path as soon as it no longer adds any value to the exchange. It transfers only signaling messages while the media messages are

transferred directly between the User Agents. SIP User Agents in most cases use URIs (Uniform Resource Identifiers) to contact each other. The SIP proxy, retrieves the current location of the invited endpoint. It then proceeds to insert the location in the Invite and forward the Invite to its final destination.

The SIP proxy can also function as an Outbound proxy. All messages from the MCU and Registrar are sent to the Outbound proxy, which forwards them to their destination according to the address included in the message header.

It should be noted that proxy servers do not initiate sessions, but forward the Invites from parties that are allowed to do so.

Registrar (Registration Server)

H.323	SIP
N/A	Optional (Recommended)

A registrar is logical entity that is part of the SIP server. User agents (UAs) upon initialization and at periodic intervals send Register messages to the registrar. The registrar accepts these Register messages and associates the UA's URI, e.g. sip:dan@polycom.com, with the device this UA is currently logged on. The registrar writes this association, also called 'binding', to a database (Location Server), which is accessed by other SIP servers in the same administrative domain to locate registered UAs. One URI can be assigned to several IP addresses, so if a user is away, another device can be used for connection.

The registration server is typically co-located with either a proxy or redirect server.

Redirect Server

H.323	SIP
N/A	Optional

A redirect server is logical entity that is part of the SIP server. A redirect server is a SIP server that responds by providing the current address of the requested endpoint which is retrieved from the location service database. Unlike the proxy which actually inserts the final destination's address in the

To: header field and forwards it, the redirect server only answers with the information—it does not forward the request to the correct address. The initiating party then uses the information provided by the redirect server to reissue its Invite directly to the correct address.

Location Server

H.323	SIP
N/A	Optional (recommended)

A location server is a server installed with an abstract service known as a location service, which provides the address bindings for a particular domain of User Agents to the devices they are logged on to. The information stored and retrieved from the location service to/from the proxy or registrar is transferred via a non-SIP protocol.