



Polycom RMX 2000 Release Notes Beta Version **2.0**

August 2007

DOC2180A



Copyright © 2007 Polycom, Inc.
All Rights Reserved

All text and figures included in this publication are the exclusive property of Polycom, Inc. and may not be copied, reproduced or used in any way without the express written permission of Polycom, Inc. Information in this document is subject to change without notice. This document also contains registered trademarks and service marks that are owned by their respective companies or organizations.

If you have any comments or suggestions regarding this document, please send them via e-mail to info@polycom.com.

Catalog No. DOC2180A
Beta Version 2.0

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 assure the accuracy of such information. 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 US7,054,820.

PATENT PENDING

Table of Contents

Version 2.0 - New Features List	1
Version 2.0 Upgrade Package Contents	4
ISDN/PSTN Upgrades Only	4
Version 2.0 Interoperability Table	5
Upgrade Procedure	7
For an IP Only Upgrade	7
For an ISDN/PSTN Upgrade	7
Installing the MCU Software	8
Detailed Description - Video	10
HD CP	10
Enabling HD CP	10
Video Display	10
Connection Speed	10
Resolution in Video Layouts	10
Video Features Supported in HD CP	10
System Resources	11
System Flag	12
Previous HD Support (Version 1.1)	12
Fade In / Fade Out	13
Detailed Description	13
Site Name Transparency	14
Video User Indication (VUI)	15
Detailed Description - Hardware	16
New RTM ISDN Card	16
RTM ISDN LEDs	16
ISDN/PSTN Clock Source	17
Installing an RTM ISDN Card and Connecting the PRI Cables	17
RTM ISDN Hardware Monitor	19
RTM ISDN Diagnostics Additions	21
Detailed Description - ISDN/PSTN	22
ISDN/PSTN Network Service Definition	22
Configuring the ISDN/PSTN Network Service	22
Configuring the ISDN/PSTN Service Using the Fast Configuration Wizard	22
Configuring the ISDN/PSTN Network Service from the Network Service List	29
Conferencing via PSTN Connections	30
Allocating Dial-In Numbers to Entry Queues for ISDN/PSTN Connections	30
Connecting to Conferences via ISDN/PSTN	31
Undefined Dial-in Participants	31
Defined Dial-out Participants	31
Encryption	31
Monitoring ISDN/PSTN Participants	32
Defining PSTN Participants	35
Detailed Description - General	37
Video/Voice Port Configuration	37
Port Usage Gauges	39

Resource Report Update	40
Overview	40
Detailed Description	40
Unicode Support	41
Display of Unicode Endpoint Names in Conference Layouts	41
Display of Unicode Text in RMX Web Client Fields	41
Display Name	42
Text Field Length	42
Routing Name	43
Multiple Web Clients on the Same RMX	43
Multilingual Web Client	44
Supported Languages	44
Translated Elements	44
Login Screen	45
Multilingual Setting	46
SNMP (Simple Network Management Protocol)	47
Detailed Description	47
MIB (Management Information Base) Files	47
Private MIBS	47
Support for MIB-II Sections	47
The Alarm-MIB	47
H.341-MIB (H.341 - H.323)	47
Standard MIBs	48
Traps	49
Status Trap Content	50
Defining the SNMP Parameters in the RMX	51
CDR Event	55
Detailed Description - IP.....	56
Configuring the Default Management Network	56
SIP Transport Layer Security (TLS)	58
SIP Digest	59
Detailed Description - Partners	60
IBM/RMX V2.0 Integration	60
Enabling IBM Integration in the RMX	60
IVR Service	60
System Configuration Flag	61
Polycom - AVAYA Collaboration (Apollo)	62
Enabling Avaya Video Features	62
ACM as Gatekeeper	62
Detailed Description - System Tools.....	64
Modem Support	64
Procedure 1: Download and Install the Local Web Client	64
Procedure 2: Configure the Modem	64
Procedure 3: Create a Dial-up Connection	65
Procedure 4: Connect to the RMX	68
Corrections and Known Limitations	69
Version 2.0 Corrections	69
Version 2.0 System Limitations	70

Version 2.0 - New Features List

The following table lists the new features in Version 2.0.

Table 1 *New Features List*

	Category	Feature Name	Description
1.	Video	HD CP	Version 2.0 supports endpoints at HD resolution in CP (Continuous Presence) mode in addition to HD in <i>Video Switching</i> mode.
2.	Video	Fade in / Fade out	In Version 2.0, when there is a change of speaker in a Continuous Presence conference, the transition is set by default to fade in the current speaker while fading out the previous speaker.
3.	Video	Transparent Site Names	In Version 2.0, endpoint names in video layouts appear against a transparent background.
4.	Video	VUI	Version 2.0 supports the VUI addition to the H.264 protocol for endpoints that transmit wide video (16:9) in standard 4SIF resolution.
5.	Hardware	New RTM ISDN card	In version 2.0, up to two RTM ISDN cards can be installed in the RMX. Each card allows the connection of up to 12 E1/T1 PRI lines to the RMX, supporting PSTN voice participant connections.
6.	ISDN/PSTN	Hardware Monitor	In version 2.0, the Shelf Management site which is responsible for the monitoring and diagnostics of the hardware components has been appended to include the status and properties of the RTM ISDN card.
7.	Hardware	RTM ISDN Diagnostics Additions	Version 2.0 includes diagnostics that can be utilized to perform tests on the RTM ISDN card in order to detect malfunctions.
8.	ISDN/PSTN	ISDN/PSTN Network Service Definition	To enable PSTN participants to connect to the MCU, an ISDN/PSTN Network Service must be defined.
9.	ISDN/PSTN	Conferencing (Connecting to Entry Queues)	The connection of PSTN participants to conferences is enabled only via Entry Queues to which an ISDN/PSTN dial-in number is assigned. Dial-out participants can be defined in the <i>Address Book</i> or directly in the ongoing conference.

Table 1 New Features List (Continued)

	Category	Feature Name	Description
10.	General	Voice/Video Port Configuration	In version 2.0, video ports can be converted to voice ports to enable maximized usage of the system's resources.
11.	General	Port Gauges	In version 2.0, an additional <i>Port Gauge</i> displays the <i>Port Usage</i> of voice ports configured in the system. The additional gauge is displayed only if voice ports are configured in the system.
12.	General	Resource Report Update	In version 2.0, the Resource Report has been adapted to display video and audio port usage according to their allocation in the video/voice port configuration.
13.	General	Unicode	Unicode (an international standard that enables the display of complex scripts such as Japanese, Chinese, etc.) is now supported with the RMX. It enables complex scripts to display endpoint names in the <i>video layouts</i> and the names of conferences, Meeting Rooms, Entry Queues and services in the <i>RMX Web Client</i> .
14.	General	Multilingual GUI	In Version 2.0, the <i>RMX Web Client</i> user interface is translated and supports 11 additional languages.
15.	General	SNMP	SNMP standard protocol is now supported with the RMX. It enables managing and monitoring of the MCU status by external managing systems, such as HP OpenView or through web applications.
16.	General	CDR Event Added	A new CDR event has been added to the CDR in order to store the <i>Display Name</i> to support the Unicode naming for endpoints (participants), conferences, Meeting Rooms, Entry Queues and services.
17.	General	Address Book Increased Capacity	<i>Address Book</i> capacity has been increased from 200 to 1000 entries.
18.	General	Meeting Rooms Increased Number	The number of <i>Meeting Rooms</i> has been increased from 200 to 1000.
19.	IP	Network Service Configuration	In Version 2.0, the direct connection method to define the <i>Default Management Network Service</i> has been modified to include a wizard.
20.	IP	SIP TLS Security	Version 2.0 supports the <i>TLS</i> cryptographic protocol, used to ensure secure communications between the SIP server and the MCU over the Internet.

Table 1 *New Features List (Continued)*

	Category	Feature Name	Description
21.	IP	SIP Digest Security	Version 2.0 supports <i>SIP Digest</i> authentication, allowing two SIP entities to authenticate credentials with each other.
22.	Partners	IBM	Version 2.0 supports the IBM/Polycom integration. It enhances IBM offering with Polycom's high quality audio and video capabilities for both Point-2-Point and Multipoint conferencing scenarios.
23.	Partners	Avaya	The RMX can function as a component of the <i>Apollo</i> R2 and R3.01 environments.
24.	System Tools	Modem Support	Remote access to the RMX's <i>Alternate Management Network</i> is supported via an external PSTN <=> IP modem.

Version 2.0 Upgrade Package Contents

Version 2.0 upgrade package includes the following items:

USB key with the following items:

- lan.cfg file
- LanConfigUtility.exe
- RMX Documentation
 - RMX 2000 Version 2.0 Release Notes
 - RMX 2000 Getting Started Guide
 - RMX 2000 Administrator's Guide
 - RMX 2000 Hardware Guide
 - RMX 2000 Quick Installation Booklet
- External DB Tools Version 2.0
 - Documentation
 - Sample Scripts
- RMX XML API Kit Version 2.0
 - RMX 2000 XML API Conferencing Overview
 - MGC to RMX XML API Conferencing Comparison
 - XML Schemas

ISDN/PSTN Upgrades Only

For clients that purchased the RTM ISDN card that enables an ISDN/PSTN Network Service, the version 2.0 Upgrade Package Contents include:

- RTM ISDN Card
 - For more information about installation, see *"Installing an RTM ISDN Card and Connecting the PRI Cables"* on page [1-17](#).

Version 2.0 Interoperability Table

The following table lists the devices with which Version 2.0 was tested.

Table 2 Version 2.0 Interoperability List

Device	Version
Gatekeepers/Proxies	
Polycom PathNavigator	7.0.0.03
Cisco gatekeeper	12.3
Radvision ECS gatekeeper	3.5.2.5
Microsoft LCS SIP proxy	2005 ver. 2.0.5470.0
Iptel proxy	0.9.6
ReadiManager SE200	2.00.00.ER029
Recorder	
Polycom RSS 2000	1.01.002
MCUs and Call Managers	
Cisco Call Manager	4.1
Tandberg MCU	D3.9
Tandberg MPS	J3.3
Endpoints	
Polycom PVX	8.0.2.0235
Polycom VS 512	7.5.4
Polycom VSSP 128	7.5.4
Polycom VSSP 384	7.5.4
Polycom VS EX	6.0.5
Polycom VS FX	6.0.5
Polycom VS 4000	6.0.5
Polycom VS FX	6.0.5.21
Polycom V500	8.5.3
Polycom VSX 3000	8.5.3
Polycom VSX 7000	8.5.3
Polycom VSX 8000	8.5.3
Polycom iPower 9000	6.2.0.1208
Aethra VegaStar Gold	6.0.49
Sony PCS1	3.31

Table 2 Version 2.0 Interoperability List (Continued)

Device	Version
TA MXP	F6.0
TA B	10.3
TA E	5.3
LifeSize	LS_RMI_2.5.1(1)
MS OC	1.0.559
Microsoft Windows MSN Messenger	5.1
HDX 9001	301-1.02
HDX 9002	301-1.02
HDX 9004	301-1.02
HDX PAL	1.0.2-354
HDX NTSC	1.0.2-354
HDX NTSC	2.0-2032

Upgrade Procedure

For an IP Only Upgrade

- A** Backup the configuration file. For more information, see the *RMX Administrator's Guide, "Software Management"* on page **11-33**.
- B** To facilitate Version 2.0 installation it is required that you first install Version 1.1.0.2xx of the software.
- C** Install the MCU Software. For more information, see "*Installing the MCU Software*" on page **1-8**.
- D** Setup the voice/video port configuration. For more information, see "*To configure Video/Voice Ports from the Setup Menu:*" on page **1-38**.
- E** Reset the MCU.



After resetting the MCU the *Active Alarms* list indicates that the MCU is in the process of updating the Software. No conferences can be initiated until the process is completed and the *Active Alarm* is removed from the list.

For an ISDN/PSTN Upgrade

- A** Backup the configuration file. For more information, see *RMX Administrator's Guide, "Software Management"* on page **11-33**.
- B** To facilitate Version 2.0 installation it is required that you first install Version 1.1.0.2xx of the software.
- C** Install the MCU Software. For more information, see "*Installing the MCU Software*" on page **1-8**.
- D** Shut down the MCU.
- E** Complete the Hardware upgrade procedures (Insert the New RTM ISDN Card). For more information, see "*Installing an RTM ISDN Card and Connecting the PRI Cables*" on page **1-17**.
- F** Turn on the MCU.
- G** Complete the Fast Configuration Wizard. For more information, see "*Configuring the ISDN/PSTN Service Using the Fast Configuration Wizard*" on page **1-22**.
- H** Complete the Voice/Video Port Configuration. For more information, see Step 15-17 "*Video/Voice Port dialog box*" on page **1-27**.
- I** Reset the MCU.



After resetting the MCU the *Active Alarms* list indicates that the MCU is in the process of updating the Software. No conferences can be initiated until the process is completed and the *Active Alarm* is removed from the list.

Installing the MCU Software



Prior to upgrading to Version 2.0 it is recommended to back up your system configuration.

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

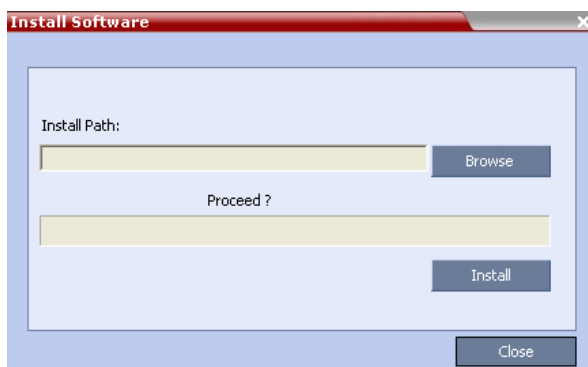
Table 1-1 Software Pre-download Checks


Pre-download Test	Error Message	Solution
Verifying the software version suits the RMX 2000	“Software is not supported on this MCU type.”	Download the appropriate version of the software from the CD, FTP or Polycom Resource Center.
Verifying 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 is required.”	Contact Polycom support team. You can manually verify the amount of disk space.

To install a software update on the RMX:

- 1 In the RMX menu bar, click **Administration > Software Management > Software download**.

The *Install Software* dialog box is displayed.



- 2 Click the **Browse** button. The *Open* dialog box appears. Navigate to the directory where the updated MCU's software version file is contained.
- 3 Select the software version file and click **Open**.
The software version's directory path is displayed in the *Install Path:* field.
- 4 Click **Install** to start the installation procedure.
After installation is complete, a caption box will appear instructing you to Reset the MCU.
- 5 Click **OK**.
- 6 In the *RMX Management* pane, click **Hardware Monitor**.
- 7 In the *Hardware Monitor* pane toolbar, click the **Reset**  button.

The MCU will begin resetting.



After resetting the MCU, the *RMX Web Client's* **System Alerts** tab will blink red indicating an Active Alarm. The MCU is presently updating the system software and will continue to indicate an Active Alarm until it is finished. No conferences may be created during the system software update.

Detailed Description - Video

HD CP

Version 2.0 supports endpoints at HD resolution in CP (Continuous Presence) mode in addition to HD in *Video Switching* mode.

HD compliant endpoints can connect to conferences at resolutions of up to 1280X720 at bit rates ranging from 384 Kbps to 4 Mbps.

Enabling HD CP

HD resolution is enabled by the MAX_CP_RESOLUTION flag in the system configuration. Once enabled, the MCU attempts to connect all participants at HD resolution in CP mode, unless the conference *profile* is set differently (HD Video Switching).

Video Display

Connection Speed

The RMX always attempts to connect to HD endpoints at the highest line rate (4 Mbps). If the connection cannot be established, the RMX attempts to connect at the next highest line rate at its highest supported resolution.

- If the endpoint cannot transmit and receive at 4Mbps:
 - the RMX attempts an *asymmetrical connection*, transmitting at 4 Mbps and receiving at 2 Mbps (the endpoint transmits SD and receives HD)
- If the endpoint cannot receive at 4 Mbps and the *asymmetrical connection* cannot be established:
 - the RMX transmits and receives at 2 Mbps

Resolution in Video Layouts

Video resolution differs according to conference and personal layout:

- In 1X1 *video layout* the MCU transmits speaker resolution (including input from HD participants) at up to SD resolution. If 1x1 is the requested layout for the entire duration of the conference, set the conference to HD *Video Switching* mode.
- In asymmetrical layouts, where participants' *video windows* are different sizes, the RMX transmits HD and receives SD or lower resolutions.
- In panoramic layouts the RMX transmits HD and receives SD or lower resolutions, the RMX scales images from SD to HD resolution.

Video Features Supported in HD CP

The following features are supported in HD CP:

- **H.239** - When an endpoint starts a Content session, the video bit rate is decreased according to the Content allocation settings, and this may result in a lower frame rate. For more information, see *RMX 2000 Administrator's Guide*, "H.239" on page [6-12](#).
- **Encryption**
- **FECC**

- **Lecture Mode**
- **Cascading** – Simple cascade links are treated as endpoints and are allocated resources according to *Table 2* on page **1-11**. Cascaded links in 1x1 *video layout* are in SD resolution.
For more information, see *RMX 2000 Administrator's Guide, "Cascading Conferences"* on page **6-24**.

System Resources

The RMX allocates HD resources to endpoints according to the following criteria:

- System resources (ports) are allocated according to endpoint capability and are optimized by allocating HD resources only to endpoints capable of receiving HD resolution.
- Endpoints with between CIF and SD30 are rounded up to SD30 while capabilities between SD30 and HD are rounded up to HD.
- Resolutions between SD and HD are not supported. The endpoint is forced to either HD or SD.
- Resources required for various video resolutions are also defined by the *Quality* settings:
 - **Motion**, when selected, results in higher frame rate.
 - **Sharpness**, when selected, sends higher video resolution and requires more system resources.

The combination of **frame rate** and **resolution** affects the number of ports required on the MCU to support the call.

The relationship between *Video Quality* (frame rate, resolution) and *port usage* when the **MAX_CP_RESOLUTION** flag is set to HD is summarized in the table below:

Table 2 Video Quality vs Port Usage – **MAX_CP_RESOLUTION = HD**

Endpoint Bit Rate Kbps	Video Quality			
	Motion		Sharpness	
	Resolution	Ports Required	Resolution	Ports Required
128	CIF	1	CIF	1
256	CIF	1	SD15	2
384	2CIF30	2	SD15	2
512	2CIF30	2	SD30	4
768	SD30	4	SD30	4
1024	SD30	4	HD	4
1472	SD30	4	HD	4
1920 +	HD	4	HD	4

System Flag

The **MAX_CP_RESOLUTION** flag can be set to one of the following levels to determine the maximum video resolution transmission for CP conferences:

- **CIF** – CIF resolution at 30 frames per second
- **2CIF/SD15** – SD resolution at 15 frames per second
- **SD30** – SD resolution at 30 frames per second
- **HD** – HD resolution at 30 frames per second

The default setting for the **MAX_CP_RESOLUTION** flag is **SD30**.

The flag's value can be modified via the *Setup* menu *System Configuration*.

For more information, see *RMX 2000 Administrator's Guide*, "System Configuration" on page **11-5**.

Previous HD Support (Version 1.1)

High Definition *Video Switching* should be selected when you want the system to:

- Run in Full Screen 1x1 *Video Layout*
- Save system resources – in HD *Video Switching* mode the MCU uses only 1 CIF port for each video connection

In this mode, all participants connecting to the conference must use the same line rate and support HD, otherwise they are connected as secondary (audio only).

High Definition *Video Switching* must be selected in the conference a Profile and assigned only to conferences and Entry Queues that you want to force to this mode.

Fade In / Fade Out

In Version 2.0, when there is a change of speaker in a Continuous Presence conference, the transition is set by default to fade in the current speaker while fading out the previous speaker.

Detailed Description

To make this transition visually pleasant, fading in the current speaker while fading out the previous speaker is done over a period of 500 milliseconds.

Fade In / Fade Out is restricted to participants with video bit rates of 768 Kbps and above. If the video bit rate changes to less than 768 Kbps: for example, if the participant starts a Content sharing session (H.239), *Fade In / Fade Out* is disabled.

The *Fade In / Fade Out* effect does not occur when changing *Video Layouts*. The reason is that the speakers' resolution may also change during a *Video Layout* change and a fade effect between two images with different resolutions is not possible.

The *Fade In / Fade Out* feature can be disabled by adding a new flag to the *System Configuration*. The *Value* of the new flag must be: FADE_IN_FADE_OUT=NO.

For more information about *System Flags*, see the *RMX 2000 Administrator's Guide*, "*System Configuration*" on page [11-5](#).

Site Name Transparency

In Version 2.0, endpoint names in video layouts appear against a transparent background.

Endpoint name backgrounds are 50% transparent, and while maintaining contrast, do not completely obscure the overlaid video.

The Endpoint Name Transparency feature can be disabled by adding a new flag to the *System Configuration*. The *Value* of the new flag must be:
SITE_NAME_TRANSPARENCY=NO.

Video User Indication (VUI)

Version 2.0 supports the VUI addition to the H.264 protocol for endpoints that transmit wide video (16:9) in standard 4SIF resolution.

If the MCU is not VUI enabled, the video from these endpoints may contain black stripes above and below the picture. These stripes are both unsightly and a waste of usable video resolution.

Version 2.0 supports VUI in Continuous Presence conferences for H.323 participants in all current Video Layouts. The MCU always sends video capabilities with the VUI extension and all sample aspect ratios are supported according to the H.241 8.3.2.11 standard.

Detailed Description - Hardware

New RTM ISDN Card

The RTM ISDN card connects directly to an MPM card. The RTM ISDN card routes data between the MPM cards and components of the system, converts ISDN T1/E1 media to IP packets and provides connectivity to external ISDN networks. Up to two RTM ISDN cards can be installed in one RMX 2000.

Each RTM ISDN card includes the following connections:

- 12 E1/T1 PRI lines
- 1 LAN port

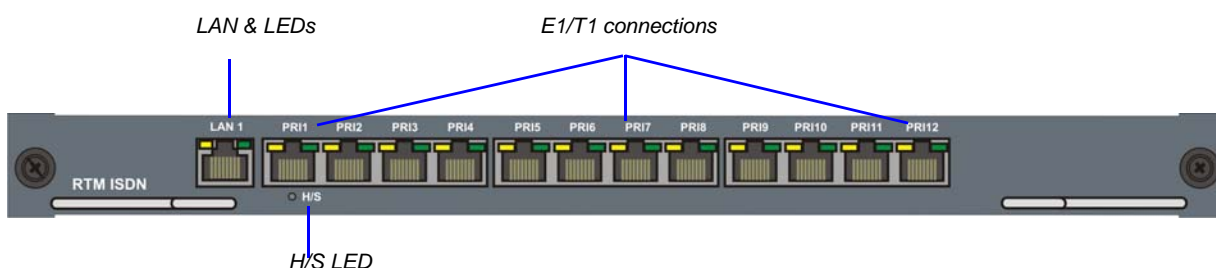


Figure 1-1 RMX 2000 RTM ISDN Rear Panel Layout



The RTM-ISDN card supports 200 participants, regardless of whether the spans are T1 or E1.

RTM ISDN LEDs

The following items appear on the RTM ISDN board:

Table 3 RMX 2000 RTM ISDN LEDs

Component	LED Name	LED Color	Description
LAN LED (1)	LNK	Green	Lit with active network connection, flickers with Packet activity.
	1 Gb	Amber	Lit when 1Gb connection online, flickers with Packet activity

Table 3 RMX 2000 RTM ISDN LEDs (Continued)

Component	LED Name	LED Color	Description
ShMG LEDs	H/S	Blue	OFF - Normal.
			Flashing - This LED is activated when the MPM card initiates a power off routine on itself and its dependent RTM ISDN board.
			ON - Power to the RTM ISDN board has been switched OFF. This LED is activated when the MPM powers itself off, and its dependent RTM ISDN board.

ISDN/PSTN Clock Source

Each RTM ISDN card has its own primary and secondary clock source. The first span to synchronize becomes the primary clock source and the second span to synchronize becomes the secondary clock source. This clock is used to synchronize ISDN spans only (it is not the system clock).

A single clock source triggers an alarm that can be turned off by setting the appropriate flag in the system configuration.

Installing an RTM ISDN Card and Connecting the PRI Cables

The RTM ISDN card installed in the rear panel of the RMX interfaces between the RMX unit and the ISDN/PSTN switch.

An RTM ISDN card must connect directly to an MPM board:

- In an RMX with a single MPM board – the RTM ISDN card must be installed in the rear panel slot on the same level as the MPM board
- In an RMX with two MPM boards – the RTM ISDN card can be installed in either of the two rear panel card slots

To install an RTM ISDN card:

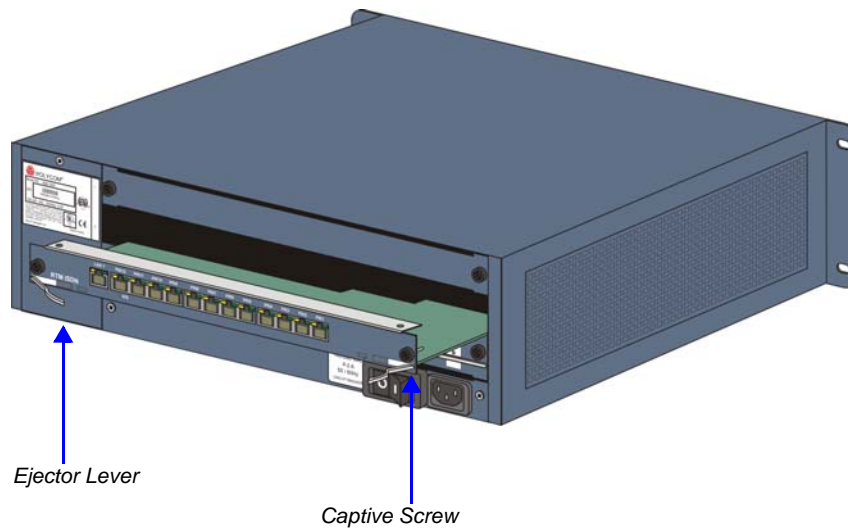


When handling electronic components, standard anti-static precautions must be observed:

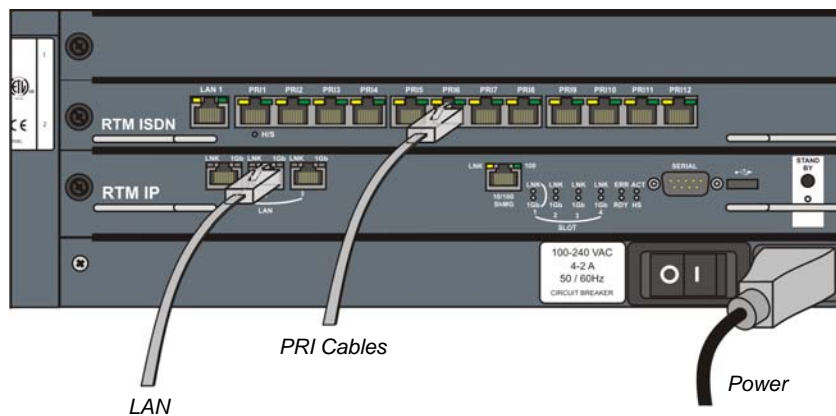
- Wear a grounding strap
- Handle cards by their edges only and do not touch their components or connector pins
- Keep components in anti-static bags, when not installed in the RMX

- 1** Power the RMX off.
- 2** Loosen the captive screws and remove the slot cover.
- 3** On the card to be installed, move the ejector levers to their fully open position.

- 4 Insert the card into the slot until the ejector levers touch the front edge of the card cage.



- 5 Push the ejector levers to their fully closed position.
- 6 Tighten the captive screws on each side of the rear panel of the card, securing the RTM ISDN card to RMX.
- 7 Connect the RJ-45 terminated PRI cables into any of the slots labeled PRI1 - PRI12:



Up to 12 PRI cables can be connected to an RTM ISDN card. When two RTM ISDN cards are installed, up to a total of 24 PRI cables can be connected.

- 8 Power the RMX on.

RTM ISDN Hardware Monitor

In version 2.0, the Shelf Management site which is responsible for the monitoring and diagnostics of the hardware components has been appended to include the status and properties of the RTM ISDN card.

The Hardware Monitor pane displays the status, voltage and temperature indications for the RTM ISDN card. When the card's status indicates a "Major" error, administrators are able to reset or shut down the MCU. Alternatively, administrators may also access the Shelf Management site to run diagnostics on the faulty card.

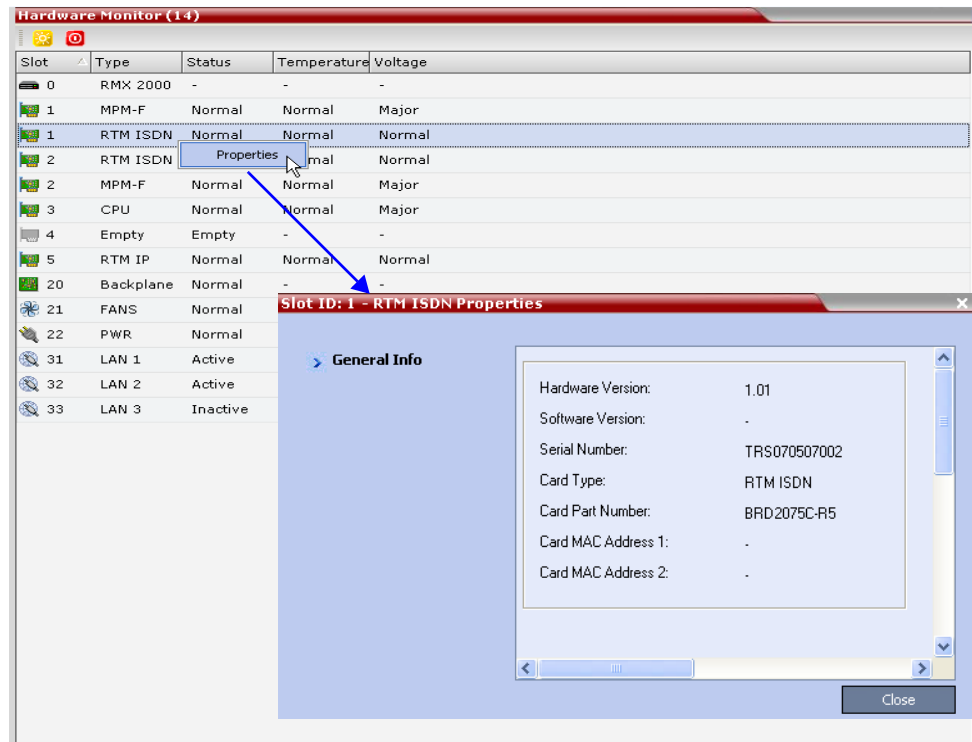
To view the RTM ISDN card's status and properties:

- 1 In the *RMX Management* pane, click **Hardware Monitor**.

The *Hardware Monitor* list is displayed, showing the current card's status, voltage and temperature.

- 2 Right-click the *RTM ISDN* card and select **Properties**.

The *RTM ISDN Properties - General Info* dialog box is displayed.



The following properties are displayed:

Table 4 RTM ISDN Properties - General Info

Field	Description
<i>Hardware Version</i>	The RTM ISDN's card version number.
<i>Software Version</i>	The version number of the installed software.
<i>Serial Number</i>	The RTM ISDN's card serial number.
<i>Card Type</i>	Displays the type of card that occupies the slot.
<i>Card Part Number</i>	The part number of the RTM ISDN's board.

Table 4 RTM ISDN Properties - General Info

Field	Description
<i>Card MAC Address 1</i>	Specific hardware address of the component. It enables the system to automatically identify it.
<i>Card MAC Address 2</i>	(If applicable) Second Mac address.

Alarms

ISDN alarms are part of the active alarms mechanism. The following alarms are issued:

- Red Alarm - a configured span is not recognized by the RTM ISDN card
- Yellow alarm - a configured span is not identified by the ISDN PBX
- Single clock source - when only one span is connected to the RTM ISDN and is used for ISDN clock synchronization. This alarm can be disabled by setting the appropriate system flag.

RTM ISDN Diagnostics Additions


Version 2.0 includes diagnostics that can be utilized to perform tests on the RTM ISDN card in order to detect malfunctions. Six tests have been added to the HW Diagnostics to test the RTM ISDN card as follows:

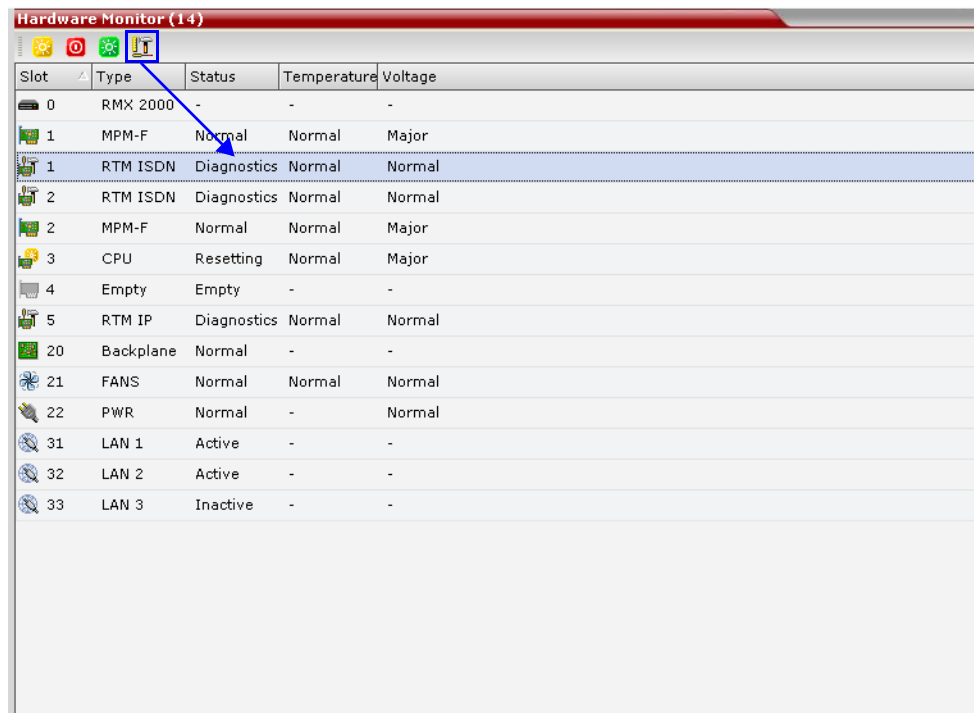
- *RTM_ISDN_DSP_SHORT_MEMORY* - tests samples of the external memory of the PSTN DSP.
- *RTM_ISDN_DSP_LONG_MEMORY* - tests all external memory of the PSTN DSPs.
- *RTM_ISDN_DSP_CLOCK* - tests the DSP clock.
- *RTM_ISDN_TDM_TEST* - tests by internal loop the TDM.
- *RTM_ISDN_LOOP_T1_TEST* - checks establishing D channel in T1.
- *RTM_ISDN_LOOP_E1_TEST* - checks establishing D channel in E1.

When results are displayed in the *Diagnostics* pane, users have a clearer understanding of which component is malfunctioning. The results will then need to be forwarded to Polycom’s technical support for further analysis and problem resolution.

Access to the Diagnostic Mode is described in the *RMX Administrator’s Guide*, “*Diagnostic Mode*” on page 12-11.

To run the diagnostics on the RTM ISDN card:

- 1 In the *Hardware Monitor* toolbar, click the **Diagnostic Mode** () button. The RTM IP, RTM ISDN and CPU components indicate a status of “Diagnostics”; the MPM cards indicate “Resetting”. After resetting, the MPM cards will also indicate “Diagnostics” status.



- 2 Right-click the RTM ISDN card and then click **Diagnostics**.
- 3 Select the test to run and the testing mode as described in the *RMX Administrator’s Guide*, “*Diagnostic Mode*” on page 12-11.

Detailed Description - ISDN/PSTN

ISDN/PSTN Network Service Definition

Installing an RTM ISDN card in the RMX enables the connection of PSTN voice participants to conferences via E1/T1 PRI lines connected to the RMX.

To enable PSTN participants to connect to the MCU, an ISDN/PSTN Network Service must be defined.

Configuring the ISDN/PSTN Network Service

There are two methods of defining the ISDN/PSTN Network Service:

- During first entry configuration, using the *Fast Configuration Wizard*
- Adding a new ISDN/PSTN Network Service to the *ISDN/PSTN Network Services* list.

The Network Service is used to define the properties of the ISDN/PSTN switch and the ISDN lines running from the ISDN switch to the ISDN card installed in the RMX.

Before configuring the ISDN/PSTN Network Service, obtain the following information from your ISDN/PSTN Service Provider:

- Switch Type
- Line Coding and Framing
- Numbering Plan
- Numbering Type
- Dial-in number range



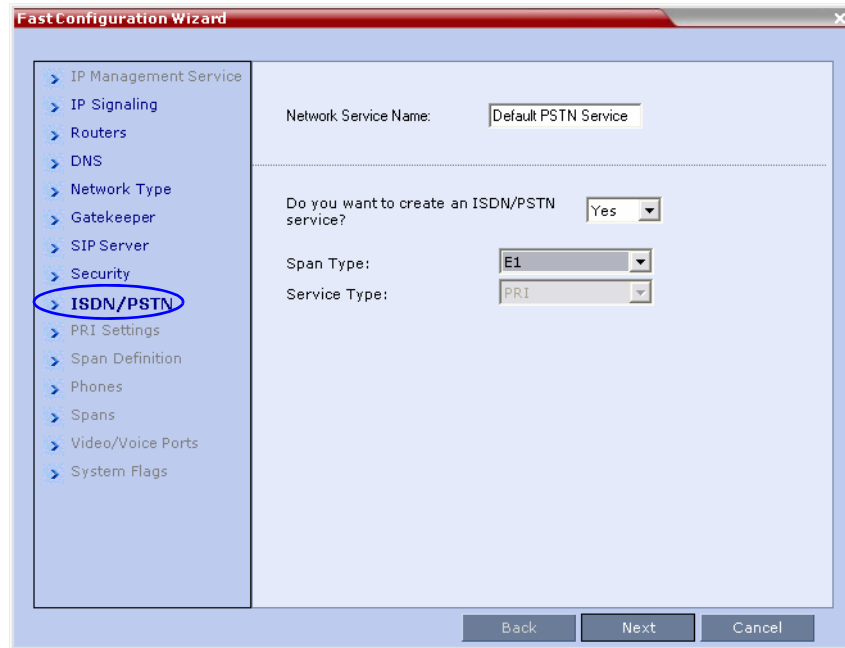
If the RMX is connected to the public ISDN Network, an external CSU or similar equipment is needed.

Configuring the ISDN/PSTN Service Using the Fast Configuration Wizard

During the initial RMX setup, if the system detects the presence of the RTM ISDN card, the ISDN /PSTN Network Service definition screens of the *Fast Configuration Wizard* are enabled.

To Configure the ISDN/PSTN Network Service Parameters Using The Fast Configuration Wizard:

The *Fast Configuration Wizard's* ISDN/PSTN configuration sequence begins with the *ISDN/PSTN* dialog box:



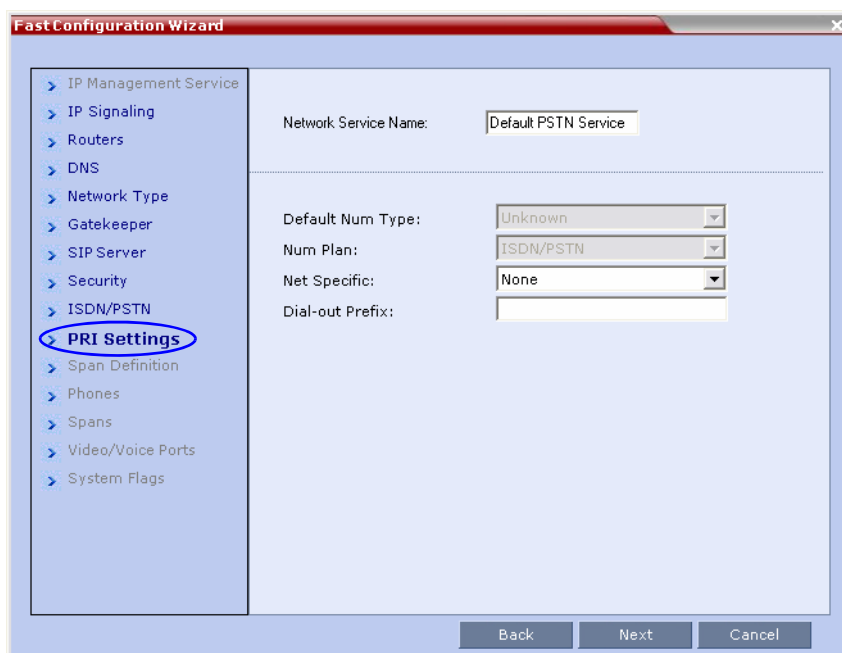
- 1 Define the following parameters:

Table 1-1 ISDN Service Settings

Field	Description
<i>Network Service Name</i>	Specify the service provider's (carrier) name or any other name you choose, using up to 20 characters. The Network Service Name identifies the ISDN/PSTN Service to the system. Default name: PSTN Service Note: This field is displayed in all ISDN/PSTN Network Properties tabs and can contain character sets that use Unicode encoding.
<i>Span Type</i>	Spans are ISDN/PSTN lines, supplied by the service provider, that are connected to the RMX. Each span can be defined as a separate Network Service, or all the spans from the same carrier can be defined as part of the same Network Service. Select the Span Type from the drop-down menu: <ul style="list-style-type: none"> • T1 (U.S. – 23 B channels + 1 D channel) • E1 (Europe – 30 B channels + 1 D channel) Default: T1
<i>Service Type</i>	PRI is the only supported service type. It is automatically selected.

- 2 Click Next.

The *PRI Settings* dialog box opens.



3 Define the following parameters:

Table 1-2 *PRI Settings*

Field	Description
<i>Default Num Type</i>	<p>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. Select the Default Num Type from the list.</p> <p>If the PRI lines are connected to the RMX 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.</p> <p>Default: Unknown</p> <p>Note: For E1 spans, this parameter is set by the system.</p>
<i>Num Plan</i>	<p>Select the type of signaling (Number Plan) from the list according to information given by the service provider.</p> <p>Default: ISDN</p> <p>Note: For E1 spans, this parameter is set by the system.</p>
<i>Net Specific</i>	<p>Enter the prefix that the PBX requires to dial out. Leave this field blank if a dial-out prefix is not required.</p> <p>The field can contain be empty (blank) or a numeric value between 0 and 9999.</p> <p>Default: Blank</p>
<i>Dial-out Prefix</i>	<p>Enter the prefix that the PBX requires to dial out. Leave this field blank if a dial-out prefix is not required.</p> <p>The field can contain be empty (blank) or a numeric value between 0 and 9999.</p> <p>Default: Blank</p>

4 Click **Next**.

The *Span Definition* dialog box opens.

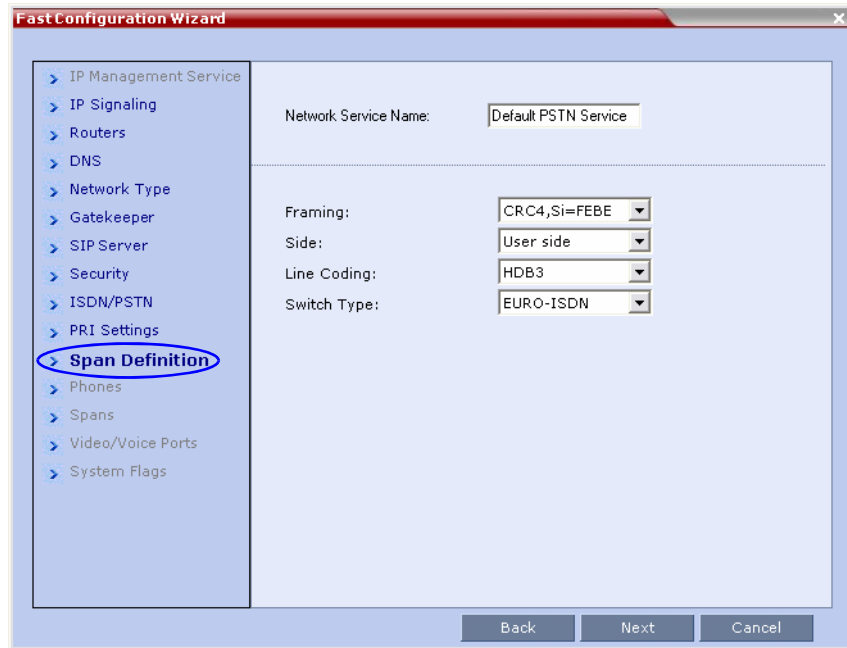
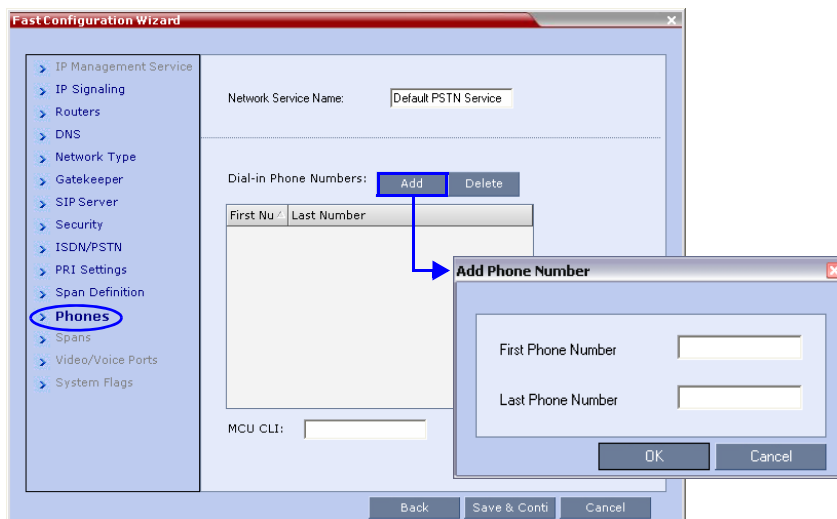


Table 1-3 Spans Settings

Field	Description
<i>Framing</i>	The frame format used by the carrier for the network interface. Select the Framing format from the list. <ul style="list-style-type: none"> For T1 spans, default is SFSF. For E1 spans, default is FEBE.
<i>Side</i>	Select one of the following options: <ul style="list-style-type: none"> User side (default) Network side Symmetric side <p>Note: If the PBX is configured on the network side, then the RMX unit must be configured as the user side, and vice versa, or both must be configured symmetrically.</p>
<i>Line Coding</i>	Select the PRI line coding method from the list. <ul style="list-style-type: none"> For T1 spans, default is B8ZS. For E1 spans, default is HDB3.
<i>Switch Type</i>	Select the brand and revision level of switch equipment installed in the service provider's central office. <ul style="list-style-type: none"> For T1 spans, default is AT&T 4ESS. For E1 spans, default is EURO ISDN.

- 5 Click **Next**.
The *Phones* dialog box opens:
- 6 To define dial-in number ranges click the **Add** button.
The *Add Phone Number* dialog box opens.



- 7 Define the following parameters:

Table 1-4 Phones Settings

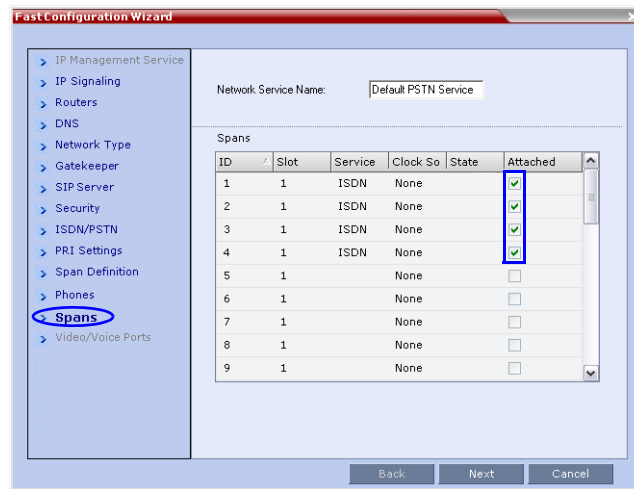
Field	Description
<i>First Number</i>	The first number in the phone number range.
<i>Last Number</i>	The last number in the phone number range.

- 8 Click **OK**.
The new range is added to the table.
- 9 **Optional.** Repeat steps 6 and 8 to define additional dial-in ranges.
- 10 Enter the *MCU CLI* (Calling Line Identification).
In a dial-in connections, the *MCU CLI* indicates the MCU's number dialed by the participant. In a dial-out connection, indicates the MCU (CLI) number as seen by the participant
- 11 Click **Save & Continue**.
After clicking **Save & Continue**, you cannot use the **Back** button to return to previous configuration dialog boxes.
The ISDN/PSTN Network Service is created and confirmed.



- 12 Click **OK** to continue the configuration.
The *Spans* dialog box opens displaying the following read-only fields:
 - **ID** – the connector on the ISDN/PSTN card (PRI1 - PRI12).
 - **Slot** – the MPM board that the ISDN/PSTN card is connected to (1 or 2)

- *Service* – the network service assigned (ISDN)
- *Clock Source* – the RTM board providing the clock source. The first span to synchronize becomes the primary clock source.
- *State* – the ISDN/PSTN card’s clock source (Primary, Backup or None)



13 Attach spans to existing network services, by marking the appropriate checkboxes in the *Attached* field.

14 Click **Next**.

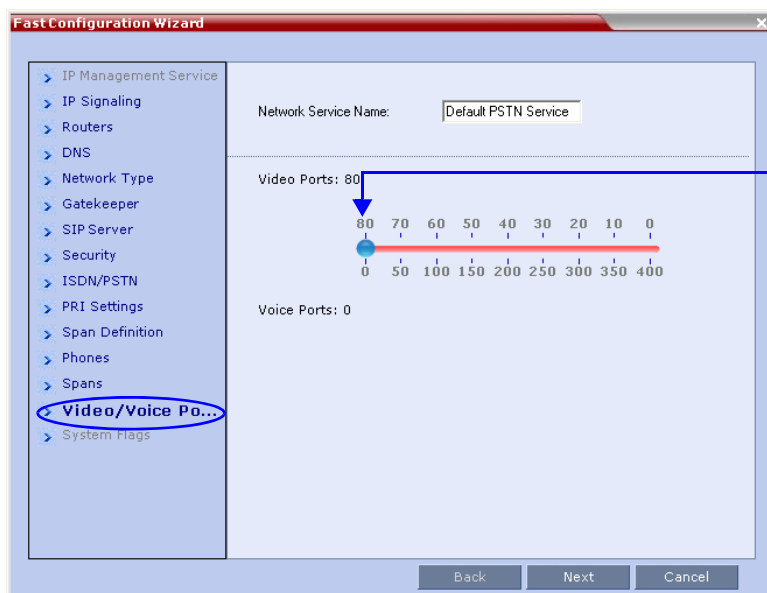
The Video/Voice Ports dialog box opens.

Video ports can be converted to voice ports to enable maximized usage of the system’s resources.

The conversion ratio is 1:5, up to a maximum of 400 (80 x 5) voice ports. The voice ports are used to connect VoIP and PSTN participants.



If the system runs out of voice ports, video ports can be used to connect voice participants. If all video ports are used, voice ports cannot be used to connect the additional video participants (unless they connect as *Audio Only*).



15 Move the slider to the required setting.

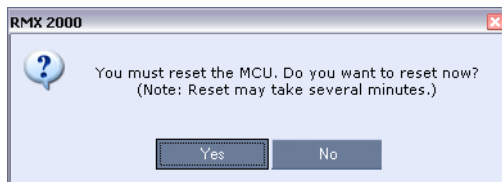


The maximum number of video ports displayed in the dialog box is taken from the license key. Only this number can be converted into voice ports.

The slider moves only in multiples of 10, converting video ports to voice ports in groups of ten, with each video port converting to five voice ports.

All available ports are initially allocated as video ports.

16 Click **Save & Close**.



17 Click **Yes** to complete the *Fast Configuration Wizard* and reset the RMX.

The ISDN/PSTN Network Service is created by the RMX and is added to the ISDN/PSTN Network Services list. If the system cannot create the Network Service, an error message is displayed indicating the cause and allowing you access the appropriate dialog box in the *Fast Configuration Wizard* for corrective action.

Configuring the ISDN/PSTN Network Service from the Network Service List

If you have not defined the ISDN/PSTN Network Service during the initial system configuration or if you have added the RTM ISDN card at a later stage, you can define the ISDN/PSTN Network Service from the ISDN/PSTN Network Services list. In addition, you can define a second ISDN/PSTN Network Service if you are using two different service providers or different switches.

To Configure a New ISDN/PSTN Network Service from the Network Services List:

- 1 In the RMX Management pane, click **ISDN/PSTN Network Services**
- 2 In the *ISDN/PSTN Network Services* list pane, click the **Add Network Service** button or right click anywhere in the list pane, and select **Add New Network Service**.

The *Fast Configuration Wizard - ISDN/PSTN Network Service* configuration sequence begins, letting you define the ISDN/PSTN Network Services properties. This is the same wizard as in the initial configuration of the MCU.

For more information see “*Configuring the ISDN/PSTN Service Using the Fast Configuration Wizard*” on page [1-22](#).

Conferencing via PSTN Connections

The connection of PSTN participants to conferences is enabled only via Entry Queues to which an ISDN/PSTN dial-in number is assigned. Dial-out participants can be defined in the *Address Book* or directly in the ongoing conference.

Allocating Dial-In Numbers to Entry Queues for ISDN/PSTN Connections

To enable PSTN participants to dial in to a conference, an ISDN/PSTN dial-in number must be assigned to the Entry Queue. Up to two dial-in numbers can be assigned to each Entry Queue. The dial-in numbers must be allocated from the dial-in number range defined in the ISDN/PSTN Network Service. You can allocate the two dial-in numbers from the same ISDN/PSTN Network Service or from two different ISDN/PSTN Network Services. The dial-in number must be communicated to the PSTN dial-in participants.



If a participant dials a number that is defined in the ISDN/PSTN Network Service but is not assigned (allocated) to an Entry Queue, upon connection to the MCU, the participant will be transferred to the Transit Entry Queue.

To enable ISDN/PSTN dial-in numbers in the Default Entry Queue after upgrade:

After upgrading the RMX from a version that did not support ISDN/PSTN, the *Default Entry Queue* does not have any ISDN/PSTN dial-in numbers allocated to it. It also does not know the name of the ISDN/PSTN Network Service and therefore cannot retrieve dial-in numbers from it.

- 1 Display the properties of the *Default Entry Queue*.
- 2 Select the **Enable ISDN/PSTN Access** check box.
- 3 Click **OK**.

This system automatically assigns an ISDN/PSTN dial-in number to the *Default Entry Queue*.

To allocate PSTN/ISDN dial-in numbers to an Entry Queue:

The dial-in number(s) can be allocated during the definition of a new Entry Queue or by modifying the properties of an existing Entry Queue.

- 1 In the *Entry Queue Properties* dialog box, select the **Enable ISDN/PSTN Access** check box.

This enables you to allocate dial-in numbers for ISDN/PSTN connections.



To define the first dial-in number using the default ISDN/PSTN Network Service, leave the default selection. When the Entry Queue is saved on the MCU, the dial-in number will be automatically assigned to the Entry Queue. This number is taken from the dial-in numbers range in the default ISDN/PSTN Network Service.

- 2 To select a different ISDN/PSTN Network Service in the service list, select the name of the Network Service.
- 3 To define the dial-in number, enter a required number from the dial-in number range defined for the selected Network Service. If this field is left blank, the system will automatically assign a number from the selected Network Service.
- 4 By default, the second dial-in number is not defined (the Network Service field is set to none). To define a second dial-in number, enter the dial-in number from the dial-in number range defined in the selected Network Service.
- 5 Click OK.

The Entry Queue is displayed in the Entry Queues list with the appropriate dial-in numbers that are assigned to it.



The dial-in number assigned to the Entry Queue can be seen in the *Entry Queues* list pane or when displaying the Entry Queue properties.

Connecting to Conferences via ISDN/PSTN

PSTN participants are *Audio Only* participants. They can connect to conferences and Meeting Rooms only via an Entry Queue.

Up to two dial-in numbers can be allocated to an Entry Queue for use by PSTN participants.

Calls to numbers within the PSTN *Dial-in Range* that are not allocated to an Entry Queue are routed to the *Transit Entry Queue*.

Undefined Dial-in Participants

Dial-in PSTN participants dial one of the dial-in numbers assigned to the Entry Queue, including the country and area code (if needed). They are routed to their conference according to the conference ID.

Defined Dial-out Participants

Dial-out PSTN participants are defined with their dial-out number. Once they are added to the ongoing conference the MCU automatically calls them, using the default ISDN/PSTN Network Service defined for the participant (usually the default service)..



You cannot add defined ISDN/PSTN dial-in participants to the Address Book or Ongoing Conferences.

Encryption

The PSTN (H.320) protocol, as well as PSTN endpoints do not support encryption. PSTN participants can therefore only connect to encrypted conferences if the system is set up to allow the mixing of encrypted/non-encrypted participants in the same conference.

Monitoring ISDN/PSTN Participants

Using the *Participant Properties* dialog box, you can monitor and verify the properties of an ISDN/PSTN participant. The dialog box's tabs contain information that is relevant to the participant's status only while the conference is running and is used to monitor the participant's status when connection problems occur.

To view the participant's properties during a conference:

- 1 In the *Participants* list, right click the desired participant and select **Participant Properties**.

The *Participant Properties - Media Sources* dialog box is displayed. This dialog box displays the video layout and capabilities to mute or block the participant's audio transmission to the conference. Only the enabled audio transmission capabilities are relevant to PSTN Audio Only conferences.

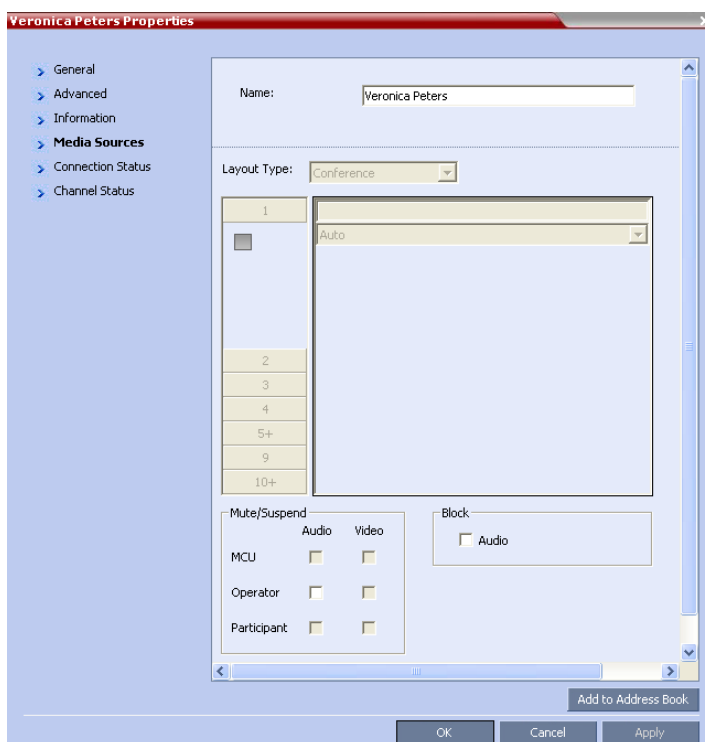


Table 1-5 ISDN/PSTN Participant Properties - Media Sources

Field	Description
<i>Mute/Suspend (by Operator)</i>	When checked by the user, mutes the participant's audio transmission to the conference.
<i>Block (Audio)</i>	When checked, the audio transmission from the conference to the participant's endpoint is blocked, but the participant will still be heard by other participants.

- 2 Click the **Connection Status** tab to view general information regarding the participant connection and disconnection causes of the participant to the conference.

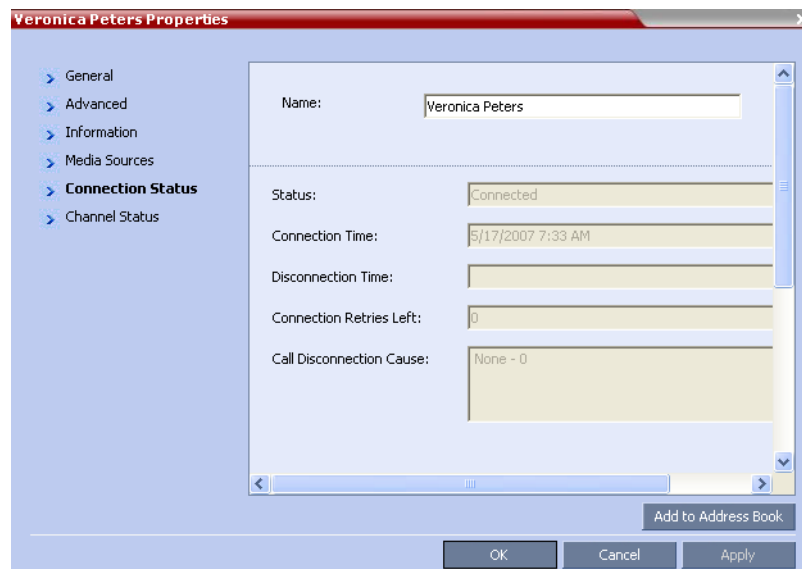


Table 1-6 ISDN/PSTN Participant Properties - Connection Status

Field	Description
<i>Status</i>	Indicates the connection status of the participant to the conference. If there is a problem, the appropriate status appears, for example, Disconnected.
<i>Connection Time</i>	The date and time the participant connected to the conference.
<i>Disconnection Time</i>	The date and time the participant was disconnected from the conference.
<i>Connection Reties Left</i>	Indicates the number of retries left for the system to connect the participant to the conference.

Table 1-6 ISDN/PSTN Participant Properties - Connection Status

Field	Description
<p><i>Call Disconnection Cause</i></p>	<p>Lists the categories and parameters which indicate the cause of participant's disconnection from the conference. The information is displayed according to the protocol/standard defined for the participant, and the parameters vary accordingly.</p> <p>Unallocated (unassigned) number – This cause indicated that the destination requested by the calling user cannot be reached because, although the number is in a valid format, it is not currently assigned (allocated).</p> <p>Channel unacceptable – This cause indicates the channel most recently identified is not acceptable to the sending entity for use in this call.</p> <p>Normal call clearing – This cause indicates that the call is being cleared because one of the users involved in the call has requested that the call be cleared.</p> <p>In a normal situation, the source of this cause is not the network.</p> <p>User busy – This cause is used when the called user has indicated the inability to accept another call. It is noted that the user equipment is compatible with the call.</p> <p>No user responding – This cause is used when a user does not respond to a call establishment message with either an alerting or connect indication within the prescribed period of time allocated.</p> <p>No answer from user (user alerted) – This cause is used when a user has provided an alerting indication but has not provided a connect indication within a prescribed period of time.</p> <p>Call rejected – This cause indicates that the equipment sending this cause does not wish to accept this call, although it could have accepted the call because the equipment sending this cause is neither busy nor incompatible.</p> <p>Number changed – This cause is returned to a calling user when the called party number indicated by the calling user is no longer assigned. The new called party number may optionally be included in the diagnostic field.</p> <p>Invalid number format – This cause indicates that the called user cannot be reached because the called party number is not a valid format or is not complete.</p> <p>Facility rejected – This cause is returned when a facility requested by the user can not be provided by the network.</p>

- 3 Click the **Channel Status** tab to view the status of a participant's channels.

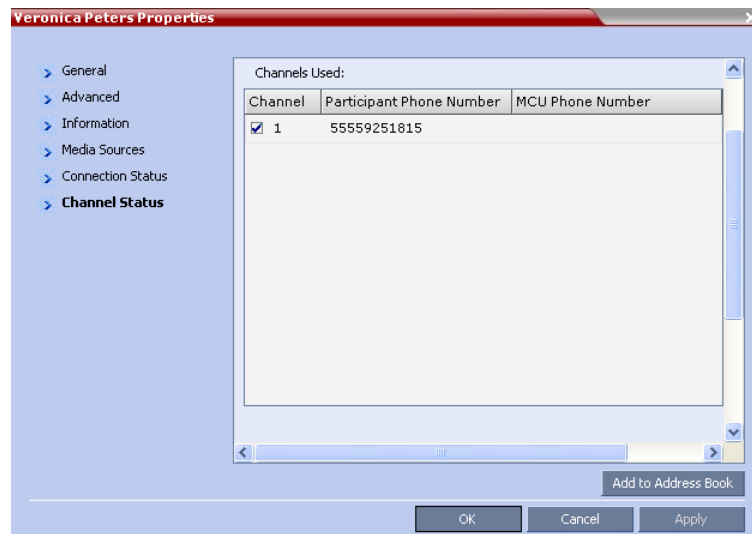


Table 1-7 ISDN/PSTN Participant Properties - Channel Status

Field	Description
<i>Channels Used</i>	<ul style="list-style-type: none"> • Channel – Indicates the channel used by the participants and whether the channel is connected (indicated with a check mark) or disconnected. • Participant Phone Number – In a dial-out connection, indicates the participant's phone number dialed by the MCU. • MCU Phone Number – In a dial-out connection, indicates the MCU (CLI) number as seen by the participant. This is the number entered in the MCU Number field in the Network Service.

Defining PSTN Participants

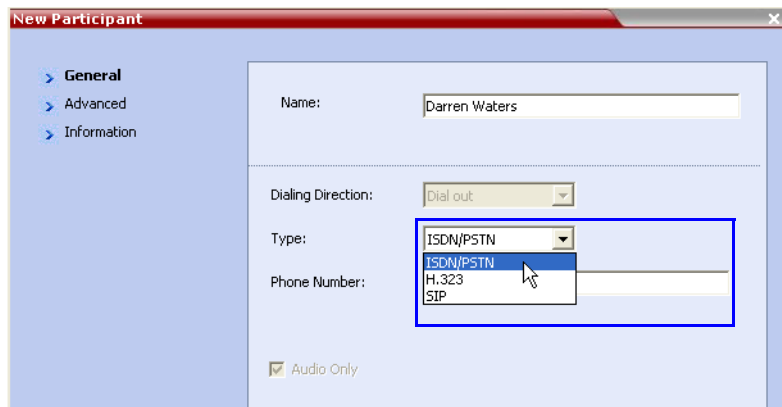
Only defined dial-out PSTN participants can be added to the Address Book or on-going conferences. ISDN/PSTN participants are added to the Address Book in the same manner that H.323 and SIP participants are added.

When adding dial-out PSTN participants to the ongoing conference, the system automatically dials out to the participants using the ISDN/PSTN service defined for the connection in the participant properties.

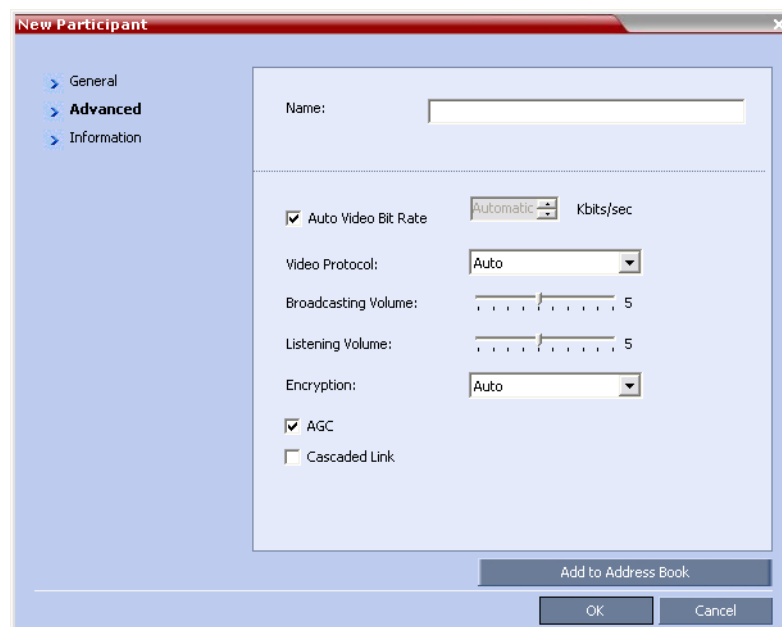
To add a defined dial-out PSTN participant to the Address Book:

- 1 In the *Address Book* list, click the **New Participant** button.
The *New Participant* dialog box opens.
- 2 In the *New Participant - General* dialog box, define the participant name.
- 3 In the *Type* field, select **ISDN/PSTN**.

The *Dialing Direction* automatically changes to dial-out (the selection cannot be changed) and the **Audio Only** option is selected.



- 4 In the *Phone Number* box enter the participant's phone number, including the Country and Area Code.
- 5 **Optional.** Click the **Advanced** tab and define the Advanced parameters.



Encryption is not supported by the H.320 Protocol, therefore it is not supported in PSTN calls. PSTN participants can connect to encrypted conferences only if the system flag is set to allow non-encrypted participants to connect to encrypted conferences.

- 6 **Optional.** Click the **Information** tab. Define additional information (as for IP participants). The information can be entered using Unicode.
- 7 Click **OK**.

The new participant is added to the *Address Book* with an Audio Only icon. The participant phone number is added to the *IP Address/Phone* list.

Detailed Description - General

Video/Voice Port Configuration

In version 2.0, video ports can be converted to voice ports to enable maximized usage of the system's resources.

The conversion ratio is 1:5, up to a maximum of 400 (80 x 5) voice ports. The voice ports are used to connect VoIP and PSTN participants.



If the system runs out of voice ports, video ports can be used to connect voice participants. If all video ports are used, voice ports cannot be used to connect the additional video participants (unless they connect as *Audio Only*).

There are two methods of configuring the Video/Voice Ports:

- During *First Entry Configuration* as part of the *Fast Configuration Wizard*
- From the *RMX - Setup* menu. This option enables you to modify the port configuration dynamically, according to changes in conferencing needs.

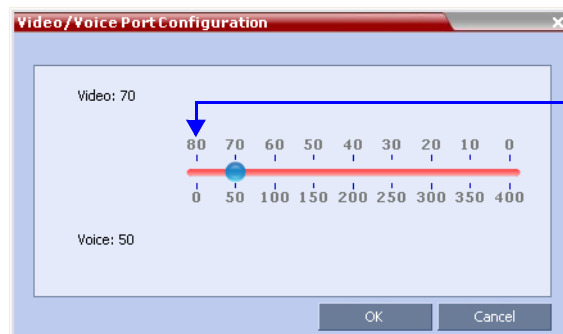
To configure Video/Voice Ports in the Fast Configuration Wizard:

After the configuration of the Default IP Network Service and ISDN/PSTN Network Service (optional), the *Video/Voice Port Configuration* dialog box is displayed.



The maximum number of video ports displayed in the *Port Configuration* dialog box is taken from the license key. Only this number can be converted into voice ports.

- ➔ In the *Fast Configuration Wizard - Port Configuration* dialog box, move the slider to the required setting.

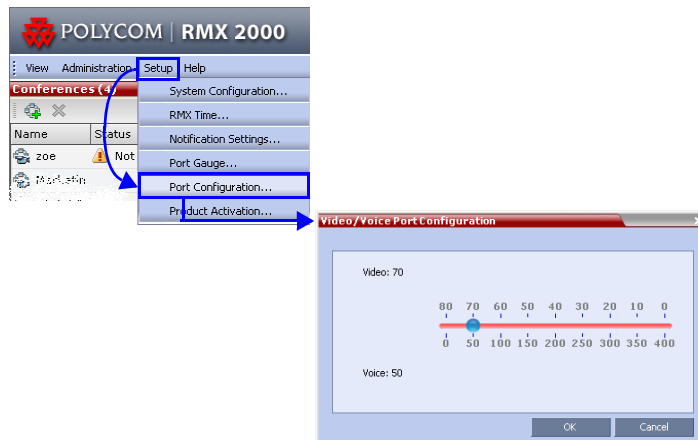


The slider moves only in multiples of 10 converting video ports to voice ports in groups of ten, with each video port converting to five voice ports.

To configure Video/Voice Ports from the Setup Menu:

Before starting this procedure be sure that no conferences are running on the MCU.

- ➔ On the RMX menu, click **Setup > Video/Voice Port Configuration** to open the *Port Configuration* dialog box.



The definition is the same as in the *Fast Configuration Wizard*.



The MCU must be reset for changes in the *Port Configuration* to take effect.

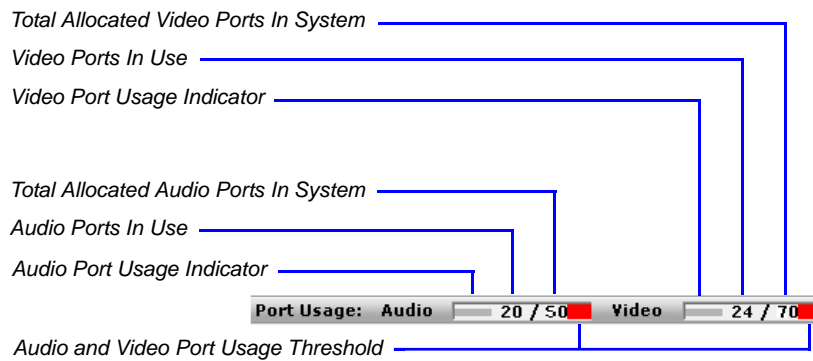
Port Usage Gauges

Viewing Permissions		
Chairperson		
Operator	✓	
Administrator		✓

In version 2.0, an additional *Port Gauge* displays the *Port Usage* of voice ports configured in the system. The additional gauge is displayed only if voice ports are configured in the system.

The *Port Usage Gauges* indicate:

- The number of ports in the system
- The number of ports in use
- The Video/Voice Port Configuration (allocation)
- The *Capacity Usage* threshold.



The usage threshold represents a percentage of the total number of video or voice ports available. It is set to indicate when resource usage is approaching its maximum, resulting in no free resources to run additional conferences. When port usage reaches or exceeds the threshold, the red area of the gauge flashes and a *System Alert* is generated. The default port usage threshold is 80% and can be set by the system administrator.

Resource Report Update

Overview

In version 2.0, the Resource Report has been adapted to display video and audio port usage according to their allocation in the video/voice port configuration.

Detailed Description

The Resource Report includes two rows: video and audio. Each row indicates resources according to port allocation.

Type	Total	Occupied	Free
Audio	50	0	50
Video	70	8	62

The *Total* column displays the number of ports remained as video ports and how many were allocated as audio ports. This number reflects the current audio/video port configuration. Any changes to the port allocation will affect the port usage displayed in the Resource Report.

Video resources usage varies according to the video resolution used by the endpoints. The higher the video resolution (quality), the greater the amount of video resources consumed by the MCU.

Table 2 Video Quality Vs. Port Usage (in CP mode)

Endpoint Connection Bit Rate	Video Quality			
	Motion		Sharpness	
	Resolution	Video Ports Required	Resolution	Video Ports Required
128kbps	CIF	1	CIF	1
256kbps	CIF	1	SD15	2
384kbps	2CIF30	2	SD15	2
512kbps	2CIF30	2	SD30	4
768 - 1472kbps	SD30	4	SD30	4
128 - 4000kbps	HD	4	HD	4

By default, the RMX is shipped with all licensed ports set to video. You can modify the port allocation settings via the RMX Web Client (Voice/Video Port Configuration) to enable voice ports. Administrators can use the Resource Report to assess that a different voice/video port configuration may be required.

When video ports are fully used, the system cannot use free audio ports for video. When audio port resources are fully used, video ports can be used, using one video port to connect one voice participant.

For more information, see “Video/Voice Port Configuration” on page 1-37.



Additional information regarding PSTN spans (PRI Lines) and faulty ports can be obtained via the Hardware Monitor.

Unicode Support

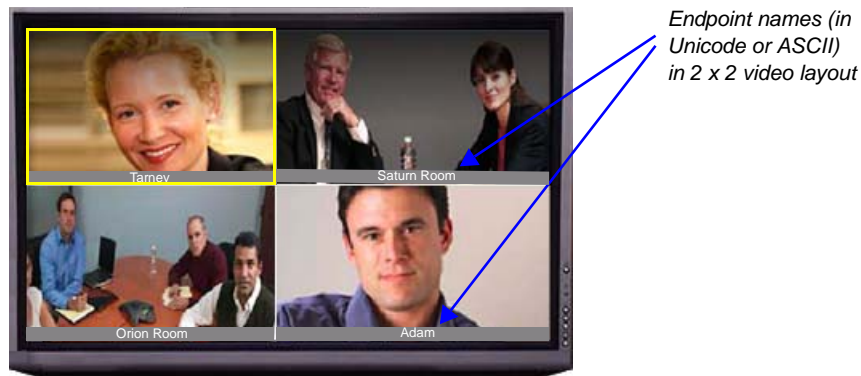
Unicode (an international standard that enables the display of complex scripts such as Japanese, Chinese, etc.) is now supported with the RMX. It enables complex scripts to display endpoint names in the *video layouts* and the names of conferences, Meeting Rooms, Entry Queues and services in the *RMX Web Client*.

Latin (western scripts) character sets (single-byte character sets) can be represented by character sets of up to 256 characters: for example, French, English, Spanish, etc. However, for complex languages such as Japanese, with more than 256 characters, it is insufficient and Unicode UTF-8 with its double-byte encoding scheme is used.

Unicode (UTF8) must be supported by the workstation's operating system and selected as the encoding method in the browser.

Display of Unicode Endpoint Names in Conference Layouts

During conferences, the endpoint name is displayed in its window that is part of the conference video layout windows. If Unicode is used to define the endpoint's name, the RMX displays the name correctly.



If the endpoint does not send its name, and it is a defined participant, the system displays the endpoint name as defined in the *Display Name* field in the participant Properties.

If the endpoint's *Display Name* is changed in the *RMX Web Client* during the conference, the new name overrides the previously defined endpoint name, or the name sent from the endpoint.

Display of Unicode Text in RMX Web Client Fields

Unicode support enables the user to enter information in native language character sets in the Name and Info text fields of the *RMX Web Client*. In conferencing entities in which the name can also be used for routing participants to their conferences only ASCII characters are allowed. Therefore, the Name field is now called Routing Name and a new field is introduced - Display Name.

Both Routing Name and Display name fields are included in the CDR files.

Display Name

The Display Name is the conferencing entity name in native language character sets to be displayed in the RMX Web Client.

In conferences, Meeting Rooms, Entry Queues and SIP factories the system automatically generates an ASCII name for the *Display Name* field that can be modified using Unicode encoding.

Text Field Length

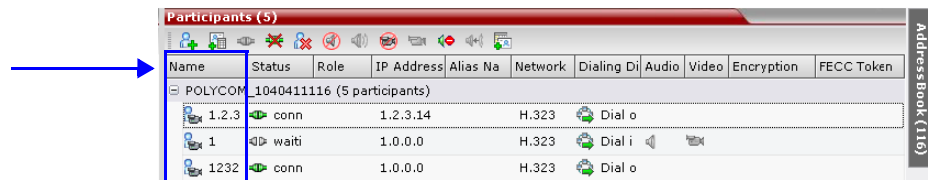
English text uses ASCII encoding and can contain the most characters (length varies according to the field).

European and Latin text length is approximately half the length of the maximum.

Asian text length is approximately one third of the length of the maximum.

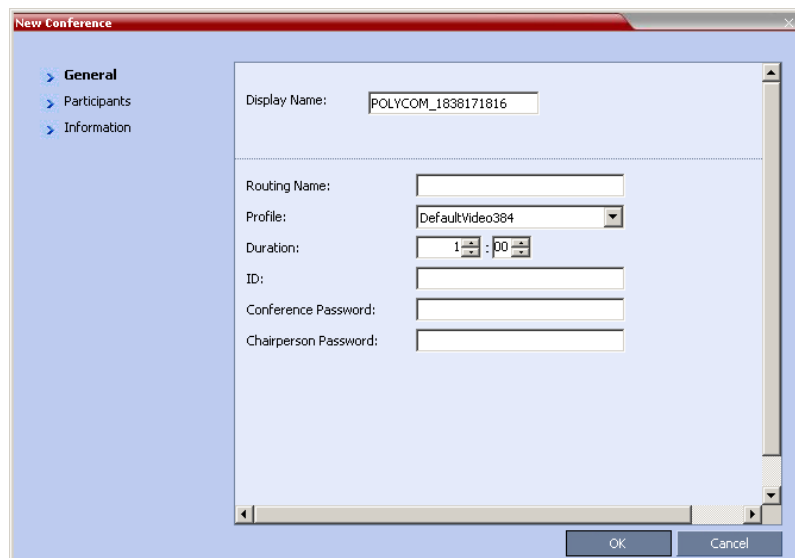
Participant Name Using an External Database

When the RMX uses an external database for participant authentication, dial in participant's name is displayed in the *RMX Web Client - Participants* list *Name* field as it is defined in the external database using the external database encoding.



The following fields can contain Unicode text:

- Participant Name (becomes the endpoint name when no name is defined at the endpoint)
- Display Name in:
 - Conference
 - Meeting Room
 - Entry Queue
 - SIP Factory
- Profile Name
- Info fields
- Service Name (IVR, Network)



Routing Name

Routing Name is the name with which ongoing conferences, Meeting Rooms, Entry Queues and SIP Factories register with various devices on the network such as gatekeepers and SIP server. This name must be defined using ASCII character set.

Comma, colon and semicolon characters cannot be used in the *Routing Name*.

The *Routing Name* can be defined by the user or automatically generated by the system if no *Routing Name* is entered as follows:

Multiple Web Clients on the Same RMX

Different *RMX Web Clients* connected to the same RMX must each support Unicode to ensure that the Unicode information is displayed correctly in all browsers.

- If an all ASCII text is entered in *Display Name*, it is used also as the *Routing Name*.
- If any combination of Unicode and ASCII text (or full Unicode text) is entered in *Display Name*, the ID (such as Conference ID) is used as the *Routing Name*.

Multilingual Web Client

In Version 2.0, the *RMX Web Client* user interface is translated and supports 11 additional languages.

Supported Languages

- English US
- Traditional Chinese
- Simplified Chinese
- Japanese
- Korean
- Russian
- Spanish (South American)
- German
- Italian
- French
- Norwegian
- Portuguese (Brazilian)

Translated Elements

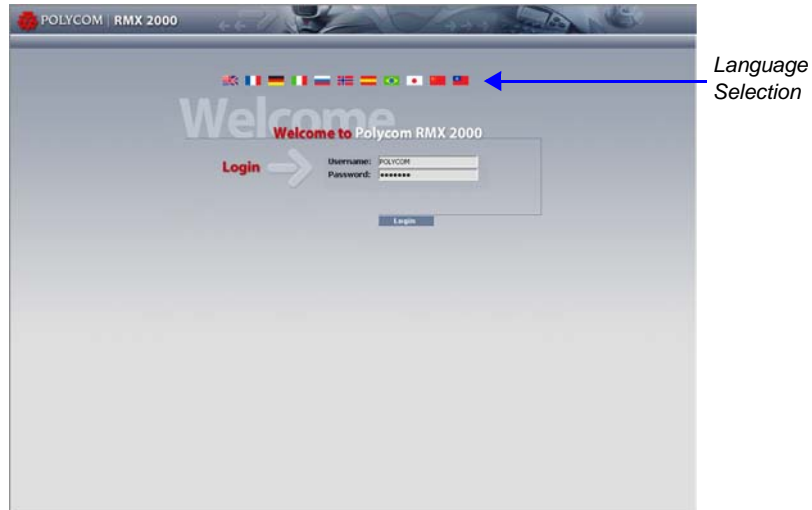
The following *RMX Web Client* elements are translated into the selected language:

- *RMX Web Client* screen strings
- Errors
- Profiles
- Services:
 - IP
 - PSTN/ISDN
 - IVR
 - SIP Factory
- Meeting Room definitions
- Entry Queue definitions
- Faults
- Alarms
- Status
- Communication messages
- Formatted CDR

Login Screen

The language is selected by clicking on the corresponding country flag.

If a language is selected the *RMX Web Client* that is not supported by the browser or the workstation's operating system, the *RMX Web Client* is displayed in English.



If a language is selected the *RMX Web Client* that is not supported by the browser or the workstation's operating system, the *RMX Web Client* is displayed in English.

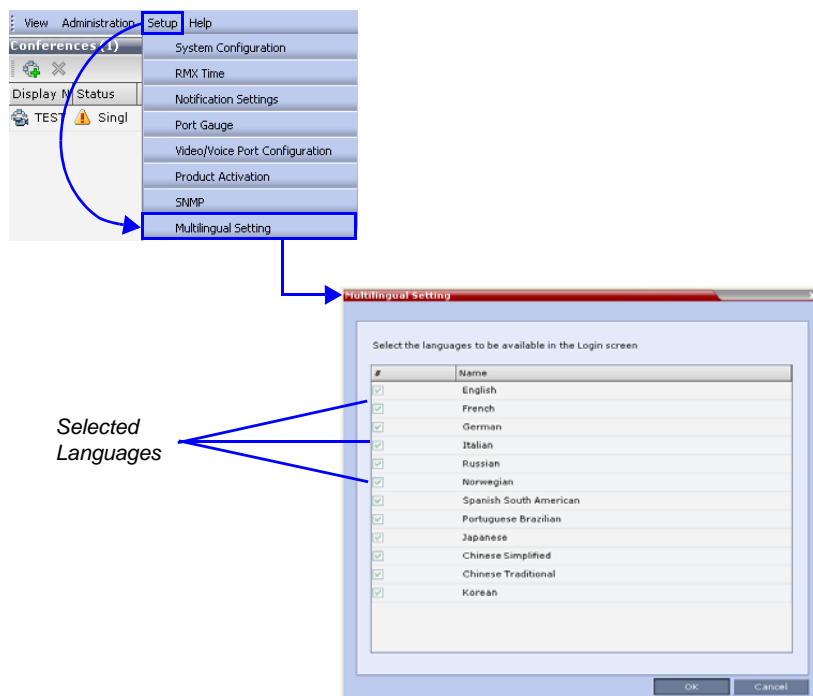
Multilingual Setting

The language selection options of the *RMX Web Client* can be modified via the *Multilingual Setting* of the system.

To customize the Multilingual Setting:

- 1 On the RMX menu, click **Setup > Multilingual Setting**.

The *Multilingual Setting* dialog box is displayed.



- 2 Place checkmarks in the boxes of the languages to be available for selection.
- 3 Click OK.
- 4 **Logout** and **Login** for the customization to take effect.

SNMP (Simple Network Management Protocol)

SNMP standard protocol is now supported with the RMX. It enables managing and monitoring of the MCU status by **external** managing systems, such as HP OpenView or through web applications.

Detailed Description

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 SNMP 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.

MIB (Management Information Base) Files

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.

The MIBS are contained in files in the *SNMP MIBS* sub-directory of the RMX 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.

Private MIBS

- *RMX-MIB (RMX-MIB.MIB)*
 - Contains the statuses of the RMX: Startup, Normal and Major.
 - Contains all the Alarms of the RMX that are sent to the SNMP Manager.

Support for MIB-II Sections

The following table details the MIB-II sections that are supported:

Table 3 Supported MIB-II Sections

Section	Object Identifier
<i>system</i>	mib-2 1
<i>interfaces</i>	mib-2 2
<i>ip</i>	mib-2 4

The Alarm-MIB

MIB used to send alarms. When a trap is sent, the Alarm-MIB is used to send it.

H.341-MIB (H.341 – H.323)

- Gives the address of the gatekeeper.
- Supports H.341-MIB of SNMP events of H.323.

Standard MIBs

This section describes the MIBs that are included with the RMX 2000. These MIBs define the various parameters that can be monitored, and their acceptable values.

MIB Name	Description
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)	This 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)	Used to identify managed objects for an H.320 MCU. It consists of four groups: System, Conference, Terminal, and Controls. The <i>Conference</i> group consists of the active conferences. The <i>Terminal</i> group is used to describe terminals in active MCU conferences. The <i>Controls</i> group enables remote management of the MCU.
H323MC-MIB (H323-MC.MIB)	Used to identify objects defined for an H.323 Multipoint Controller. It consists of six groups: System, Configuration, Conference, Statistics, Controls and Notifications. The <i>Conference</i> group is used to identify the active conferences in the MCU. The <i>Notifications</i> group allows an MCU, if enabled, to inform a remote management client of its operational status.
MP-MIB (H323-MP.MIB)	Used to identify objects defined for an H.323 Multipoint Processor, and consists of two groups: Configuration and Conference. The <i>Configuration</i> group is used to identify audio/video mix configuration counts. The <i>Conference</i> 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.
ENTITY-MIB (ENTITY.MIB)	Describes the unit physically: Number of slots, type of board in each slot, and number of ports in each slot.

Traps

Three types of traps are sent as follows:

- 1 ColdStart trap. This is a standard trap which is sent when the MCU is reset.

```
coldStart notification received from: 172.22.189.154 at 5/20/2007
7:03:12 PM
Time stamp: 0 days 00h:00m:00s.00th
Agent address: 172.22.189.154 Port: 32774 Transport: IP/UDP Pro-
tocol: SNMPv2c Notification
Manager address: 172.22.172.34 Port: 162 Transport: IP/UDP
Community: public
Enterprise: enterprises.8072.3.2.10
Bindings (3)
  Binding #1: sysUpTime.0 *** (timeticks) 0 days
  00h:00m:00s.00th
  Binding #2: snmpTrapOID.0 *** (oid) coldStart
  Binding #3: snmpTrapEnterprise.0 *** (oid)
```

Figure 2 An Example of a ColdStart Trap

- 2 Authentication failure trap. This is a standard trap which is sent when an unauthorized community tries to enter.

```
authenticationFailure notification received from: 172.22.189.154
at 5/20/2007 7:33:38 PM
Time stamp: 0 days 00h:30m:27s.64th
Agent address: 172.22.189.154 Port: 32777 Transport: IP/UDP
Protocol: SNMPv2c Notification
Manager address: 172.22.172.34 Port: 162 Transport: IP/UDP
Community: public
Enterprise: enterprises.8072.3.2.10
Bindings (3)
  Binding #1: sysUpTime.0 *** (timeticks) 0 days
  00h:30m:27s.64th
  Binding #2: snmpTrapOID.0 *** (oid) authenticationFailure
  Binding #3: snmpTrapEnterprise.0 *** (oid)
  enterprises.8072.3.2.10
```

Figure 3 An Example of an Authentication Failure Trap

- 3** Alarm Fault trap. The third trap type is a family of traps defined in the POLYCOM-RMX-MIB file, these traps are associated with the RMX active alarm and clearance (proprietary snmp trap).

```

rmxFailedConfigUserListInLinuxAlarmFault notification received
from: 172.22.189.154 at 5/20/2007 7:04:22 PM
Time stamp: 0 days 00h:01m:11s.71th
Agent address: 172.22.189.154 Port: 32777 Transport: IP/UDP
Protocol: SNMPv2c Notification
Manager address: 172.22.172.34 Port: 162 Transport: IP/UDP
Community: public
Bindings (6)
  Binding #1: sysUpTime.0 *** (timeticks) 0 days
  00h:01m:11s.71th
  Binding #2: snmpTrapOID.0 *** (oid)
  rmxFailedConfigUserListInLinuxAlarmFault
  Binding #3: rmxAlarmDescription *** (octets) Insufficient
  resources
  Binding #4: rmxActiveAlarmDateAndTime *** (octets)
  2007-6-19,16:7:15.0,0:0
  Binding #5: rmxActiveAlarmIndex *** (gauge32) 2
  Binding #6: rmxActiveAlarmListName *** (octets) Active Alarm
  Table
* Binding #7: rmxActiveAlarmRmxStatus *** (rmxStatus) major
    
```

Figure 4 An Example of a Alarm Fault Trap

Each trap is sent with a time stamp, the agent address and the manager address.

Status Trap Content

The MCU sends status traps for the following status:

- **MAJOR** - A trap is sent when the card/MCU status is MAJOR.

All trap content is considered "MAJOR".

Defining the SNMP Parameters in the RMX

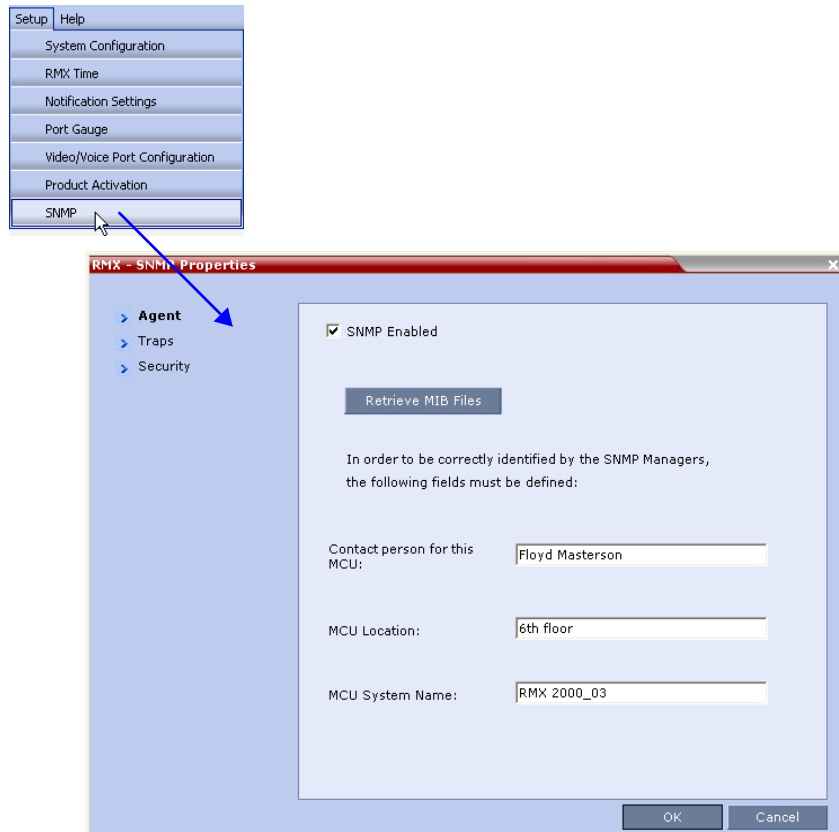
The SNMP option is enabled via the RMX Web Client application.

The addresses of the Managers monitoring the MCU and other security information are defined in the RMX Web Client application and are saved on the MCU's hard disk. Only users defined as Administrator can define or modify the SNMP security parameters in the RMX Web Client application.

To enable SNMP option:

- 1 In the RMX Web Client menu bar, click **Setup>SNMP**.

The *RMX-SNMP Properties - Agent* dialog box is displayed.



This dialog box is used to define the basic information for this MCU that will be used by the SNMP system to identify it.

- 2 In the *Agent* tab, click the **SNMP Enabled** check box.
- 3 Click the **Get MIB Files** button to obtain a file that lists the MIBs that define the properties of the object being managed.

The **Get MIB Files** dialog box appears.

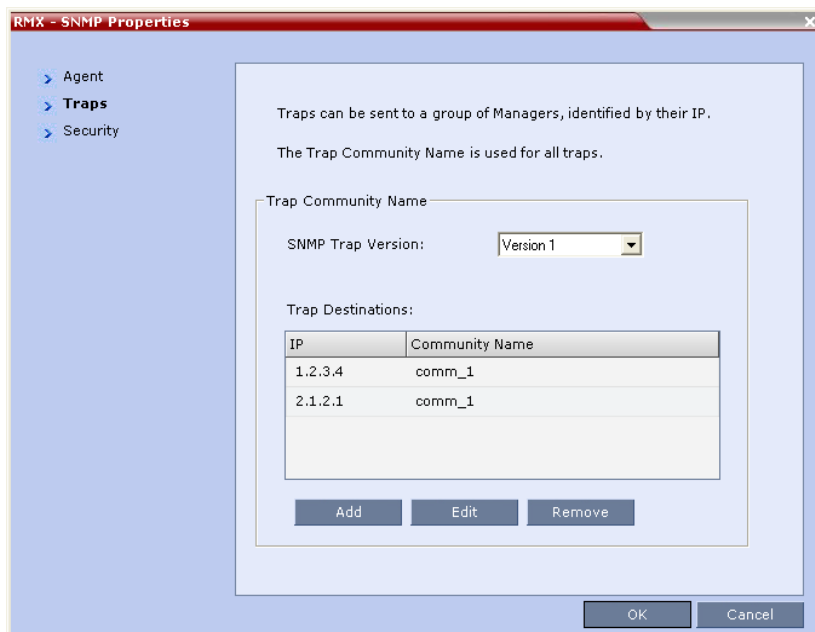
- 4 Click the **Browse** button and navigate to the desired directory to save the MIB files.
- 5 Click **OK**.

- 6 Define the following information in the *Agent* tab:
 These details allow the SNMP Management System and its user to easily identify the MCU.

Table 1-1 *SNMP Properties Options*

Field	Description
<i>Contact person for this MCU</i>	Type the name of the person to be contacted in the event of problems with the MCU.
<i>The Location of this MCU</i>	Type the location of the MCU (address or any description).
<i>The System Name of this MCU</i>	Type the MCU's system name.

- 7 Click the **Traps** tab.
 The *RMX-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.

- 8 Define the following parameters:

Table 1-2 *SNMP Properties – Traps Options*

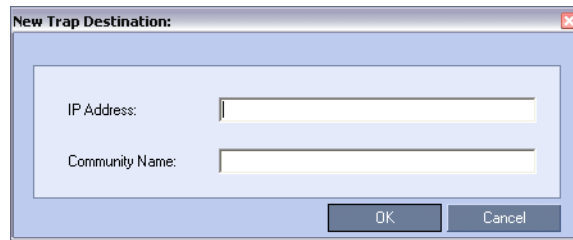
Field	Description
<i>SNMP trap version</i>	Type a string of characters that will be added to the message that is sent to the external Manager terminals. This string is used to identify the message source by the external Manager terminals. Note: The <i>Community Name</i> parameters must be defined identically in the external SNMP application.

Table 1-2 SNMP Properties – Traps Options (Continued)

Field	Description
<i>Trap Destination</i>	This box lists the currently defined IP addresses of the Manager terminals to which the message (trap) is sent.

- Click the **Add** button to add a new Manager terminal.

The *New Trap Destination* dialog box opens.



- Type the **IP Address** and the **Community name** of the manager terminal used to monitor the MCU activity, and then click **OK**.

The *Community name* is 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 terminal.

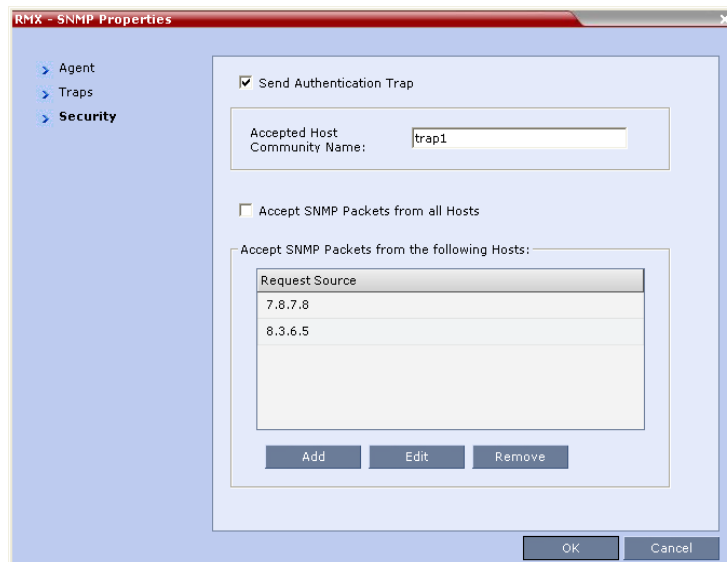
The new *IP Address* and *Community name* is added to the *Trap Destinations* box.

- 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.

- Click the **Security** tab.

The *RMX-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.

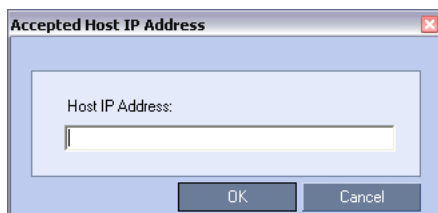
12 Define the following parameters:

Table 1-3 MCU-SNMP Properties – Security Options

Field	Description
<i>Send Authentication Trap</i>	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.
<i>Accept Community Names</i>	Type the strings added to queries that are sent from the SNMP Manager to indicate that they were sent from an authorized source. Note: Queries sent with different strings will be regarded as a violation of security, and, if the <i>Send Authentication Trap</i> check box is selected, an appropriate message will be sent to the SNMP Manager.
<i>Accept SNMP Packets from any Host</i>	Select this option if a query sent from any Manager terminal is valid. When selected, the <i>Accept SNMP Packets from These Hosts</i> option is disabled.
<i>Accept SNMP Packets from These Hosts</i>	Lists specific Manager terminals whose queries will be considered as valid. This option is enabled when the <i>Accept SNMP Packets from any Host</i> option is cleared.

13 To define the IP address of a specific Manager terminal, ensure that the *Accept SNMP Packets from any Host* option is cleared and then click the **Add** button.

The *Insert Accept Packet IP Address* dialog box opens.



14 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.



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.

15 In the *RMX - SNMP Properties - Security* dialog box, click **OK**.

CDR Event

A new CDR event has been added to the CDR in order to store the *Display Name* to support the Unicode naming for endpoints (participants), conferences, Meeting Rooms, Entry Queues and services.

The event name is *CONFERENCE START CONTINUE 10*, and the event code is 11001. In addition to the standard event fields, the event will contain one field, *Display Name*.

The value of the *Display Name* field, as well as the values of other fields that support Unicode values, such as the *info* fields, will be stored in the CDR file in UTF8. The application that reads the CDR must support Unicode.

The *Conference Name* field in the *Conference Summary Record* will contain the *Routing Name*.

Detailed Description - IP

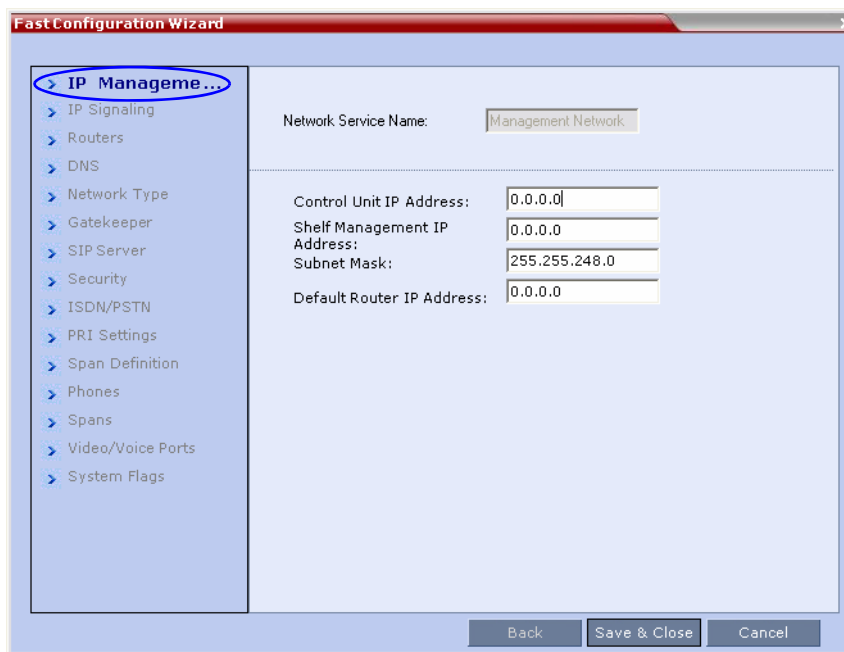
Configuring the Default Management Network

In Version 2.0, the direct connection method to define the *Default Management Network Service* has been modified to include a wizard.

During power-up, the system compares the *Default Management Network's* IP parameters with the *Factory Defaults* in the *lan.cfg* file stored on the *USB key*. If they are the same, it means the *Default Management Network's* settings have not been modified in the *USB key* and the *Fast Configuration Wizard* is started.

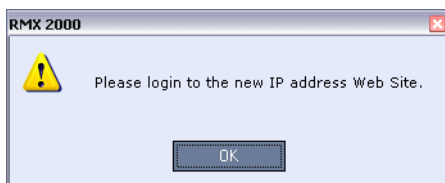
To Configure the Default Management Network:

- 1 In the *Fast Configuration Wizard – Management Network Properties* dialog box, define the parameters as set out in the *RMX Administrator's Guide*, "Modifying the Management Network" on page 8-4.



- 2 Click **Save & Close**

You are prompted to login using the *Control Unit IP Address* you have just entered.



- 3 Logout of the *RMX Web Client*.
- 4 Connect the RMX the local network via **LAN 2 Port**.
For more information see the *RMX 2000 Getting Started Guide*, "Connecting Cables" on page 2-3.
- 5 Start the RMX Web Client application on the workstation, by entering `http://<Control Unit IP Address>` as defined in the *Fast Configuration Wizard – IP Management Network Properties* tab and pressing **Enter**.

SIP Transport Layer Security (TLS)

Version 2.0 supports the *TLS* cryptographic protocol, used to ensure secure communications between the SIP server and the MCU over the Internet.

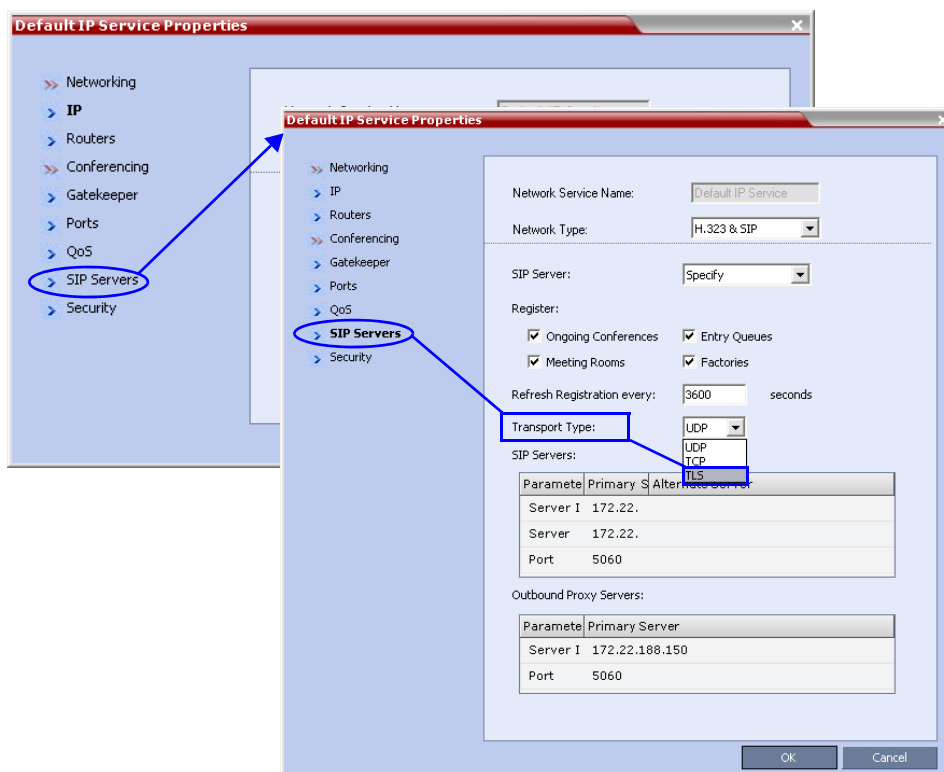
Only the server is authenticated while the client remains unauthenticated.

The following protocols are supported:

- TLS 1.0
- SSL 2.0
- SSL 3.0.

To enable TLS:

- 1** In the *RMX Management* pane, click **Network Services**.
- 2** In the *Network* list pane, double-click the **Default IP Service** entry.
- 3** Click the **SIP Servers** tab.



- 4** In the *Transport Type* list select **TLS**.

The *Signaling Host* listens on secured port 5061 only and all outgoing connections are established on secured connections. Calls from SIP clients or servers to non secured ports are rejected.

SIP Digest

Version 2.0 supports *SIP Digest* authentication, allowing two SIP entities to authenticate credentials with each other.

SIP Digest authentication is established by both SIP entities transmitting an MD5 (Message-Digest Algorithm 5) encrypted, shared password to each other without having to send a password in plain text over the network.

A SIP Server may require the RMX to authenticate itself during registration of SIP URIs such as Conferences, Meeting Rooms, Entry Queues and SIP factories, or when the RMX is trying to establish dial-out call via the SIP server.

To create a SIP Digest password:

- 1 In the *RMX Management* pane, click **Network Services**.
- 2 In the *Network* list pane, double-click the **Default IP Service** entry.
- 3 Click the **Security** tab.



- 4 Complete the following fields.

Table 2 *SIP Digest Authentication*

Field	Description
<i>Authentication User Name</i>	Enter the conference, Entry Queue or Meeting Room name as registered with the proxy. This field can contain up to 20 ASCII characters.
<i>Authentication Password</i>	Enter the conference, Entry Queue or Meeting Room password as defined in the proxy. This field can contain up to 20 ASCII characters.

If the *Authentication User Name* and *Authentication Password* fields are left empty, the *SIP Digest* authentication request is rejected. For registration without authentication, the RMX must be registered as a trusted entity on the SIP server.

- 5 Click **OK**.

Detailed Description - Partners

IBM/RMX V2.0 Integration

Version 2.0 supports the IBM/Polycom integration. It enhances IBM offering with Polycom’s high quality audio and video capabilities for both Point-2-Point and Multipoint conferencing scenarios.

The solution is based on Polycom’s integration with IBM’s SameTime (ST) Connect/ Web conferencing and Lotus Notes. The solution is achieved via a backend IBM server side API integration with Polycom’s SIP based conference Application Sever (PCAS – RAS 200i). RAS 200i manages the setting up and manipulating of Point-2-Point, as well as multipoint calls using Polycom’s high quality video endpoints and MCUs.

The following communication protocols are supported: SIP, PSTN and H.323.

Solution Components:

<u>IBM</u>	<u>Polycom</u>
• SameTime Client V.7.5	• PVX V.8.X
• Lotus Notes 6.5.5 and later	• VSX V.8.X
• IBM SIP Server	• RAS 2001 (PCAS for IBM)
• IBM Domino Server	• RMX MCU
	• Polycom Plug In SW (PPI);
	• PSTN Endpoints
	• H.323 Video Clients
	• H.323 GK (PN)

Enabling IBM Integration in the RMX

IVR Service

The external database application authentication must be enabled in the conference (or Entry Queue) IVR Service.

An IVR external application is used for dial-in SIP, H.323 and PSTN endpoints. The application needs to support participants with or without a PIN code. The PIN Codes are sent to the IBM external application for approval and if approved are marked with their audio/video presence according to the PIN code. Users without a PIN code are marked in the IBM web application as anonymous.

Dial-in SIP, H.323 and PSTN endpoints connecting to the conference enter their PIN Code as conference password.

The external database application can be configured to use the <ACTUAL_PARTY_PHONES> parameter of an API call, instead of a PIN Code, to identify the participant. The <ACTUAL_PARTY_PHONES> is set as follows:

- **ISDN participants** – the calling participant’s CLI number is used (available only if this information has been passed to the MCU)

- **H.323 participants** – the first E.164 alias. If no E.164 alias was defined, the first H.323 ID alias is used.
- **SIP participants** – the identification is derived from the participant's SIP URI.

System Configuration Flag

This feature is controlled by the *PIN_CODE_USAGE* system flag. The flag can be modified in the *system.cfg* file. It has the following possible values:

- **Yes** – a PIN Code is required
- **DEL** – users can enter a PIN Code or the # delimiter without a PIN Code

The default value of the flag is **Yes**.

Polycom – AVAYA Collaboration (Apollo)

The RMX can function as a component of the *Apollo* R2 and R3.01 environments.

In the *Apollo* environment, the *Avaya Communication Manager* (ACM) serves as a call manager for *Avaya* legacy phones, IP phones, and IP Soft Phones as well as a Gatekeeper for H.323 endpoints.

ACM utilizes *Apollo* to add desktop video capability to its large scale telephony environment.

The *Apollo* environment currently supports H.323 and ISDN/PSTN networks.

Endpoints within the *Apollo* environment can change their capabilities dynamically: for example, a voice call can become a video call.

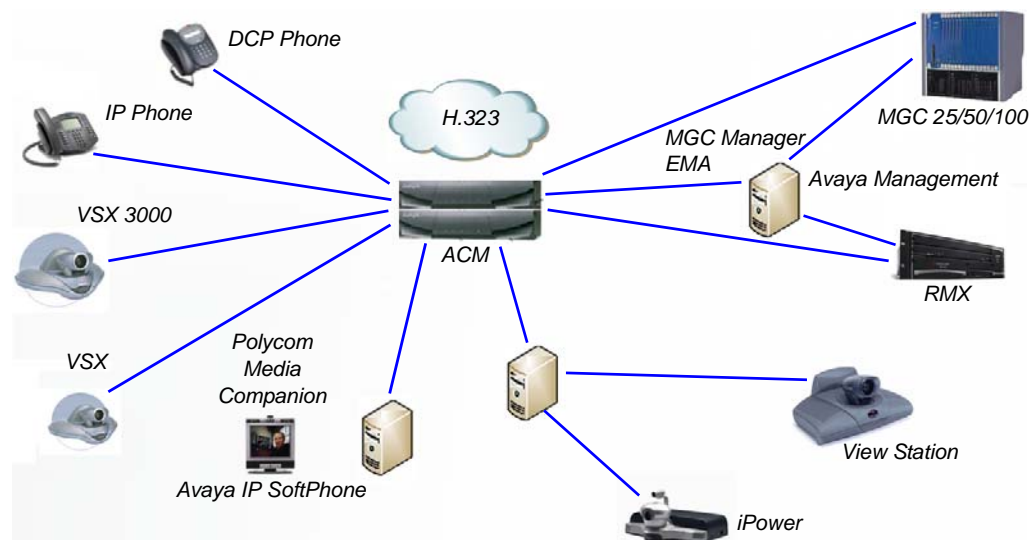


Figure 1-1 *Apollo* Environment R2 & R3.01 Architecture and System Components

Enabling Avaya Video Features

Avaya Video Features (AVF) support is licensed and is enabled by a specific field the RMX's license key.

Avaya Video Features (AVF) support is detected automatically and is activated if both of the following conditions are true:

- The RMX is licensed for *Avaya Video Features* (AVF) support
and
- *Avaya Communication Manager* (ACM) is selected as Gatekeeper

ACM as Gatekeeper

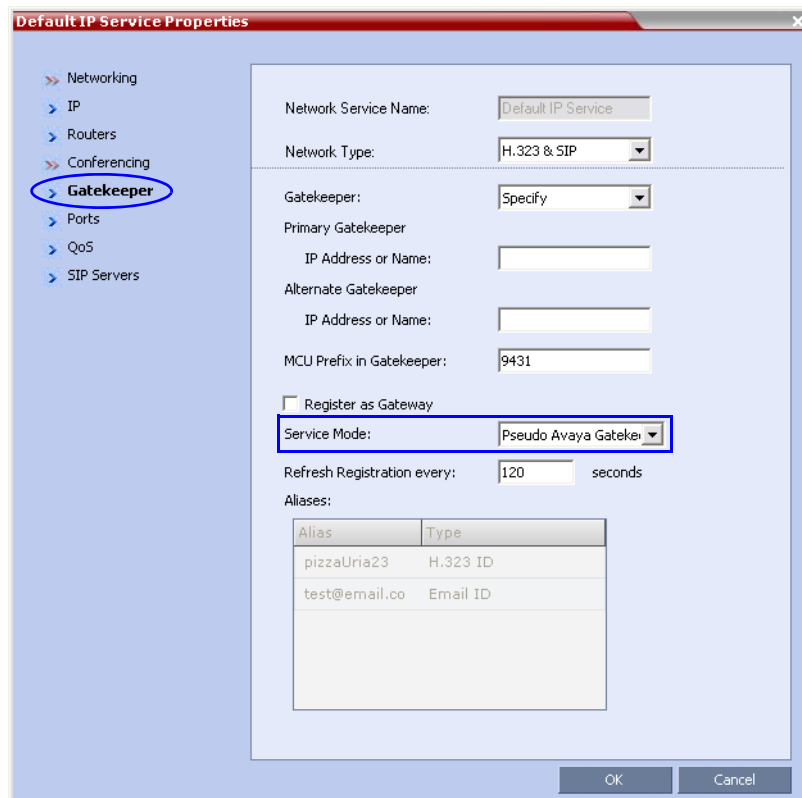
In its role as Gatekeeper, ACM performs the following functions:

- Management of bandwidth
- Routing of H.323 signaling (RAS, H.225, H.245)
- Initiation and control of telephony features

To select ACM as Gatekeeper:

- 1** In the *RMX Management* pane, click **IP Network Services**.
- 2** Double-click **Default IP Service** in the *IP Network Services* list pane.

- 3 Click the **Gatekeeper** tab.



Default IP Service Properties

- >> Networking
 - > IP
 - > Routers
 - >> Conferencing
 - > **Gatekeeper**
 - > Ports
 - > QoS
 - > SIP Servers

Network Service Name: Default IP Service

Network Type: H.323 & SIP

Gatekeeper: Specify

Primary Gatekeeper

IP Address or Name:

Alternate Gatekeeper

IP Address or Name:

MCU Prefix in Gatekeeper: 9431

Register as Gateway

Service Mode: **Pseudo Avaya Gatekeeper**

Refresh Registration every: 120 seconds

Aliases:

Alias	Type
pizzaUria23	H.323 ID
test@email.co	Email ID

OK Cancel

- 4 In the *Service Mode* drop-down menu, select **Pseudo Avaya Gatekeeper**.
- 5 Click **OK**.

Detailed Description - System Tools

Modem Support

Remote access to the RMX’s *Alternate Management Network* is supported via an external PSTN <=> IP modem.



To connect via modem to the *Alternate Management Network* the following procedures must be performed:

- 1 Procedure 1: Download and install the Local Web Client** - the web client enables direct access to the RMX for support purposes.
- 2 Procedure 2: Configure the modem** - by assigning it an IP address on a specific subnet in the *Alternate Management Network*.
- 3 Procedure 3: Create a dial-up connection** - using the *Windows New Connection Wizard*.
- 4 Procedure 4: Connect to the RMX** - via the *RMX Web Client*.

Procedure 1: Download and Install the Local Web Client

Before installing the *Local Web Client*, verify that you have at least 150Mb of free space on your workstation.

- 1** Download the *Local Web Client* from the Polycom website.
- 2** Open the *Local Web Client* folder and double-click the *.exe file.
- 3** Allow the installation to complete.

A shortcut to the *Local Web Client* () is placed on the Windows desktop and an Apache icon () is placed in the system tray .



The *Local Web Client* installs a **Pearl Script** and an **Apache Web Server** on your workstation. Port contention issues may arise if an *IIS* or *Apache Web Server* are currently installed on your workstation prior to the *Local Web Client* Installation. To remedy this issue, uninstall the *IIS* and *Apache Web Server* on your workstation and then run the *Local Web Client* installation file.

Procedure 2: Configure the Modem

Configure the modem as follows:

- **IP address** - near 169.254.192.nn
- **Subnet Mask** - 255.255.240.0



The following IP addresses should **not** be used:

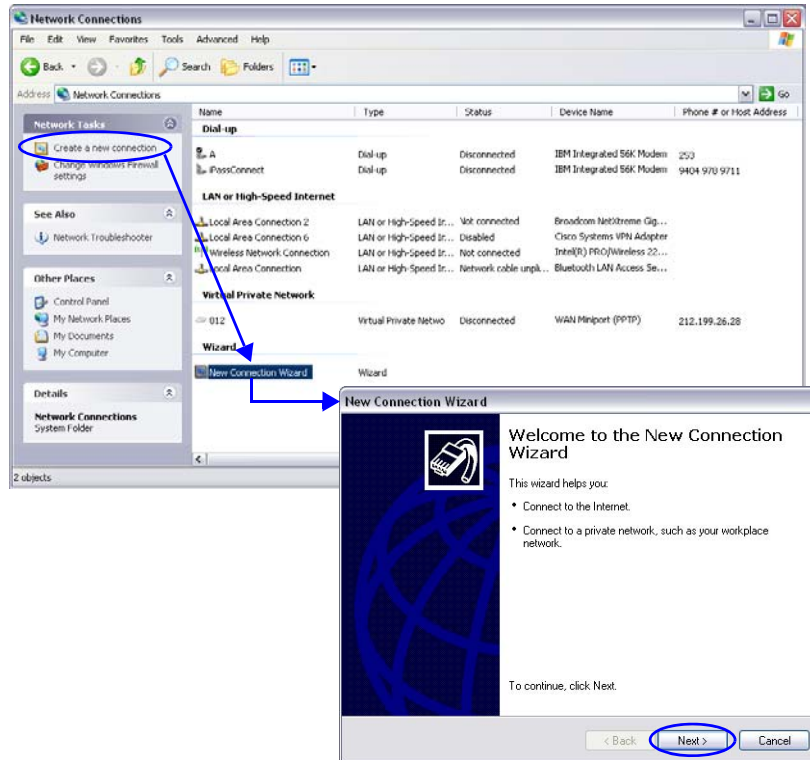
- 169.254.192.10 – the *Control Unit IP Address*
- 169.254.192.16 – the *Shelf Management IP Address*

Procedure 3: Create a Dial-up Connection

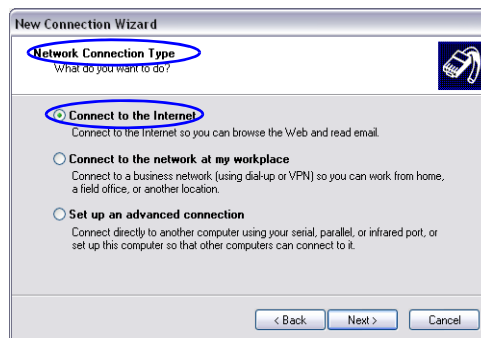
To create a dial-up connection:

This procedure is performed once. Only the *Dial* field in the *Connect* applet (see step 10 on page 1-68) is modified for connection to different modems.

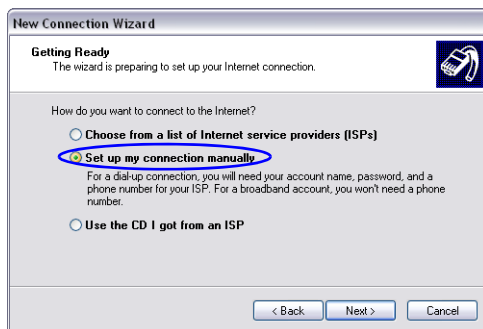
- 1 In *Windows*, navigate via the *Control Panel* to the *Network Connections* applet and select **Create a new connection**.
- 2 When the *New Connection Wizard* is displayed, click **Next**.



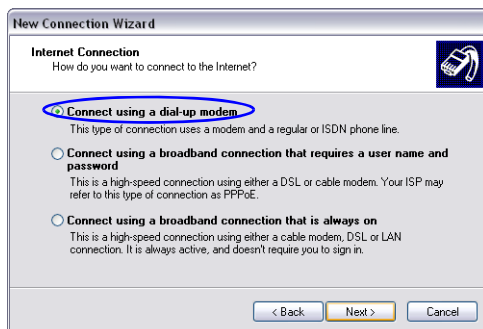
- 3 In the *Network Connection Type* box, select **Connect to the Internet** and click **Next**.



- In the *Getting Ready* box, select **Set up my connection manually** and click **Next**.



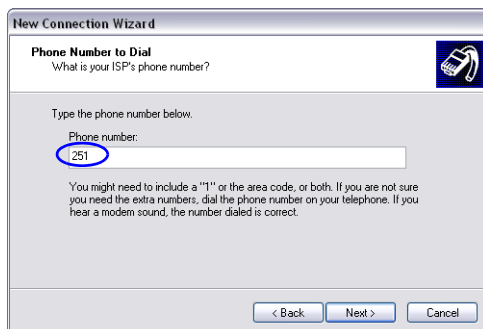
- In the *Internet Connection* box, select **Connect using dial-up modem** and click **Next**.



- In the *Connection Name* box, enter a **Name** for the modem connection (e.g. *Modem Connection*) and click **Next**.



- In the *Phone Number to Dial* box, enter the **Phone Number** for the modem and click **Next**.



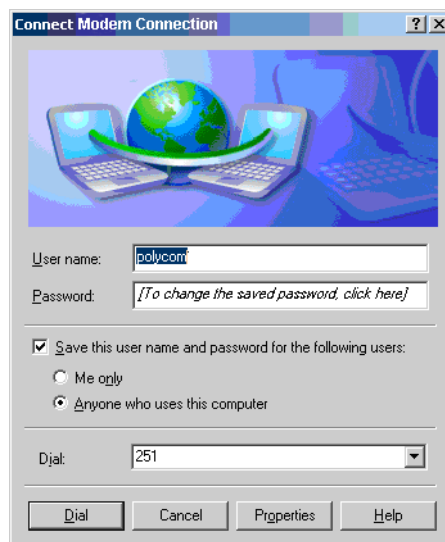
- 8 In the *Connection Availability* box, select **Anyone's use** and click **Next**.



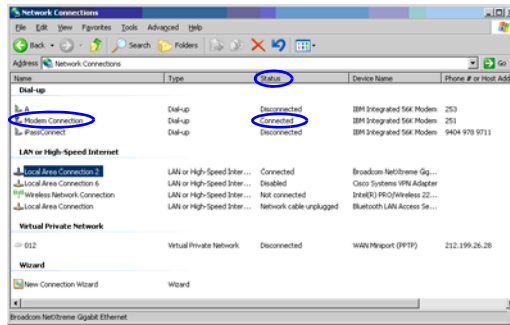
- 9 In the *Internet Account Information* box, complete the *Username*, *Password* and *Confirm Password* fields and click **Next**.



The *Connection* applet is displayed with the field values filled in as specified by the *New Connection Wizard*.




- 10 Click **Dial** to establish a connection to *LAN 3 Port* via the modem.
The *Windows – Network Connections* applet displays *Connected* status for the new connection.



Procedure 4: Connect to the RMX

To Connect to the RMX Web Client:

- 1 Double-click the shortcut to the *Local Web Client* () on the Windows desktop.
The *Local Web Client – Welcome* screen is displayed:



- 2 Enter the following:
 - *Username* <username>
 - *Password* <password>
 - *MCU IP* 169.254.192.10
 - *Port* 80
- 3 Click **Login**.

Corrections and Known Limitations

Version 2.0 Corrections

Table 3 Corrections

No.	Category	Description	ID - VNGR#	Workaround/ Remarks
1.	Cascading	In cascaded conferences the MCU connection may lose video.	2507	
2.	FECC	Various endpoints (View Station FX, Vcon-HD300, Aethra) failed to send FECC data.	3990 3770 3785 CQS	
3.	General	During RMX restart there is no indication or message of the system's reset.	3198	
4.	H.239	When an HDX endpoint switches from an H.239 Slide to 4SIF Video, an on-screen flash occurs.	3885 CQS	
5.	RMX Web Client	<p><i>RMX Web Client</i> does not display information in <i>Rarely Used</i> and <i>Frequently Used</i> sections of the <i>RMX Management</i> pane in the following Windows environments:</p> <ul style="list-style-type: none"> WinXP SP2 Pro Russian with IE6 SP2, .NET 1.1, 2 WinXP SP2 Pro Multilingual with IE6 SP2, .NET 1.1, 2 	4354	
6.	Video (SD)	Video distortion occurs when an HDX endpoint transmits movement, while connected at 1920K, at SD resolution.	3964 CQS	
7.	Video (SD)	In SD calls the fourth skin (the one with circles) is replaced by the third skin (the one with triangles).	3719	

Version 2.0 System Limitations

Table 4 System Limitations

No.	Category	Description	ID - VNGR#	Workaround/ Remarks
1.	Audio	AGC picks up background noise.	4845	Uncheck the participant's AGC checkbox in the <i>RMX Web Client</i> .
2.	Backward Compatibility	Version 2.0 has a different log file format to Version 1.1. Following an upgrade from Version 1.1 to Version 2.0, all log files from Version 1.1 are deleted.	4235	
3.	CDR	When the conference termination time is changed, the CDR is not updated.	1569	
4.	CDR	CDR records are not fully implemented for PSTN participants.	5865	
5.	Conferencing	When a busy signal is returned by a PSTN dial-out participant, the RMX does not redial, it disconnects with " <i>party hung-up-0</i> " status.	4405	
6.	Encryption	The Encryption field is missing from the CDR section.	3011	
7.	Entry Queue	When a Participant enters an Ad Hoc Entry Queue and creates an Ad Hoc conference with an ID that already exists as a conference name, the participant remain in the Entry Queue.	1528	
8.	Entry Queue	Defined dial-in participants are not recognized when connecting to a conference via an Entry Queue.	321	
9.	Gateway	All endpoints that dial-in to a conference using a Gateway receive identical names in the <i>Participants</i> pane,	1011	
10.	General	The <i>Click & View</i> menu doesn't appear in 64 Kbps calls.	3824	Use <i>RMX Web Client</i> .
11.	General	Legacy endpoints that support only H.261 do not connect or connect as Secondary	978	
12.	General	Upgrading V1.1 to V2.0 can take more than 15 minutes	5685	

Table 4 System Limitations

No.	Category	Description	ID - VNGR#	Workaround/ Remarks
13.	HD	In HD conferences, Tandberg endpoints may connect as Secondary when HD frame rate capabilities are less than 7.5 frames per second.	3089	Use HDCP.
14.	Inter-operability	HDX/VSX endpoints cannot connect directly to conferences while registered with Cisco Gatekeeper using the IP##NID string.	4652	Connect directly using the MCU IP Address via the <i>Transit Entry Queue</i> .
15.	Inter-operability	VSX (release 8.5.3) and FX (release 6.0.5) endpoints connect as secondary when connecting to RMX via MGC Gateway when MGC Gateway is in Video Switching mode.	5448 5446	Connect in CP mode.
16.	Inter-operability	MGC IP card crashes in Gateway call with RMX when the MGC Gateway is configured with <i>H.264 in GW</i> flag=NO. Crash occurs when ISDN endpoints are connected.	5569	Set <i>H.264 in GW</i> flag to YES.
17.	Inter-operability	HDX SIP participants connect at 4 SIF instead of HD 720p at 1920 Kbps. Applies to V1.0. Fixed in V2.0.	4698	
18.	Inter-operability	Faulty connection status is indicated when the RSS 2000 is the only participant in a conference. The MCU does not synchronize the video stream and of the RSS 2000.	3977	Be sure to connect at least one participant followed by the connection to the RSS 2000.
19.	Multilingual	Multilingual Setting is not reflected on the shelf login page	5310	
20.	Multilingual	In Multilingual mode, an undefined dial-in participant's name is displayed in English in the <i>RMX Web Client</i> when using HDX and VSX 7000 endpoints.	5151	
21.	NTP	RMX Time dialog box: While operating the external NTP (enable/disable) the clock is updated after 2 minutes. When updating the time manually, the clock is updated after 10 seconds.	3629	
22.	SIP	SIP participants cannot connect to a conference when the conference name contains blank spaces.	3276	

Table 4 System Limitations

No.	Category	Description	ID - VNGR#	Workaround/ Remarks
23.	Web Client	Windows Explorer >Internet Options> Security settings must be set to <i>Medium</i> or less when using the RMX Web Client.	2473	